TU Delft

Delft University of Technology

Challenging the chain. Governing the automated exchange and processing of business information

Bharosa, N; van Wijk, R; de Winne, N.; Janssen, MFWHA

DOI
10.3233/978-1-61499-497-8-i

Publication date
2015

Document Version
Final published version

Citation (APA)
Bharosa, N., van Wijk, R., de Winne, N., & Janssen, MFWHA. (Eds.) (2015). *Challenging the chain. Governing the automated exchange and processing of business information*. IOS Press.
https://doi.org/10.3233/978-1-61499-497-8-i

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

CHALLENGING THE CHAIN

Governing the automated exchange and processing of business information

Colophon

Edited by:
N. Bharosa PhD
R. van Wijk MA
N. de Winne MSc
M.F.W.H.A. Janssen PhD

Co-authors:
S. Bal MA LLM RA
E. Rigter MSc
H. van der Voort PhD
W. Fokkema LLM
B. Hendriksen MSc
V. den Bak MSc
P. Leijnse MSc
I.M. Saturday MSc
R.J. van der Meij MSc
S. Korpershoek MSc

Delft (the Netherlands), March 2015
This study was commissioned by Logius and carried out by Delft University of Technology.

Illustrations and cover design: Annemarie van der Linde
Background information: challengingthechain.com

ISBN: 978-1-61499-496-1 (print)
ISBN: 978-1-61499-497-8 (online)
DOI: 10.3233/978-1-61499-497-8-i

Published by IOS Press under the imprint Delft University Press. Published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.

© 2015 Logius & Thauris. All rights reserved.
No part of this publication may be duplicated, replicated and/or otherwise published without the written consent of the authors. Pursuant to Article 16 of the Dutch Copyright Act, the authors must be contacted beforehand for the reproduction of parts of this publication in readers or other collections. Although every possible care has been taken in the production of this publication, neither the authors, editors nor the publisher accept any liability for any errors and omissions or the consequences thereof.

Table of Contents

Preface by the Director of Logius

Logius provides standardised ICT solutions for electronic information processing and exchange. The need for such solutions is steadily increasing and it is a trend that cannot be stopped. Standardisation is therefore crucial. If everyone were to go their separate ways in computerisation, this would create heterogeneity and we would – to a huge extent – fail to utilise the opportunities provided by ICT to do more with less. That would seem not only stupid, but perhaps even dangerous. After all, money has become scarce. In addition, we have to realise that the labour market is shrinking rapidly because of demographic developments and we could end up with too few staff for operating information chains, although this may sound very strange to some people in the light of current unemployment rates.

It is evident to Logius that standardisation does not lead to limitations: on the contrary, it leads to increased freedom to achieve organisational objectives. Cleverly chosen standard building blocks and standard services enables flexibility, because they can easily be configured in numerous variations, depending on how new requirements and applications evolve. If used at a large scale – "mass is cash" – this may create permanent, substantial reductions in transaction costs for society as a whole. In addition, this is essential, because all the money that ends up siphoned off somewhere between the production and use of goods and services is wasted money.

In 2009, I gladly accepted the implementation of the Standard Business Reporting (SBR) programme under my supervision. This programme was committed to the realisation of far-reaching uniformity in the exchange and processing of business reports between businesses and administrative authorities. This uniformity requires stringent control of the standardisation of data, processes and technology. Logius accepted the role of chain orchestrator in this complex, public-private partnership.

The SBR concept might seem straightforward on the drawing board, but in 2009 there were only a few persons in the Netherlands who were capable of putting it into practice. A greater critical mass was required if this standardisation game was to be played at the appropriate level on a national scale. I therefore developed an ambitious knowledge agenda as part of the SBR programme. One of its offshoots is an executive master curriculum accommodated by Delft University of Technology. The first graduates of this curriculum are now working for employers such as Logius. This book leans on the concepts and theories that are taught in the curriculum that educates professionals in analysing and (re)designing information chains. It is a very useful guidebook for Logius and all other

parties who are working with Standard Business Reporting, or who would like to work with it. The book is also a source of inspiration to everyone who wants to gain more knowledge on the large and complex transformations that are taking place within our society under the banner of 'information chain computerisation'. This is because the book is not only about business reporting. I am firmly convinced that this book is also very suitable and relevant for the development of other information-intensive chains and collaborative networks.

I would like to take this opportunity to express my gratitude. First, I would like to thank the authors and reviewers for their efforts in writing this book and making the accumulated knowledge accessible for a broad audience. I support the invitation that they have issued – and that this book embodies – to everyone who is active in information chains to participate in the creation of later editions of this book. And of course, I would also like to thank the Tax and Customs Administration of the Netherlands for their decisive role as the 'launching customer' for Standard Business Reporting in the Netherlands. This country is one of the world's pioneers in these developments – which not only enhances our competitive position, but is also something to be proud of.

Steven Luitjens,
Director of Logius

Preface by the Director-General of the Tax and Customs Administration of the Netherlands

Over recent years, the Tax and Customs Administration has become part of increasingly longer information chains in which it collaborates with numerous actors. Our Medium-Term Plan for 2014–2017 even declares 'collaboration' as one of the four focus points.

To name a few examples: those who are obliged to withhold taxes have for a long time now been responsible for more than just the calculation and payment of wage taxes. They have also become providers of monthly wage data managed by the UWV (Dutch Employee Insurance Agency) that is widely used in the public sector. In addition – for crucial parts of the electronic infrastructure – the Tax and Customs Administration has become a customer of Logius, which also operates the DigiD (digital ID) system and the generic infrastructure. The generic infrastructure is one of the constituent elements of Standard Business Reporting (in addition to the Netherlands Taxonomy and the XBRL standard). SBR is also an outstanding example of collaboration that is not restricted to the governmental agencies only, but also extends to partners such as tax service providers, accountants, software developers and private users of data such as the banks.

After a lengthy start-up phase, SBR is now going full steam ahead (although this may be a somewhat outdated metaphor to use for such an innovative project). Let the numbers speak for themselves. By means of SBR, the Tax and Customs Administration has now received more than 4 million messages over the period from 2008 to mid-January 2014 (3.5 million of which were in 2013). It has registered over 400,000 authorisations and has sent 50,000 digital tax assessment copies. The Dutch Chamber of Commerce received 40,000 messages in the same period, 28,000 of which were in 2013. These numbers evidently demonstrate that we are making progress.

Because we are convinced of the added value of standardisation, the Tax and Customs Administration joined the development of Standard Business Reporting right from the start. Standardised information requests are good for companies that have to provide data to the government, and good for the government agencies that request this data. Now that the information exchange process has been set up and large numbers of messages are utilising the infrastructure, it is time to look ahead; this will then involve extending this success story to other sectors in society.

That is why I am pleased by the publication of this book. It sketches a realistic image of the challenge that awaits when a sector decides to employ SBR. It also highlights the risks that need to be managed and the opportunities offered. Consequently, this book can provide a positive impulse for expansion of the SBR concept. From my perspective as chair of the SBR council, I argue that this is valuable and that everyone should get the chance to use SBR. That is why I believe it is a great idea that Logius is presenting this book as a gift to its clients and partners. It will be a useful gift.

I would like to congratulate the editors and authors on this book, commend Logius for the idea of offering it as a gift, and encourage those receiving it to read about the possibilities provided by SBR. And above all, this book encourages collaboration!

Peter Veld,
Director-General of the Tax and Customs Administration of the Netherlands

About the Editors

Nitesh Bharosa
Nitesh Bharosa holds a PhD in information systems from the Delft University of Technology. Nitesh acted as lead researcher in the knowledge retention project that led to this book. In close collaboration with the chair of the editorial team (Remco van Wijk), Nitesh coordinated the writing, reviewing, editing and publishing activities for this book. He is the main author of Chapter 7 (Technical Foundations of SBR) and Chapter 8 (Information Chain Security). He co-authored Chapter 1 (Introduction), Chapter 4 (Steering Change) and Chapter 5 (Managing Data).

Nitesh is a consultant at Thauris | Management Centrum and visiting scholar/lecturer at Delft University of Technology. He can be contacted via n.bharosa@thauris.nl

Remco van Wijk
Remco van Wijk MSc designed the overall structure of this book. On the one hand, this structure had to reflect all the different aspects of the Standard Business Reporting (SBR) programme and its history. On the other hand, this structure had to provide those who want to work with SBR with a simple and precise understanding of all the elements and their relations. Remco is the main author of Chapter 1 (Introduction), Chapter 4 (Steering Change), Chapter 6 (I-Processes), Chapter 9 (Governance and Management) and Chapter 11 (Final Conclusions). He has also co-authored all the other chapters. Since 2007, Remco has played various roles on all levels of SBR and is often regarded as the 'intellectual conscience'. For the partners of Logius – the shared service centre – Remco was the go-to guy during the prelude to mandatory business reporting via SBR. He also designed the organisational blueprint for the SBR chain services provided by Logius. Within the SBR programme, Remco continues to promote knowledge transfer, proper project/programme management and open innovation.

Remco is currently a member of the Board of Thauris | Management Centrum. He regularly gives lectures and presentations about SBR and other chain innovations. Remco can be contacted via r.vanwijk@thauris.nl

Niels de Winne
Niels de Winne MSc has been involved in the SBR initiatives in various roles from 2004. The insiders consider Niels as the founding father of the overall SBR architecture. Niels was the programme manager for the Requirements Elicitation Programme for the generic infrastructure (GEIN). This programme yielded the (service-oriented) architecture for electronic communication between businesses and authorities. Niels was the project manager for the realisation and the initial use of the generic infrastructure, thereby providing a basis for the Digipoort, which is also used for SBR. Niels was responsible for the implementation impulse of SBR, in the role of operational programme manager on behalf of Logius from the end of 2009 to the beginning of 2013. Within the programme, he always championed a clear approach to the architecture.

Niels lend his extensive practical experience to ensure the quality of the content of this book. He was involved in producing all the chapters, focusing particularly on the (technical) correctness, structure (usefulness) and coherence.

Niels is currently a member of the Board at Thauris | Management Centrum and can be contacted via n.dewinne@thauris.nl

Marijn Janssen
Professor Marijn Janssen PhD took on the knowledge retention project that resulted in this book. He holds the Antoni van Leeuwenhoek chair of ICT & Governance at the faculty of Technology, Policy and Management of Delft University of Technology. He teaches a variety of subjects, including Design of Innovative ICT Infrastructures and Services and Business Process Management & Architecture. He also teaches Business Process & Technology for the MBA in Business Information Technology at the Nyenrode Business University. Marijn is also involved in classes at the Erasmus University Rotterdam. In addition, he is the manager of the master's in Compliance Design & Management, which discusses this book integrally as classroom material.

He co-authored Chapter 6 (I-Processes). As the proof-reader for various chapters, he focused on the relationships between practical issues and theory (concepts, insights and methods).

Marijn can be contacted via m.f.w.h.a.janssen@tudelft.nl

A Word of Thanks

Why did we write this book?
Standard Business Reporting (SBR) is a proven solution for system-to-system information exchange and processing. Various specialists from a range of knowledge areas have contributed to this solution. There are a few reasons for disseminating the acquired knowledge using an open access book.

Firstly, for the parties involved – the insiders – it is important that the lessons learned and the tacit knowledge of the involved specialists are captured in a book. This book should provide an overview, as well as detailed descriptions of the building blocks of the SBR solution. Looking ahead, this book should further streamline communication and cooperation between specialists by providing clear definitions and detailed descriptions of the relevant concepts, methods and relations.

Secondly, it is important for the outsiders – other parties who might be interested in using SBR in other domains/information chains – to have an overview and a proper picture of the SBR building blocks, plus the conditions for a positive business case when they intend to employ (parts of) the SBR solution in an information chain.

Thirdly, the knowledge captured is useful for educational purposes. Although there are already numerous textbooks on the various relevant disciplines such as ICT, law, change management, governance and service management, few books provide interdisciplinary accounts on the challenges and solutions for information chains. For those academic programmes looking for inter-disciplinary course material, this book may be a good starting point.

Finally, it is vital for the academic community to continuously evaluate and define the most pressing research questions and under-explored fields of study. We gratefully made use of the existing literature when writing this book. In doing so, we concluded that previous work has not yet covered some of the relevant concepts and their relations integrally. The final sections of various chapters in this book discuss a number of possible avenues for further research.

How did we write this book?
This book is the result of a joined effort by both practitioners and scholars. The editors have written some parts of this book and coordinated the contributions made by others. Contributions from other authors include writing, reviewing or more general input (such as taking part in think tank sessions and interviews,

providing documentation and so forth). Appendix B sketches the writing process in more detail.

It is important to note that this book was initially written and published in Dutch. After publication in March 2014, the Dutch version was translated into English. However, the current version is not simply a translation of the Dutch version. As editors, we have received some constructive comments on the Dutch version. This includes comments regarding:

- The overlap between chapters 2, 3 and 4 regarding the instruments for steering change.
- The substance of chapters 5, 6 and 7 (restructuring and updates).
- The sequence of the chapters 5 and 6; a reversed treatment of the subjects I-processes and data was suggested by multiple readers.
- The scope of Chapter 8 (information assurance versus security).
- The phases, guidelines and supporting figures in Chapter 10.
- Overall: the definition of SBR building blocks and the consistent use of definitions throughout the various chapters.

The editorial team is committed to sharing the insights and best practices with the (inter)national community. The publication of the Dutch version revealed that both practitioners and scholars use this book as a reference. From an editorial perspective, it is important that the contents are as timely, correct and accurate as possible. Therefore, we were pleased with the comments. In order to process the comments in a structured and coherent way, we set up a small team of persons that would help update the various chapters of the translated version in close collaboration with the initial authors. We also appointed some additional reviewers to read and check the resulting updates. Accordingly, the English version has a longer list of authors and reviewers than the Dutch version. The section entitled 'About the contributors' lists all who have contributed to both the Dutch and the English version. The remainder of this acknowledgement discusses the types of contributions from those involved.

Who were involved?

Let us start with the authors. These are all specialists in their fields. During the process of writing, it became clear that getting their tacit knowledge on paper was hard, especially considering the stringent requirements imposed by Logius (the principal) and the editors. The chapters had to provide in-depth descriptions of the knowledge acquired in SBR, as well as being up to date and factually accurate. Arguments should have either theoretical or empirical support. They also needed to be concrete, whereas parts of the SBR story were still diffuse and unfolding. Moreover, the resulting chapters had to be easy to read for everyone (without too much community jargon). To comply with all these requirements, the authors' creative processes not only required expertise, but also took a lot of time and flexibility.

In close consultation with the authors, we asked their peers to review a chapter, i.e. check it for inconsistencies and factual errors. All the reviewers immediately

responded enthusiastically and affirmatively to the request to review a chapter. Shortly after that, the chapters and review forms were sent to them. Interim discussions with the reviewers revealed that the review process was turning out to be a tough job. One of the reviewers summarised this process nicely as *"you're asking me to review complex stuff with many concepts that overlap and depend on one another. Moreover, we are still in the midst of understanding the latest developments regarding SBR. I'm doing what I can to complete my review within four weeks..."* Fortunately, the reviewers were still able to provide some concrete suggestions. With these, we started an improvement process in consultation with the authors. The bulk of these points were about simplification and clarification (using familiar examples). However, we do have to admit that not all suggestions for improvement were finally implemented. This was because we – the editors – had to maintain a certain storyline. Some suggestions for improvement – such as specifying the workings of the generic infrastructure in Chapter 1 – were understandable from the point of view of the single chapter under review. Sticking to the storyline (where Chapter 7 elaborates on the workings of the generic infrastructure) led us to not implementing these types of suggestions. Nevertheless, the reviewers will still be able to recognise the majority of their comments in this book.

Finally, we would like to put the spotlights on four people for a moment. Firstly, we would like to thank Frans Hietbrink for his very active feedback on the entire book. Frans plays an imperative role in SBR and we had to resist the temptation to include him in the list of success factors in several of the chapters. We would also like to thank Rob Kuipers. In his role as the 'Dutch SBR commissioner', Rob contributes significantly to the implementation of SBR in other domains. Ella Broos and Jan Pasmooij also deserve our gratitude because of their patience in their role as process controllers at Logius. The stringent quality requirements that the individual chapters had to meet demanded a great deal of harmonisation and patience. Ideas had to bloom. There were some occasions when parts that at first seemed complete, had to be broken down and rebuilt after all. Ella and Jan managed to facilitate this superbly. Thanks to you all!

The editors
Delft (Netherlands), March 2015

Prologue

If someone were to tell you at a party that her job encompasses financial reporting, software development, accountancy, assurance, administrative and fiscal law, auditing, public key infrastructures, credit reporting, information processes, XBRL, taxonomies and public-private partnerships, you might wonder for a while what on earth she is talking about. You might even suspect that the person in question is suffering from a narcissistic personality disorder. However, we can assure you that this person may be less crazy than you think. People who are involved in the implementation of Standard Business Reporting (SBR) simply have to know something about all the disciplines and professional fields mentioned above. To put it even more strongly, the list was not even exhaustive. This does not mean that they are specialists on all of these subjects. However, they should have mastered the basic principles and interrelationships.

SBR is about electronically exchanging and processing information between reporting and requesting parties in a standardised way. This may relate to filing tax returns (e.g., VAT, corporate income tax), submission of annual financial statements, production and investment statistics and more. Reporting parties include small, medium and large businesses, but also intermediaries or service providers that may act on their behalf. Requesting parties include public agencies or private parties. SBR also prescribes how return messages or e-notifica-

tions from requesting parties can be obtained by the reporting parties in a reliable and confidential manner. To achieve the standardised exchange and processing of business information, public and private parties use the SBR framework of agreements. This framework provides guidance on the lawful configuration of information chains for specific reporting obligations. A reporting chain starts with the business that has to account for its actions and performance, and ends at the party that requested the information. In order to exchange data for these reporting obligations, the chains use various common services provided by a shared service centre. This creates interdependencies between the parties within these chains, which demands that they are all singing from the same hymn sheet. This certainly does not mean that SBR as a concept is only intended for the *uomo universale*. On the contrary. SBR is about the integral understanding of a certain cross-section of the world. Because this cross-section is different from what we are used to, it may seem excessive, but in practice it is not so. The problem is that people have been searching in vain for an overview that provides an outline of this cross-section. This book can be considered as a starting point.

The idea for consolidating the knowledge about SBR came up at the end of 2010. At that moment, some administrative authorities were already successfully using SBR in financial reporting chains. However, this only involved relatively small volumes, whereas (as often applies to standardisation in general) the business case for SBR benefits from large-scale and wider use of the standard. A stable and broad knowledge base may help bring about this scaling up. The possible upscaling suddenly came quite a bit closer in December 2010 when the Tax and Customs Administration presented a plan to start phasing out (from 2013 onwards) the information exchange channel that competed with SBR: BAPI[1]. The Association of Chambers of Commerce and Statistics Netherlands suddenly indicated that they would be taking measures in the long run to reduce paper communication and that SBR would also be their standard for setting up the electronic channels. The requisite knowledge base was suddenly no longer just nice to have and had instead become a 'must have'. Logius and Delft University of Technology have therefore combined the knowledge and experience of experts from the SBR domain into a single overview work.

The experiences of the specialists involved in SBR provide the foundations for this book. Scholars from different backgrounds helped elaborate and enrich the practical examples using theoretical concepts and frameworks.

The result shows that the SBR programme is an eventful, content-rich change initiative with a considerable information and communication technology (ICT)

1 BAPI is an acronym for Belastingdienst Advanced Program Integration. Before the implementation of SBR, reporting parties were required to use this channel for filing business reports exclusively to the Tax and Customs Administration.

component. In their work, the authors pay a lot of attention to how this development has come about and the background information required for understanding the current SBR application. The development of SBR is very much driven by a policy-based ambition to use ICT to tackle administrative burdens. SBR therefore is part of a series of initiatives that are often still ongoing and which aim to create smaller and effective administrative authorities by means of systematic redesign of chains. The retrospective considerations of the SBR case in this book provide insights and best practices that may be relevant for parties who do not use SBR in their search for cost-effective information chains.

Looking more closely, we see that this book discusses two perspectives on SBR. On the one hand, it provides insights into the creation of an initiative such as SBR and describes the challenges that actors face when striving to redesign and improve information exchange and processing in information chains. In this respect, we can see SBR as a challenge for information chains. On the other hand, this book provides concrete descriptions of the SBR solution components (building blocks) realised in the Netherlands. These building blocks can be used in a 'plug and play' manner in an information chain to make sure it operates more cost-effectively. In an empirical approach, the black box is broken open in order to create a picture of the technology, interactions, interrelationships and interdependencies that control the developments and choices. In our opinion, connecting these two perspectives – approaching SBR as a challenge and as a solution – fits within the general policy valuation of ICT initiatives.

For some years now, there has been political pressure on government agencies to do 'more with less'. While considerable cutbacks are being imposed on administrative authorities, citizens and businesses seem to expect higher service levels in their interactions with the government. Many government activities are knowledge-intensive (e.g., policy-making and legislation) or require administration (e.g., processing requests and business reports). It is therefore obvious to think that the government should be able to reap huge benefits from efficient use of ICT. IT-based innovations are often seen as a panacea, a miracle drug that will take us towards leaner government. The Scientific Council for Government Policy (WRR) concludes that the use of technology is seen as only natural at the national, international and European levels (WRR, 2011). Technology is rolled out, practices are streamlined and services are updated. The confidence of politics and policy in technology is being translated into large-scale ICT ambitions, not only in a technical sense, but undoubtedly in terms of policy too.

Anyone who regularly follows the news will keep hearing about unsuccessful governmental ICT projects. Large ICT projects have a tendency to get out of hand: they are often more expensive and work less well than had been expected. In 2007, the Netherlands Court of Audit published two in-depth reports on the lessons learned from governmental ICT projects (Algemene Rekenkamer, 2007, 2008). Conclusion: billions are being wasted in large ICT projects. According to the Netherlands Court of Audit, this is caused by unrealistic ambitions, the tendency of authorities to make projects more complex than necessary and the urge

to get additional requirements added later on (scope creep). According to this report, the tensions between political, organisational and technical factors are underestimated. Continuous changes, uncertainty about the impact and lack of mandates for the business cases are other factors that play a role (Janssen et al., 2010). If a project is failing or on the verge of failing, cancelling the project is an extreme measure that is often preceded by difficult decision-making processes (Wortmann & Kremer, 2011). Unfortunately, there are only losers in such cases. Neither the client nor the contractor wants this to happen. A few notorious examples of problematic cases in the Netherlands include[2]:

- the modernisation of the Municipal Personal Records Database (GBA) used by government organisations and designated institutions that has been going on for more than a decade,
- the Electronic Patient Dossier – a virtual file for storing and sharing medical data on a national scale – facing strong resistance from physicians and patients;
- the incident registration system of the Dutch Police that still does not satisfy the required quality standards.

Failures of projects – in both the public and private sectors – have not gone unnoticed and have led to an increasing number of studies, inside and outside the Netherlands. Although the majority of the studies focus on exposing the causes of project failures after the event, we are also seeing a growing number of 'best practices' methods that should provide guidance for the successful realisation of programmes and projects. The best practices concentrate on project management in general (e.g., PRINCE2 and Managing Successful Programmes), as well as on ICT projects in particular (e.g., Agile and SCRUM).

However, the number of ICT projects that are not successfully completed is still inexplicably high, particularly given the amount of best practices that are available. This contrast is elegantly described in Cobb's paradox, which states: *"We know why projects fail, we know how to prevent their failure – so why do they still fail?"* (Martin Cobb, quoted in an article of the Royal Academy of Engineering, 2004).

A typical feature of examples of problematic ICT implementations is the fact that they involve complex change processes. The complexity is expressed in various dimensions. These could be the throughput time, for instance, or the financing model, change control, the large number of parties involved or the high degree of uncertainty regarding the technology and its impact on cultures, organisational structures and processes. The implementation demands knowledge and experience from various (specialist) disciplines. This generally involves multiple autonomous parties, aiming to create a system that has an effect on core processes

[2] The final report of the Temporary Committee on Government ICT Projects (2014) provides more details and examples.

of the parties involved, or at least some of them. The initiatives affect the public interest and are therefore subject to considerable political interference. The provision of services must continue (the shop remains open during the renovation). The public context demands a proper alignment between the actual implementation, the legislation and the general principles of good administration. Such regulatory frameworks cannot be changed easily. The cooperation between parties with a public task is brought about in a different way than in the commercial sector. Parties depend formally on each other in the public domain. Generally, we cannot assume a hierarchical relationship between the cooperating parties. Moreover, drivers such as a jointly determined business opportunity or a necessity to cooperate imposed by financial factors.

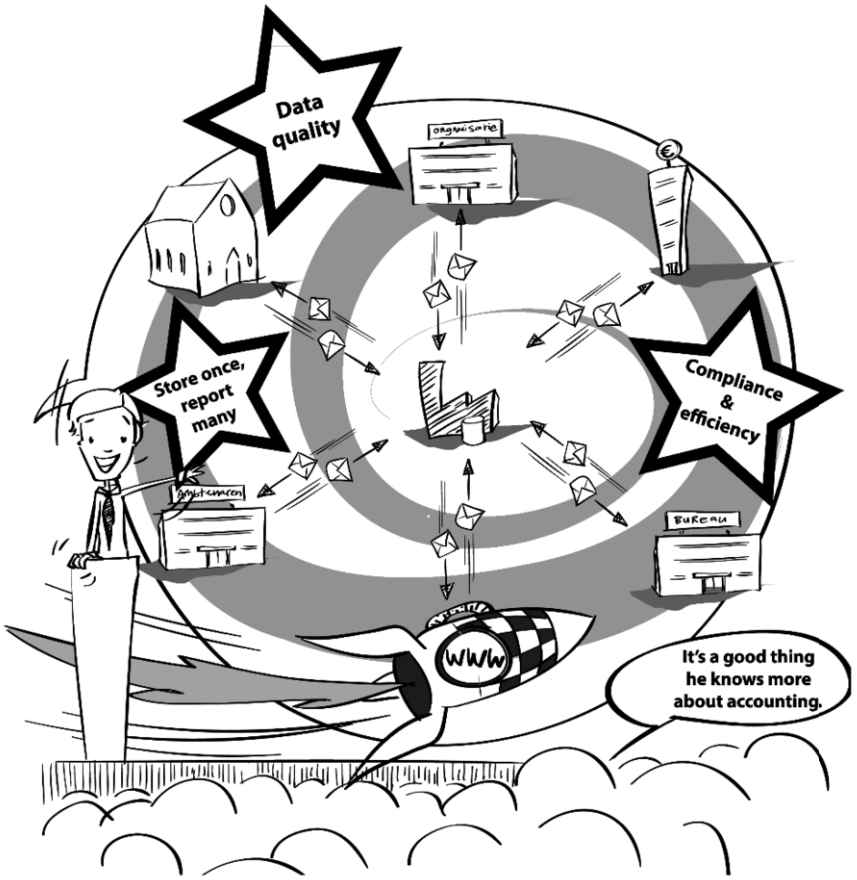
Although the description of the difficulties stated above only relates to a few items, we have to ask ourselves whether the ICT initiatives mentioned are just ICT projects. In other words, are we incorrectly sticking the ICT label onto a large number of fundamental changes within society? Should we adjust our expectations about costs and benefits of ICT in the public domain? Or can we actually reap the benefits against 'acceptable' cost? Are there any lessons learned that we should follow to get it right?

This book provides unique insights into the history, context and realisation of one such extensive ICT programme. It gives the reader new insights to help find answers to the questions stated above, using a concrete case. These insights by no means tell you what you should do in terms of the management of large ICT programmes. We do not claim to have a solution for all problems that occur in ICT programmes. Nevertheless, we have chosen to use formulations that are as generic as possible for the problems, dilemmas and solutions to ensure that they can be identified and used in other contexts and programmes too. Others can learn from this so that they will not have to go through the same learning process again. This book has gratefully made use of the knowledge and experience of experts who are involved in SBR.

Although all chapters contain some degree of SBR as a challenge and as a solution for information chains, the editors have divided this book into two parts. Part A elaborates on the challenge to be found in the redesign of information chains: "SBR as a challenge". The three chapters in Part A expose some very specific obstacles in information chains. It is important to understand these obstacles because they shape the requirements for a solution. Part B – "SBR as a solution" – discusses the concrete setup of SBR chains, the individual building blocks and how they contribute to the cost-effective exchange and processing of information. Part B consists of six chapters, each of which cover a specific SBR building block, ranging from data specifications to the SBR chain governance.

This page intentionally left blank

1 Introduction



Chapter highlights

- How Standard Business Reporting is relevant to you
- The evolution of information exchange
- Benefits of standardised information exchange and processing

1.1 What is business reporting?

Business reporting, by which firms are required to disclose financial and non-financial information about their performance to internal and external parties (e.g., creditors and public agencies), is a common practice in most countries. In fact, the majority of the world's democratic governments currently call for some form of information disclosure for a variety of purposes, assessing taxes, building

statistics, drafting industry guidelines and so on, as well as to enact proper governance, policy-making and enforcement. Business reports enable government agencies to do their jobs and implement their policies. They also lead to the formation of several business reporting chains. Examples of business reporting include the publication of financial statements, VAT declarations to the Tax and Customs Administration and credit reporting to banks. From the perspective of the company or firm doing the reporting, information exchange usually involves submitting 'business reports.' Such reporting can be realised with or without the help of (financial) intermediaries (also known as service providers) and specialised commercial software for the preparation and electronic filing of reports. The term 'business' is used to describe a range of reporting parties that are required to disclose or file information, from entrepreneurs to multi-national corporations. Businesses can hire intermediaries to do (part of) their business reporting for them, such as accountants, bookkeepers, financial advisers, tax consultants and fiscal advisers. In practice, the majority of businesses employ intermediaries to prepare and electronically file business reports to public and private organisations (e.g., banks) on their behalf.

Some examples of business reports

- Value added Tax Return
- Corporate Income Tax Return
- European sales list
- Annual financial statements
- Production and investment statistics
- Credit reports to banks

1.1.1 *What is driving the agenda?*

The extent of the actual reporting varies per country and domain but is generally substantial and has increased over recent years due to more rigorous regulatory requirements (OECD, 2009). Historically, business reporting requirements have grown in a piecemeal fashion, often driven by diverse legislation and disparate government agencies with little to no coordination between them regarding what information should be reported and how it should be reported. A reporting party will often end up reporting the same information multiple times in different formats to separate government agencies via different channels. Government agencies, on the other hand, receive low quality information and are often unable to capture the benefits of standardisation or advanced information technology.

To address such issues, public agencies in the Netherlands have collaborated extensively with the private sector to develop a generic and sustainable solution known as Standard Business Reporting (SBR). SBR provides governments and businesses with an unequivocal, cost-effective, secure and adaptable method for the exchange of business information between organisations in a reporting chain. SBR applies international open standards, including XBRL, X.509 and SOAP-based web services. Standards are used in a way that enables loose coupling and a high degree of automation within the business reporting process – from data gathering and transfer to validation and processing. SBR is currently being used in multiple business reporting chains in the Netherlands. Chains that have adopted the SBR building blocks are known as SBR chains.

As detailed in Appendix A, several consecutive projects and programmes have contributed to the realisation of SBR in the Netherlands, all of them aimed at improving information exchange and processing between businesses and government agencies. The overall vision was to achieve this through the proper use of 'advanced' information technology (IT) within the numerous reporting chains. A preliminary proposal for the solution was presented in 2006, with slogans such as '*store once, report many*' and '*chain reversal*'. Service providers involved in business reporting then entered a covenant with governmental bodies, in which both sides promised to make an effort to set up the reporting chains in accordance with the proposed solution. The covenant included the signatures of numerous software providers, key audit firms, the VNO-NCW (Confederation of Netherlands Industry and Employers), and SMB Netherlands (Association for small and medium-sized businesses), as well as the signatures of three ministers and one State Secretary.

Despite a promising start, however, the effort turned out to be more difficult than expected. Seven years after the covenant was signed and two years following it implementation, only one large-scale application of SBR was in place, in a single fiscal chain. Why did the implementation take so much time? The objective of the first part of this book (Part A) is to share insights into the challenges that led to this delay. An obvious cause for the delay is that the realisation and implementation of the necessary information technology required more effort than anticipated. The proposed solution – which we will describe in detail in section 1.5 – needed to meet a complex need. In addition, the technology that was a precondition for the proposed solution was not yet in widespread use when the SBR-related initiative started. Therefore, there were still a number of technical issues affecting the design and development of the initiative.

Yet, in hindsight, it is clear that the biggest challenges were more organisational in nature than technological. One of the challenges, in particular, was the need to create an appropriate governance structure for the solution as it matured, which would

1) have sufficient capabilities to realise the next step in the development and implementation process, and
2) fit in properly with future structures, fitting both the solution and its governance structure (i.e. the final organisational embedding).

Our statement that realising a proper governance proved to be more challenging than technology is supported by the fact that the technology and its underlying architecture – as adopted at the outset of the SBR Programme – has essentially remained unchanged. The governance and its embedding across the various parties, however, *has* been subject to various radical metamorphoses over time; furthermore, because of the increased (and more mature) application of SBR in terms of reporting, at least one further radical change will be necessary in the future. Part A of this book, entitled "SBR as a challenge," explores, in particular, the organisational aspects of the challenge. The chapters of Part A first discuss the organisational context (i.e. the chains, links and dependencies), followed by

the challenges of change management within chains and how to control for changes in inter-organisational information systems.

SBR is now widely used in fiscal and financial reporting chains (e.g., corporate income tax, VAT tax, annual financial statements). Generic components that use SBR standards have been developed by governmental bodies for this purpose. Part B of this text defines SBR as a solution for reporting to public agencies. The chapters provide the theory underlying certain SBR building blocks, and also describe the current state of SBR. The issues addressed include data management, process management, technology, information security, governance, control, and finally, how stakeholder involvement in a particular reporting chain can transition to SBR in a structured way. The book ends with a reflection on the opportunities and threats for SBR as a solution.

In order to provide the necessary background for Parts A and B, and to outline the relationship between the two parts, this introduction presents the long-term vision that the SBR Programme and its predecessors were based on. The introduction provides an outline of SBR as a generic governmental solution for system-to-system (S2S) exchange and shared processing of business reports. The remainder of this chapter proceeds as follows:

- **Section 1.2** presents the technological developments that enable the S2S integration of information chains and digital reporting. We will consider the potential for, and the consequences of, S2S information processing.
- **Section 1.3** discusses the S2S integration of business reporting chains and describes the design requirements for the intended solution, based on the characteristics of business reporting chains.
- **Section 1.4** reveals the technological components of the proposed solution that are needed in order to satisfy the complex design requirements in business reporting chains.
- **Section 1.5** continues with an analysis of the organisational context in which the technology needed to be implemented. We shall pay some attention to chain governance, which was originally a somewhat neglected aspect of the solution.
- **Section 1.5** concludes this introduction with a reading guide that introduces the subsequent chapters.

1.2 What are the enablers for digital reporting?

1.2.1 *Computerisation and chain information systems*

In the late eighties and early nineties, computerisation of information processing within organisations increased tremendously (Chaffy, 2004; van Oost, Alberts, van den Ende, & Lintsen, 1998). Information processes are partially or entirely

handled by automated information and communication technology (ICT) systems[3]. The processing of information as part of an organisation's administrative processes – such as bookkeeping, stocks, etc. – is usually the first element to be considered for computerisation (Jans, 1991). Furthermore, cooperation and sharing of information between organisations effectively leads to the creation of a supra-organisational information system. We call this the inter-organisational information system or chain information system. Note that the term chain information system is usually reserved for information exchange between more than two organisations. In such systems, actors often long for more efficiency through further automation.

Take, for example, a car parts retailer and his supplier, who do not have linked/coupled information systems. The retailer sees a message in his stock management system informing him that only two items of a particular component are still in stock. The retailer decides to order the additional items from his supplier by phone. The supplier writes down the order on paper and places the order in his sales system. Human intervention is thus required to process the information passing between the retailer and supplier. This is known as human-to-human (H2H) coupling within information systems, and is depicted in Figure 1.1.

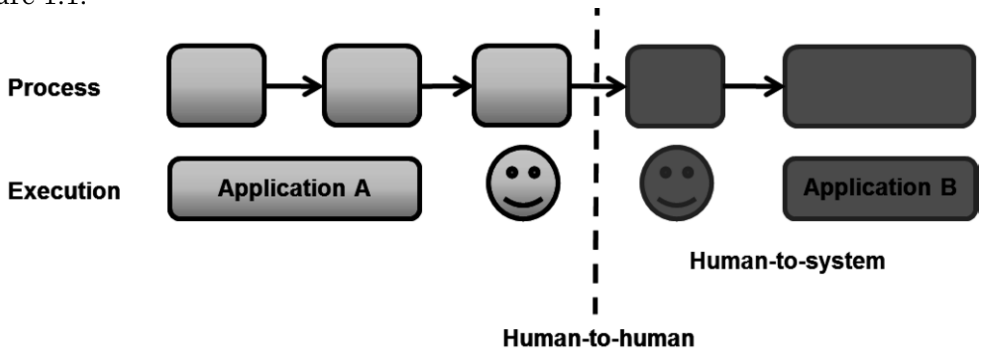


Figure 1.1 – H2H and H2S interaction between organisations within an inter-organisational information system

When organisations use human-to-human communication for information exchange, humans are often the weak link in the inter-organisational information chain. There are several reasons for this:

- Re-entering of information leads to risk for errors.
- Intermediate actions (approvals) take a lot of time.
- Human actions become relatively more expensive as computing power and storage become cheaper.

3 The era of automated and semi-automated information systems, often simply referred to as 'systems' for the sake of simplicity, was triggered by the emergence of information and communication technology (ICT). Such information systems consist of one or more computers (hardware), programs (software), datasets, procedures and people (Looijen, 2004).

These disadvantages begin to weigh heavily once the volume and frequency of information transfer between organisations increases. One well-documented example is the automotive supply chain, in which companies are increasingly dependent on information from other businesses' systems for their own business processes (Tuunainen, 1999).

The emergence of information exchange standards such as the Electronic Data Interchange (EDI) developed in the eighties has provided a mitigating effect for the disadvantages listed above by reducing the human element of inter-organisational information processing.

Hansen & Hill (1989) define EDI as *"the movement of business documents electronically between or within firms (including their agents or intermediaries) in a structured, machine-retrievable data format that permits data to be transferred, without re-keying, from a business application in one location to a business application in another location" (p.405).* This definition of EDI emphasises the following points:

1. The transfer of data between applications is done electronically within or between organisations.
2. Machines (computers) can retrieve and transfer information without having to retype it (thus avoiding human intervention).

Whether the data exchange and processing is fully automated (system-to-system integration) or whether some parts of the data exchange or processing are assisted by human operators (system-to-human integration) is an important aspect of chain information systems (see Kauremaa, Kärkkäinen and Ala-Risku, 2009).

A second revolution, in the field of automation (i.e. computerisation), took place during the mid-nineties through the turn of this century. Wide adoption of the TCP/IP protocol, the emergence of the Internet and an enormous increase in available bandwidth ensured that parties could connect, with the ability to inexpensively transfer of large amounts of data.

As a result, S2S chain integration became both more feasible and more lucrative (Hofman, 2003; Vidgen, Avison, Wood, & Wood-Harper, 2002). In addition, the emergence of the Internet led to an enormous increase in what is referred to as human-to-system (H2S) chain integration, in which users can log directly into the systems of other parties in a chain. Figure 1.2 provides an example of chain integration using the Internet.

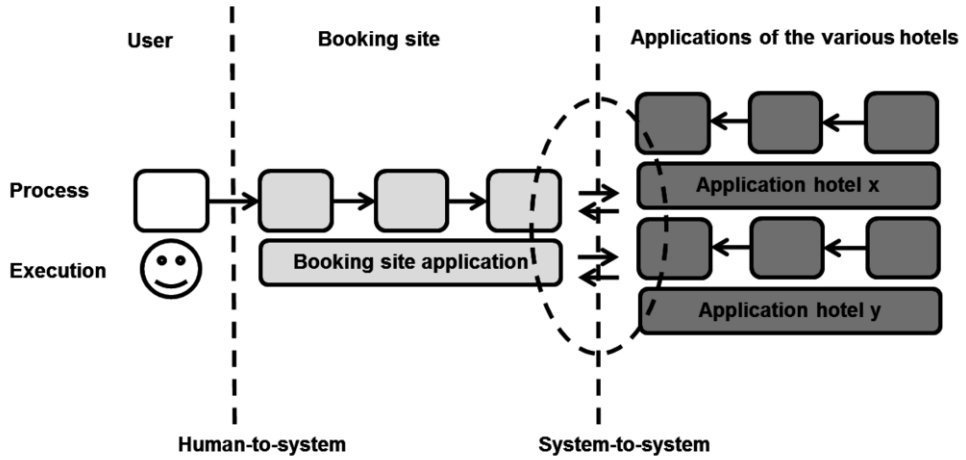


Figure 1.2 – A booking site as an example of chain integration over the Internet: H2S chain integration (user logs into the booking site) and S2S chain integration (between the booking site and the systems of the hotels)

1.2.2 *Horizontal and vertical S2S integration*

As S2S chain integration plays a key role in SBR, it is important to make a distinction between the two different types of integration. The first integration type has already been mentioned; it comprises more efficient and more effective coupling of organisations' IT systems. We call this 'horizontal S2S integration' of the inter-organisational information system. Some of the advantages of horizontal integration are as follows:

- **More efficient processing:** Systems (front office/back office and inter-organisational) are able to process information in only a fraction of the time required for people to do it. Time is saved by not needing to look up addresses, sources of information, or exchange conditions (e.g., the maximum message size) every time a message comes in. Because connection parameters have been defined and processing runs automatically, quick feedback is ensured in the form of receipt confirmations or error notifications. Greater efficiency is achieved by eliminating duplicate actions, for instance by ensuring that information does not need to be retyped.
- **Fewer errors/higher-quality data:** Research has shown that re-keying information often leads to errors (Redman, 1995). The risk of unauthorised access or modifications is also reduced when S2S integration is in place, as it allows for better access control than when human intervention is required. Other information security aspects will be addressed in Part B of this book.

An important precondition for horizontal S2S integration is a high level of interoperability. In general, this concept refers to the extent to which the various technologies used within a chain can communicate with each other or can be used together for a given purpose. Information systems are layered entities (Reynolds & Stair, 2013). Organisations must often create multiple layers of

agreements if interoperability is to be attained. In the literature, theoreticians have linked a variety of definitions to this concept of interoperability, depending on the emphasis chosen (one layer or multiple layers). The following is a summary of a few definitions from the literature (Scholl & Klischewski, 2007):

- Technical interoperability: The ability of systems to communicate with each other at the infrastructure (communications network) and software levels. Simply put, it refers to two-way communication between two or more applications over a physical network.
- Syntactic interoperability: The ability of systems to use information received immediately (without the need for manual conversions) in an information process (an 'I-process'). This indicates the use of a common meta-language between parties for recording data, which can be thought of as applying the same grammar and alphabet to a common vocabulary. XML (eXtensible Markup Language) and XBRL (eXtensible Business Reporting Language) are examples of frequently-used meta-languages; these will be described in Chapter 5.
- Semantic interoperability: The ability of systems to interpret the data from the sending and receiving parties in the same way. Explicitly recording the interpretation of data meaning is recommended.
- Organisational interoperability: The ability of organisations to set up systems (including roles, tasks, structures and processes) in such a way that data can be exchanged in an automated way. This often requires harmonisation of assumptions with regard to responsibilities, security, financing, etc.
- Legal interoperability: On one hand, the ability of organisations to make agreements about communication and/or exchange of data; on the other hand, facilitating the actual communication and/or exchange of data in accordance with these agreements and general legal frameworks.

The definitions listed above are relatively abstract. The example of the booking site allows us to illustrate the concept of interoperability:

- The booking site's systems must be able to find and access the hotels' systems (technical interoperability).
- The hotels' systems must be able to process the format in which the booking site's request is sent, such as XML (syntactic interoperability).
- There must be a shared definition of concepts such as what 'child-friendly' refers to (semantic interoperability).
- The user's actions on the booking site must be processed in the appropriate database of the hotel being booked (organisational interoperability).
- The booking site and the hotels must have agreements in place regarding how data is handled (e.g., measures associated with privacy protection) and which party is responsible in the event of loss, damage or errors in data processing (legal interoperability).

Considering the technical aspect (the process automation), the following components of horizontal system-to-system integration are important from the supra-organisational perspective:

- Data specifications:
    - The messages (reports) that are exchanged between systems:
        - The different data elements
        - The different types of reports
- Process specifications:
    - Descriptions of how information is handled: the business process requirements of the involved parties often shape the information processing flow and conditions.
- Interface services:
    - Technical services based on an exchange protocol, which handle the dialogue between organisations' systems.

Figure 1.3 illustrates the H2H information chain and the integrated S2S chain, which includes the listed components.

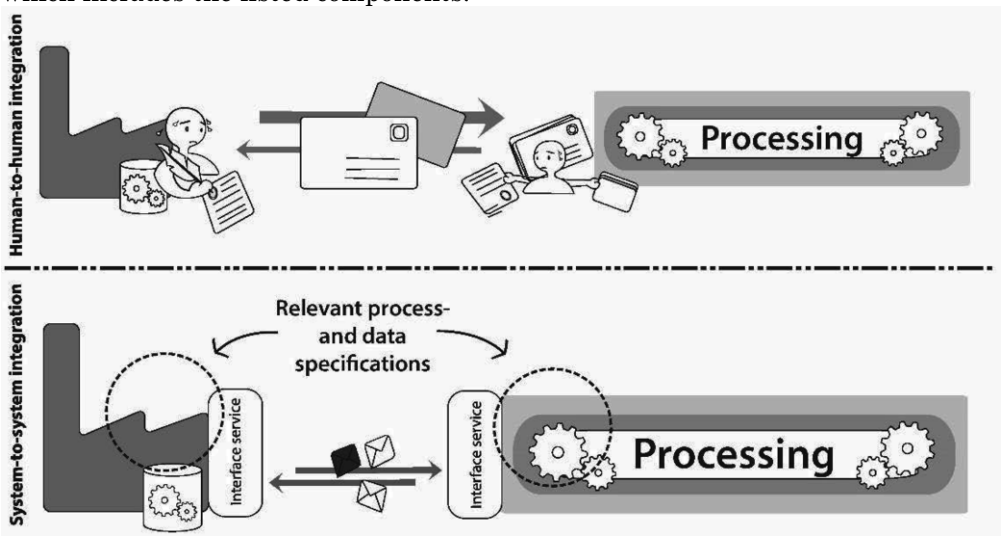


Figure 1.3 – An H2H information chain (top) and a horizontally integrated S2S information chain (bottom), including the data specifications, process specifications and interface service components

The second type of integration – vertical – is derived from the first type: horizontal. Vertical integration involves outsourcing information services to a specialist service provider. The service provider handles various information processes for multiple outsourcing parties. Modularisation of IT components makes it easier to outsource services (Baldwin & Clark, 2000). Each module can be considered as a separate, autonomous functional block that processes specific inputs to give specific outputs (Parnas, 1972). Most information systems nowadays are modular in design and are managed as modules (Reynolds & Stair, 2013).

One special type of outsourcing is the use of a shared service centre (SSC). Also known as a 'shared service provider,' an SSC is a specialist organisation that provides the same services to a number of similar users (Bergeron, 2003). In this text, the term 'outsourcing' refers specifically to the use of an SSC. This type of outsourcing provides advantages in terms of both effectiveness and efficiency.

I. More efficient processing

According to the law of economic specialisation, parties will achieve economies of scale by specialising in certain services. According to the literature, these scale benefits can be attained through specialisation, concentration of specialist knowledge, reuse of standard solutions and large-scale execution of shared processes (Janssen & Wagenaar, 2004). This works as follows:

- Marginal cost - the cost to provide one additional information process for an existing infrastructure - is low.
- Infrastructure and development costs can be split up across a larger group of users.
- Lowering of the above costs reduces the cost to each user.

IT costs can also be lowered by centralising the systems: savings are gained due to less need for local hardware, reduced costs for staffing, training and further development, and reduced management costs (Looijen, 2004). However, while costs savings are one of the most important reasons for organisations to use an SSC, they are by no means the only reason (Buijs, Doorn, & Noordam, 2004). For example, an SSC can bring considerable efficiency benefits for parties preceding the SSC in the chain. In this case, SSC operates as a standardisation platform. With PayPal, for instance, the same front-end can be used – irrespective of the user's bank – to do business with multiple web shops. This is much easier than having separate payment applications for individual banks. Changes within the processing chain are also implemented more easily via an SSC, as the change will only affect a single link in the chain rather than the entire chain.

II. More effective processing

By outsourcing, organisations can make sure that their resources are focused on adding value to their core tasks (Lee, Huyn, Kwok, & Pi, 2003). The efficiency advantage because of the greater scale makes it possible to accumulate more specialisation and invest in more qualified staff. The SSC can invest in highly educated, specialised experts such as legal experts, information security experts and organisational consultants.

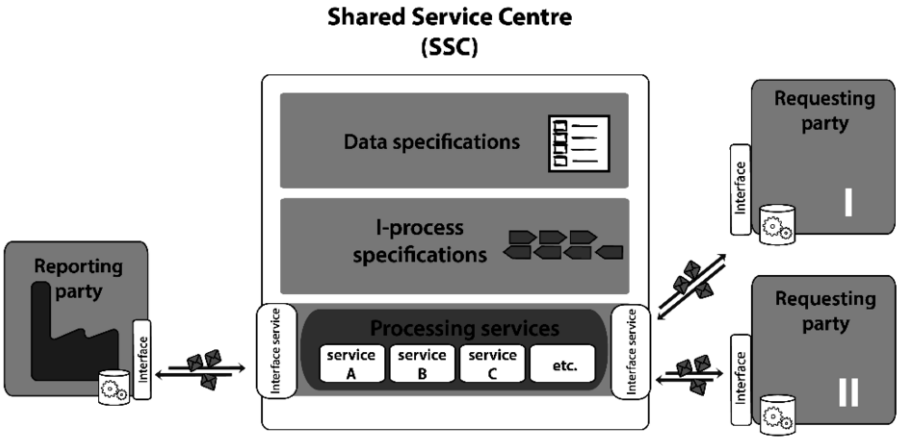


Figure 1.4 – Vertical S2S integration: shared services provided by an SSC

In vertically integrated chains, the SSC's processing services acquire supra-organisational significance. A single processing service must be suitable for multiple organisations in multiple information chains. The more an I-process is reused, the more efficient the SSC becomes. In Figure 1.4, a single reporting party is connected to two comparable requesting parties through services provided by an SSC. The SSC has interface services on both ends: facing the reporting party and facing the two requesting parties.

1.2.3 *Dependency as the price of S2S chain integration*

Both horizontal S2S chain integration and vertical chain integration come with a price. Parties that want to maintain interconnectivity must jointly guarantee interoperability. This creates dependencies. For example, parties can no longer unilaterally implement changes in their data models, as doing so would affect the semantic interoperability. Any modification to any of the shared aspects could affect the other parts of the chain.

Returning to the example of the booking site, let us consider an optional functionality that allows the user to select whether he or she wants carpeting in the hotel room being booked. Implementation of this functionality would require that all connected hotels be aware of this classification and recognise it, and that they be able to provide information about the presence of carpeting in their rooms. This would require harmonisation, and therefore, time and effort. However, parties within the chain often work with different business cases, financing methods and objectives. If the parties fail to reach a single shared solution, they will need to differentiate, which would result in additional costs. New dependencies will also be created in the vertical integration, engendering a mutual dependency between the client and the SSC. The client depends on the services of the contractor (and the quality of those services) in order to meet its objectives. The contractor is provided the required resources (money, approvals, information) from the client. From the client's perspective, it may also want to have a say in how its outsourced processes are performed. Such involvement is associated with

so-called 'agency costs.' To keep agency costs to a minimum, the parties must agree about who will be involved, in what way, and in which decisions (i.e. governance). With efficiency as the objective, the contractor aims to minimise diversification in the services provided and optimise reuse. The same applies to automated services, as an SSC cannot immediately achieve economies of scale for new variants, or may not want to reduce the economies of scale for certain services due to new development costs.

1.2.4 *The business case for S2S chain integration*

The benefits of coupling IT systems between organisations and the use of shared service centres must outweigh the 'price paid' in terms of increased dependency. Information chains have a number of characteristics that are determining factors in the business case for chain integration.

The benefits of horizontal S2S chain integration are best expressed in information chains with following characteristics:

- The chain contains processes by which organisations jointly carry out identical information processes on a periodical basis.
- The volume of information processed in the chain is high (there are many messages).
- The organisations are able to handle the back-office tasks that must be carried out immediately after information comes in using automated software systems.

Switching to an SSC for the handling information processes can be lucrative when the following conditions apply:

- The information processing is comparable between the organisations:
    - In terms of functionality.
    - In terms of knowledge content.
    - In terms of the applicable formal (legal) frameworks.
- The organisations are present in multiple reporting chains. The SSC acts as a standardisation platform.
- It is possible to unbundle the outsourced processes from the company's core processes. The outsourcing organisation is able to provide a clear description of the process (existing or required) to be handled by the SSC (based on Buijs, 2004).

1.3 S2S integration for digital business reporting

Business reporting chains consist of inter-organisational information flows that have been set up to generate and process business information. Business reports in this sense comprise information meant for a third party, regarding the performance of an organisation or the situation within an organisation. This book focuses primarily on reporting chains that are used to comply with legislative and regulatory requirements. The private and public parties within such chains are obliged to submit business reports, including financial statements and various

forms of tax statements, to various government agencies. The government agencies request such information for policy-making and legislation, and policy implementation, monitoring and enforcement. In addition, most modern societies have agencies that require organisations to disclose meaningful financial and other information to the public, with the aim of protecting investors, maintaining orderly and efficient markets, and facilitating capital growth.

The need for such business reports derives from the government's need for information to complete its role in controlling finance, taxes, safety, social security, the environment, healthcare, education and working conditions (Nijsen, 2003). To monitor and enforce compliance with the government's policies, businesses and other organisations are required to inform the government about their performance and internal/external situation. It has been argued that this requirement is for the sake of the public interest (Rutgers, 2011),.

The following are examples of what business reports may contain and for what purposes (based on Nijsen, 2003 and Rutgers, 2011):

- Information about the performance of public and semi-public organisations that are charged, for instance, with the execution of care, education and housing.
- Information about financial monitoring of private organisations.
- Information about personal revenues, turnover, profits and deliveries by companies. This information ensures that parties are making contributions to the public treasury, and that their primary income is distributed/redistributed.
- Statistical information at the macro level as input for policy and legislative decisions. It can include annual statistics, production statistics, investment data and turnover statistics.
- Public financial data for businesses. This information is published for commercial sectors to protect the general public against 'the market' and to ensure the legality of market activities.

Several governmental agencies are required by law to request and process business reports. In this book, the term 'requesting party' is sometimes used to refer to these agencies. When setting up the reporting chain, each requesting party should comply with the Dutch Online Administrative Business Act and should carry out the required processes, including authentication, checking the authorisation of the sending party, or checks for completeness. This information processing is often computerised.

Business reporting applies to a large number of businesses that are obliged to provide insights regarding their performance and level of compliance with established norms. Reporting is done periodically. Generally, organisations that are obliged to report must send information to multiple requesting parties. This information often comes directly from their computerised business administration or is derived from it. The reporting parties often use the similar financial service providers (e.g., tax consultants, accountants) for different chains. The business

reporting domain scores well on the criteria that determine the business case for S2S chain integration. Summarised, the following applies:

1. Requesting parties typically request the same information but for different periods.
2. The processing volume of many reporting chains is large because of the large number of parties with reporting obligations.
3. Both reporting parties and requesting parties often use IT systems to process business reports.
4. The requesting parties make use of the same legal frameworks for administrative communication, carry out comparable processing and require data on the administrative organisation and internal controls.
5. The same reporting parties (or their service providers) send information to multiple requesting parties and would therefore benefit from a standardised infrastructure.
6. The requirements and associated processes for sending and receiving business reports electronically have been included in the Online Administrative Business Act and thereby determine the setup of the reporting process.

1.4 The envisioned SBR solution

1.4.1 *Creation of a standardised S2S business reporting architecture*

Given the uses described above, it is not surprising that the possibilities for system-to-system chain integration (both horizontal and vertical) between reporting and requesting parties have been under exploration since the start of the millennium. At that time, a great deal of political attention was being given to the burden associated with business reporting to the administrative authorities.

Using the BAPI specifications and facilities, the Tax and Customs Administration already required horizontal coupling of automated information systems. In addition, the Dutch Government was striving for greater efficiency through the deployment of generic ICT applications. Having generic components of reporting processes with shared service providers – outsourcing them – was expected to increase the efficiency of data collection.

However, the solution had to align with the characteristics of the information chains in the business reporting domain. In 2004 and 2005, projects such as the Netherlands Taxonomy Project (NTP) and the Requirements Elicitation Programme for the generic infrastructure (GEIN) created a standardised architecture for integrated S2S reporting chains.

1.4.2 *Characteristics of business reporting and SBR solution requirements*

The relation between business reporting and legislation
The most important requirements for reporting chains are laid down within legislation and regulations. These acts often prescribe, for instance, which organisations need to submit business reports, the expected contents, structure, format and when they have to be submitted. The may also pose requirements on handling business reports and providing return messages. These kinds of requirements cannot be ignored by the public parties acting as information receivers. Moreover, they constrain the space for redesigning (parts of) the reporting process. Even if the change is only a relatively minor one that will yield a large benefit for one or more chain parties, it may no longer be in line with the reporting requirements. If the law is changed, the reporting chain will also have to be changed. Certain changes – for instance, modifications to what data elements must be disclosed – do occur frequently in the Netherlands.

In some chains, business reports over a specific period (monthly, quarterly, annually) need to be submitted before a fixed date. In other chains, reporting may occur on various moments and may span multiple timeframes. The requesting party may issue a notification prior to the business report's due date, or once the report has been received. The legal entity of the reporting party may also vary. A fiscal entity for example may consist of multiple legal entities. Finally, there are reporting chains that do not use a single information request model. Examples include financial statements, in which the legislation permits the governmental body (requesting party) to request reports that allows it to obtain sufficient insights regarding the reporting party, but there are no requirements with regards to which model is to be used to provide this business insight. These insights can be obtained using different information request models, which may require data elements specific to each sector. All of these characteristics have led to the following requirements for setting up system-to-system integration:

- Various reports (messages) from different chains must be generated, exchanged and checked (validated) in a standardised manner. This requires a standard format for defining and generating report (message) specifications.
- Within the chosen format, report specifications for the reporting chains have to be easily expandable with additional data elements.
- If requesting parties request the same information, they must be able to utilise the same data elements. The selected format for the report specifications must be able to support multiple reports using the same data elements.
- It must be possible to change the report specifications independently of the process specifications.
- The SSC processes must comprise generic information processing services, each of which carry out their own frequently recurring tasks. It must be possible to operate these services separately and to modify them separately.

- The process specifications of the reporting processes (or their relevant components) must be documented in a standard format.
- It must be possible to easily create a new information delivery process.
- The same submission process must be able to support business reporting for various periods at the same time.

Business reporting and administrative law
As stated earlier, electronic reporting to governmental parties in the Netherlands is subject to the Online Administrative Business Act. This act imposes requirements regarding the reliability and confidentiality of the information exchange and provides the grounds upon which the government is allowed to reject a report. The law also states how the government should act in such cases. One feature of the administrative law is that the purpose and nature of the business report determines how conflicting requirements (e.g., ease of use vs. confidentiality) are handled.

The purpose limitation principle is another important principle in administrative law, Based on these and comparable stipulations (e.g., the Personal Data Protection Act and the Public Records Act in the case of the Netherlands), the following requirements can be imposed on a S2S integration solution:

- It must be possible to electronically identify the reporting parties, the service provider, and the requesting parties.
- Parties must be able to safely take part in the business reporting process on behalf of others. This requires the capability to submit authorisation claims (approvals) and verify them.
- Information processing should be accompanied by feedback regarding the intermediate (e.g., report is received) and final results (e.g., the claims in the report are approved).
- Requesting parties must be able to differentiate between various levels of confidentiality if the purpose or nature of the business reporting so requires.
- Parties with reporting obligations must be able to choose for themselves when information is sent as business reports from their administration systems and for what purpose.

The societal function of business reporting
Business reporting has an important societal function, which also applies in the case of reporting as part of agreements based on civil law. Such could be the case when parties must provide business information to banks to obtain credit, or when a company is held accountable to quality mark institutions for its corporate social responsibilities.

In the old paradigm, the business processing capabilities, workflow structure and preferences of the requesting party shape the structure and exchange conditions of business reports. 'Chain reversal' has been the new paradigm from the time government agencies began studying the potential of large-scale S2S inte-

gration in reporting chains. In the chain reversal paradigm, the information already available in the business administration at the side of the reporting party is now the starting point for defining the structure and information exchange conditions. The administration of the business is recognised as the source of information for business reports. This paradigm implies that when requesting parties would like to receive information from the source, it has to be done in as standard a manner as possible. Seen from this perspective, it is logical that the government would use standard methods and technologies for the generic components.

It would be very interesting for the reporting parties if not only the public requesting parties but all stakeholders were to operate using the principle of chain reversal. If private parties were to use the same technological standards as the government, the full breadth of such reporting could be realised more efficiently.

With this vision in mind, it is necessary to publish the standards and their application methods in the reporting chain, enabling private parties to adapt reports to the standards accordingly. Because standardisation is no longer restricted to vertical chain integration – the use of an SSC as a standardisation platform – frameworks for S2S integration within reporting chains must be detailed at a higher level of abstraction. The adoption of such a framework of agreements would be encouraged by the use of generally accepted and familiar standards. The intention to realise S2S integration in a standard way within public and private reporting chains yields the following requirements for the architecture of the solution.

- The components of the solution should preferably be based on generally accepted standards.
- Where necessary, architectures shall be set up to guarantee unambiguous application of the standards in various reporting chains using the SBR framework of agreements.

1.4.3 *Realising SBR chains using generic building blocks*

Considering these and other requirements, an outline of the solution was presented in 2006 as the architecture for standard reporting chains in the public domain. Figure 1.5 presents an outline of the solution and its key building blocks.

The key building blocks in the SBR solution outlined in 2006 are numbered and explained below. Since 2006, certain components of the building blocks were refined, and there have been various additions and refinements within the same architecture. For example, some functionality has been added. However, the essence of the solution has remained largely unchanged. Part B of this book provides a much more detailed description of the building blocks.

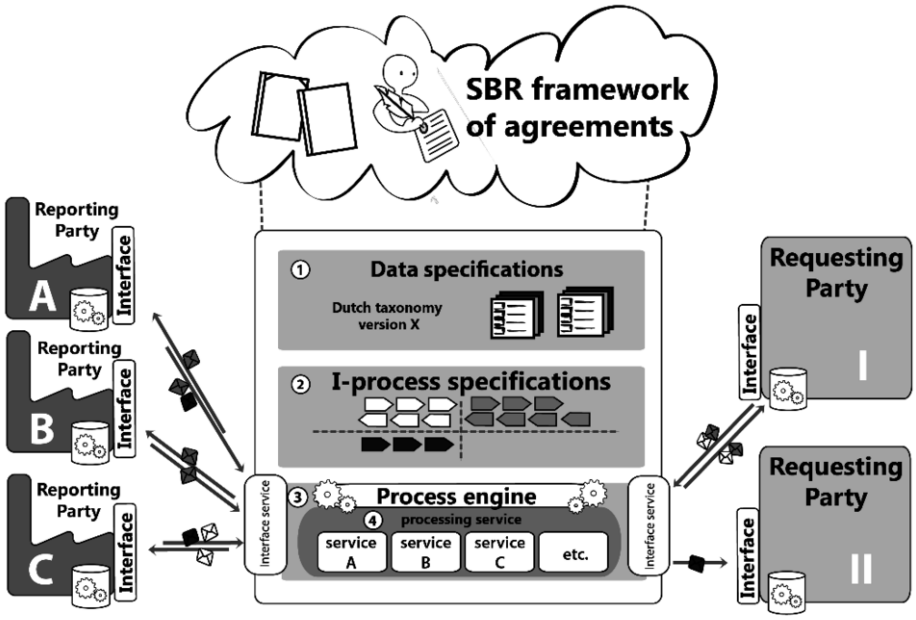


Figure 1.5 – Outline of the SBR solution used by public requesting parties

We proceed with a brief description of the generic building blocks.

1. The Netherlands Taxonomy

Data specifications form the first building block. Every business report starts with the question of what information the requesting party wants to have or provide. The Netherlands Taxonomy (NT) is a computer-readable description of the information that the requesting party wishes to receive from, or provide to, a reporting organisation for processing. The SBR solution uses eXtensible Business Reporting Language (XBRL) to define this structure. XBRL is an internationally accepted standard for the structure and use of taxonomies for reporting. Defining the data specifications ensures that the interpretation of data will be determined unambiguously and independently of the system. The first version of the shared taxonomy was delivered by the NTP (Netherlands Taxonomy Project). The taxonomy is loosely coupled to the technical infrastructure.

2. I-process specifications for reporting processes (in BPMN)

I-process specifications form the second building block. Aside from the need to define the data sent by a reporting party an integrated S2S chain requires clearly defined specifications for handling this data. The process specifications prescribe how the requesting party wants data – that has been or shall be submitted by the reporting party – to be handled. More specifically, process specifications prescribe the (automated) actions (e.g. authentication, validation) performed in the information chain from sender to receiver. Certain processing aspects are more relevant than others and require detailed specifications. Actions that are performed by the SSC are always relevant, because both the reporting party and

the requesting party are connected directly to it. In addition, the accomplishment of these actions by the SSC is seen as the service provided to the requesting party. Processes carried out by the SSC are always described using the open standard, Business Process Modelling Notation (BPMN). There are two reasons for this. Firstly, it is easier for parties to understand and compare processes if a single, uniform language is used. Secondly, BPMN enforces a certain degree of consistency, which allows it to be easily converted into code (including the open standard BPEL). This technical code can be implemented by the SSC directly in the so-called generic infrastructure. The SSC handles the actions automatically. In this book, we generally refer to actions carried out by the SSC within the chain as an 'I-process', which is short for an information process. Typical information processes include receiving, transferring and validating data. In order to understand and build information systems, the information processes must be understood i.e. modelled in a unequivocal manner.

3. Interface services

Interface services are the technical applications that can accept messages (e.g., business reports and notifications) from outside the SSC or deliver messages to another interface service. Messages can include content (i.e. a business report) or contain processing status information (e.g., the message has been received successfully and is accepted for further processing). The description of how an interface service operates is part of the I-process specification. The chosen technical exchange protocol (the technical envelope that the message is embedded in) is the Simple Object Access Protocol (SOAP). Because the interface services are accessible to the outside world, they contain the main access security checks. A standard security protocol for system-to-system traffic was chosen as part of the proposed solution. A bidirectional secure connection based on an X.509 certificate is set up between an external party and the SSC. The same type of certificate must also be used to supplement the message with an digital signature – the digital equivalent of a handwritten signature or a stamped seal – solving the problem of tampering and impersonation in digital communications. The solution also provides the possibility for using a person-bound qualified digital signature. Digital signatures provide the added assurances of evidence to origin of an business report, as well as acknowledging informed consent by the signer. We can distinguish three types of interfaces from the perspective of the SSC: (1) message delivery interfaces; (2) message retrieval interfaces; and (3) status information interfaces. Status information interfaces provide information on what has happened to a sent message, or what is being done with a request.

4. Processing services

Processing services are the various applications that realise automated handling of the I-processes. An interface service 'picks up' a message from a reporting party and the process engine then uses the process specifications for that specific type of message to determine and orchestrate which processing services will handle the message and in what sequence this should be done. The key processing services for a generic solution are the following:

- Authentication service: Checks the integrity of the message and validates the certificate against a blacklist to confirm that the certificate has not been withdrawn.
- Authorisation service: Uses a trusted approvals (permissions) registry to confirm whether a reporting party is authorised to send or request a certain message on behalf of a represented party.
- Validation service: Using the NT specifications, this service can examine any submitted business report and establish whether it complies with the requirements imposed on it by the NT.

Due to loose coupling, the previously listed building blocks operate independently from each other and can be modified independently as well.

5. SBR framework of agreements

The final building block of the solution is the SBR framework of agreements. This framework encompasses agreements that describe which standards must be used when setting up an SBR reporting chain. The underlying premise is that SBR can be used in other domains using the same standards. A distinction must be made between specifications for SBR reporting and non-specific specifications. The latter are standards that are also used outside the solution outlined in figure 1.5, such as BPMN and XBRL. The Netherlands Taxonomy Architecture, an architecture for I-processes (based on GEIN), and Technical Architecture, have been part of the framework since the solution was first outlined.

1.4.4 *Benefits than can be anticipated in SBR chains*

Chains that employ a configuration of the building blocks are called SBR chains. It's difficult to list the exact benefits to be gained by businesses, intermediaries, software providers and requesting parties in a SBR chain. The reason for this is that the actual benefits will vary as a result of several factors, such as the type of business reports, the requirements imposed by legislation, the employment of intermediaries versus self-filing and the maturity of the software used for preparing and filing business reports. Moreover, benefits such as efficiency and security can be derived from the end-to-end- exchange and processing of information. Some actor groups may feel that they are the ones that invest while the actual benefits are reaped by the actors at the end of the chain. The benefits for the entire chain taken as a whole may not feel like a benefit for a single actor group. For instance, SBR requires businesses to buy a digital certificate. The use of certificates combined with other security measures enables a high level of end-to-end security, but it's the businesses who have to purchase it. Regardless of the fact that alternatives also have a cost, businesses may still feel that the benefits are not equally distributed throughout the chain. Having placed this disclaimer, the implementation of SBR in the Dutch context allows us to specify some benefits that can be expected in a 'typical' chain that uses the SBR components. Table 1.1 provides an overview of anticipated benefits.

Table 1.1 – Benefits that can be anticipated when using the SBR solution

	Actors				More details in chapter
Anticipated benefits	Businesses	Intermediaries	Software providers	Requesting parties	
The elimination of paper as exchange format, enabling organisations to reap the benefits of the use of structured digital data (better quality, lower costs, more timely)	x	x	x	x	5
Reduction of manual activities (e.g., re-keying data between different systems and portals, interpreting agency specific terms on forms to understand what is required, mapping to concepts and definitions).	x	x		x	5 & 6
Accelerating the process of compiling business reports by businesses or intermediaries, lowering the cost of preparation and filing.	x	x			5
Efficiency: store once, report many times (to various requesting parties).	x	x			7
Improving the quality of business reports: less prone to errors, early error detection through automated validation.	x	x	x	x	5 & 6
Assuring the receipt and processing status of the business reports in a standardised way.	x	x	x	x	7
Continuous compliance: the taxonomy is always actual as far as changes to current legislation are concerned. Using the taxonomy also lowers the cost of compliance.	x	x		x	5
The processing services of the SSC are always compliant with the latest laws and regulations, therefore the requesting parties also comply, at least for the outsourced information processes.				x	9
De-compartmentalisation of the software market: lowering entry barriers for software vendors in reporting chains, leading to an increase of service providers. This should lead to innovation, higher service quality and lower cost.	x	x	x		2
The use of a generic infrastructure operated by a SSC allows for the development and maintenance of generic services at lower cost (thanks to economies of scale).				x	9
Uniformity: it is clear where to find the specifications for information exchange with government agencies (at the SSC) and to which address messages need to be send (generic infrastructure end-point).	x	x	x	x	9
Redesigning the back-office of governmental agencies leading to more efficient and effective government.	x	x	x	x	6
Piggybacking on high service requirements and high quality standards. When a service and the underlying infrastructure is approved and used by the Tax and Customs administration, you can assume it is of high quality.	x	x	x	x	6

Since some of the listed benefits require a more detailed description of a component or interaction, the table includes a column with references to more details regarding the mentioned benefit.

1.5 Implementing the solution in a pluriform domain

1.5.1 *A transition with an enormous scope*

The solution outlined above provided enough motivation for the boards and directors of large organisations to sign a covenant in 2006. It seemed that everyone could see the potential of the solution. As stated earlier, the parties to the covenant agreed that everyone would make an effort to implement their own share of the solution. For the chosen scope – business reporting for the areas covered by the Tax and Customs Administration, Statistics Netherlands and Chamber of Commerce – the domain affected by the transition consisted of roughly

- 12,000 tax specialist
- 2,000 accountants
- 500 commercial software providers (software that can used to prepare and file business reports)
- 1,300,000 companies
- 3 requesting parties (Tax and Customs Administration, Statistics Netherlands, Chamber of Commerce)
- 6 reporting chains
- NTP project and Logius (at that time, GBO.Overheid)

The covenant thus affected a huge playing field, with various parties all faced with the technical implementation of the SBR components in their operations. The technical implementation implied a transition from a heterogonous state to an S2S integrated chain. An outline of that technical implementation is provided in Figure 1.6 and explained in the subsequent text.

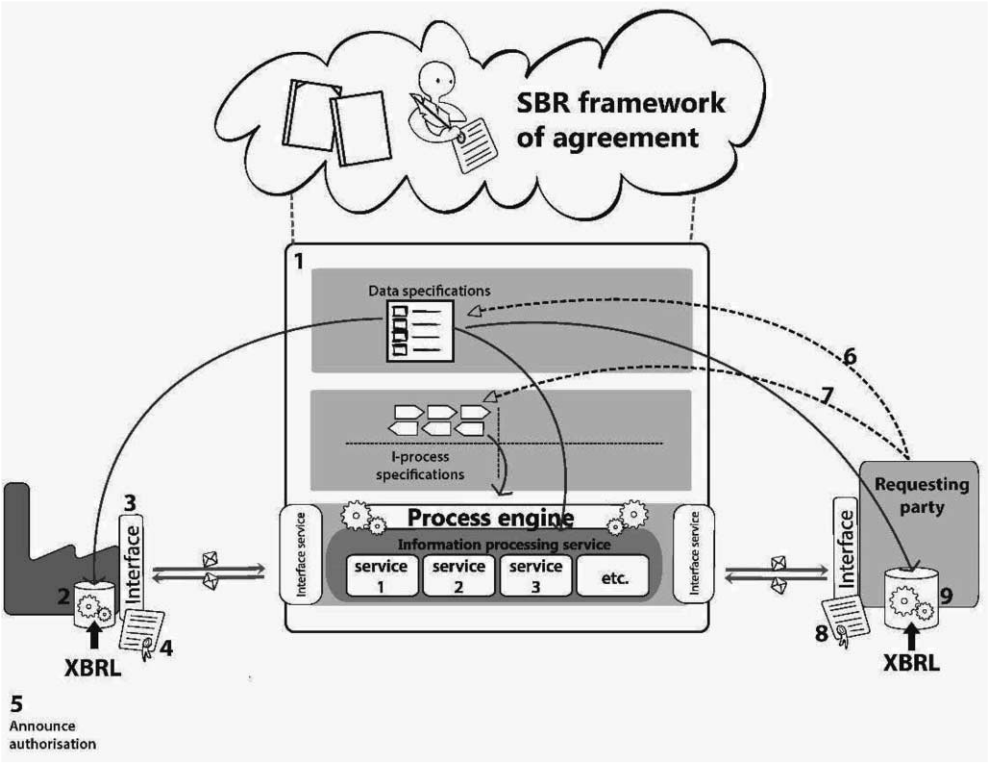


Figure 1.6 – The technical implementation of SBR in an information chain: 9 changes to be realised by the various parties involved.

1. In order to facilitate the transition to S2S information exchange and processing, a 'generic' platform needed to be realised. The adverb generic implies that the platform should be able to service multiple information chains. The term platform refers to services and a generic infrastructure. Services include both organisational services (e.g., helpdesk support, training sessions for software providers) and technical services (i.e. interface services and information processing services). Generic infrastructure components include interface specifications, I-process specifications and (meta)data specifications. The SSC needed to develop the initial versions of the generic infrastructure components. In the Netherlands, the combination of the generic process infrastructure and associated technical services is known as 'Digipoort'.

The following matters also must be settled for an SBR reporting chain to be operational:

2. The software used by the reporting parties must be able to 'read' an XBRL taxonomy. Users must be able to map items from their own databases onto the elements of the taxonomy. The software must be able to generate a message based on the NT.

3. The software used by the reporting parties must implement an interface service to make sure that the software can correctly deliver messages to the SSC (i.e. in the correct digital envelope).
4. The reporting parties must have a certificate that will allow the SSC to establish the authenticity of the messages.
5. When a reporting chain requires authorisation checks, the reporting party must have submitted such an authorisation to a third party designated for that purpose.[4]
6. The requesting party should make sure that the message specifications are available in XBRL.
7. The requesting party must draw up the specifications for the I-processes in BPMN.
8. The requesting party must have a certificate so that the SSC can establish the authenticity of the message traffic.
9. The software used by the requesting party must be able to 'read' an XBRL taxonomy. The requesting party must be able map items from its own databases onto the elements of the taxonomy. The software must be able to process an XBRL message that has been drawn up using the NT.

In sum, implementing SBR for the first time requires significant effort from the various parties involved. However, once a party is connected to SBR, it takes far less effort to set up another SBR chain. When a software provider has implemented an interface, for example, that interface can exchange all types of business reports with the generic infrastructure. Any party that wants to send information to the generic infrastructure only needs to obtain a certificate once. In setting up SBR, a distinction should be made between (1) the realisation of the SBR factory (the SSC platform), (2) connection of the reporting and requesting parties and (3) the implementation of a new SBR reporting chain.

Regarding the first aspect, the SSC platform services are currently up and running. Considering the second aspect, some information chains have yet to start using SBR, but this is the case for a steadily decreasing number of chain parties. The reason for this is that almost every organisation has to provide business information to the tax office. Once these organisations already have the means (directly or via intermediary) to report business information for a specific information flow (e.g. VAT and corporate income tax), more information flows (also to other requesting parties) can be supported by the same installed base. Implementing new SBR reporting chains is therefore becoming less and less complex. In 2006, all three aspects needed to be created for the first time and this had to be done coherently. Thus, the launch of SBR required stricter coordination and management than was initially expected.

[4] This component has been changed in the current solution, bringing it more in line with the generic architecture. Please refer to the text boxes provided in this chapter.

1.5.2 *Implementation in a deadlock*

Because of the lack of unambiguous SBR governance during initial implementation, the parties were left with various questions that were difficult to answer:

- How serious is SBR? How important is it to start investing in it now?
- Who can I contact if I have any questions about the connection and who determines what kind of connection support is necessary?
- How can I exert influence on the way SBR is implemented?

The 2006 covenant assumed a broad and voluntary rollout of the solution within an enormously multi-faceted domain. However, the realisation of functional SBR chains based on a paper agreement turned out to be too big a challenge. By the end of 2009, various leading parties had started implementing small pieces of the chain, but no large-scale SBR chains were yet operational. The sceptics who had said that SBR would not get off the ground were proven right for the time being, and they recommended to their bosses and other parties that SBR was not a good investment. SBR was deadlocked.

The need for acceptance of the governance system: a practical illustration
For the implementation of SBR in an information chain to be successful, achieving support for the governance is essential. The initially outlined SBR solution required that parties (such as fiscal intermediaries) provide proof to a private authorisation service provider that they had a mandate to act on their clients' behalf. Because the term 'authorisation' can refer to both the process and the outcome, we'll call the proof an approval. Although it is an attractive idea from the point of view of administrative law to have such approvals checked automatically, the way it had been designed in the solution was a major obstacle to implementation. Firstly, the marketplace for authorisation services was by no means mature. This meant that the process of providing notifications or announcing approvals was complicated. Secondly, there was much discussion regarding the need for formal notification of approvals for sending in messages. Why would anybody want to send messages on behalf of anyone else without being asked? Thirdly, reporting parties were expected to pay for the services provided by the authorisation service provider. This was perceived as an extra burden. Finally, intermediaries did not like the idea of making their relationships with their customers known to third parties. It became clear that this part of the solution would have to be modified in order to remove it as an obstacle to implementation. But who was to decide whether this was possible? Who was responsible for coming up with an alternative solution? Who was to decide whether the new solution was sufficient and what the scope of that solution should be? Up until the end of 2009, unstructured discussions took place with some of the SBR pioneers regarding this problem, but there were no formal structures to resolve this issue. Intervention in the SBR Programme changed this. We will return to this story in the next box.

1.5.3 *Governance for controlling the implementation*

To move forward the implementation of SBR, three interventions were broadly carried out to end the SBR deadlock:

1. A governmental manager was appointed. The Ministry of Economic Affairs and the requesting parties became involved in controlling the implementation at a high administrative level. This intervention showed

the government's view of SBR as a serious development, and it became clear to the critics that SBR might be here to stay. This led to increased willingness of critics' to take part in harmonisation forums.
2. A number of forums were set up in which structured decision-making about various components of the implementation and further development of SBR could take place.
3. A programme team of experts was set up at Logius with instructions to actively facilitate governance with regards to the content related aspects of SBR and to help implement SBR in the various reporting chains.

Although the above-mentioned intervention focused on the control and coordination of the SBR implementation programme, more and more of the parties involved became convinced of the following: in addition to the new technology, the SBR solution that was to be implemented included a very large organisational component. Changes would be required even after the initial implementation of SBR. Thus, it needed to be possible for new reporting chains to easily take part in the SBR governance. An operating governance structure would therefore be required to safeguard permanent coordination of the S2S integration, even after implementation was completed. A clear outline on how to achieve such adaptive governance had not yet been created in 2006, thus requiring some catching up to be done. It also became clear to policy-makers and the parties receiving Logius's services that the role of SSC would be much bigger than merely providing the functionalities of the standard reporting. Content-related and process-related facilitation of governance would become one of its core tasks. Thus, it needed to become clear how Logius could realise these core tasks and what competences were required. However, in order to do so, first the SBR solution needed to be worked out in more detail.

How an accepted governance system can remove an obstacle
Harmonisation in the new, properly supported forums allowed the SBR Programme create a new proposal for resolving the authorisation services issue. The obstacle impeding implementation was eliminated in the following manner. Certainty about authentication was reinforced. Henceforth, PKI-government certificates would be used. PKI-government thus became an element of the SBR framework of agreements. Each reporting chain could determine whether it needed to enable, disable or optionally employ an authorisation service. Expectedly, the providers that were ready to deliver authorisation services were not happy with this choice, but they also understood that they would earn nothing for their services if SBR never got off the ground. Making authorisation services optional meant that those fiscal intermediaries that were already set up to use an authorisation service would not have to make further modifications to their processes. In the meantime, a facility was created to retrieve return messages from government agencies, thereby allowing the announcement of approvals directly from the intermediaries' reporting software. This was done using the generic infrastructure (see Chapter 7).

1.5.4 *Governance and management as neglected components of the SBR solution*

In 2006, it was determined that Logius (GBO.Overheid at the time) would be charged, as an SSC, with the management of the Netherlands Taxonomy and the generic infrastructure (I-processes, interface services and processing services). However, what was not defined was the question of how the parties would relate to one another in the event of changes. Neither was there an exact picture of how the various parties involved would be connected with each other due to SBR, and how the new dependencies would relate to the existing situation.

1. Horizontal harmonisation of each reporting chain
Firstly, using an SBR solution in a reporting chain (e.g., for corporate income tax) requires harmonisation in terms of implementation, maintenance and further development. The existing situation is different for each reporting chain. In 2006, tax chains in the Netherlands already used a form of S2S integration using the BAPI standard. The information chain of the Chamber of Commerce was still largely paper-based and e-mail was used to send information in digitally. A human-to-system interface was still the dominant modality for submitting statistics reports. Moreover, different principles were being applied within the chains. Apart from businesses with reporting obligations, fiscal service providers and software providers also have a role in the reporting chain and need to be aware of the different principles applied. The circle in Figure 1.7 positions these actors.

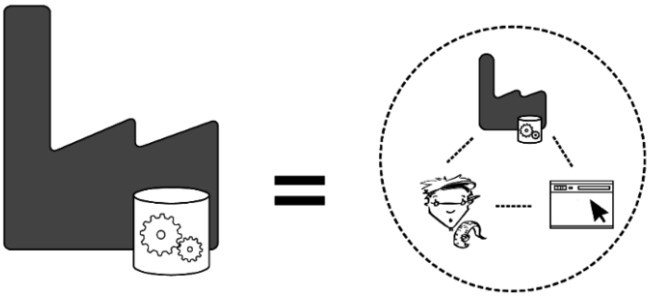


Figure 1.7 – Usually, the business with reporting obligations is supported by parties such as fiscal service providers and software providers

A reporting party can be anything from an independent freelance journalist to a multinational enterprise. A fiscal service provider can be a local accountant, or one of the Big Five companies. Therefore, differences in investment capacity and levels of ICT maturity among the parties is expected.

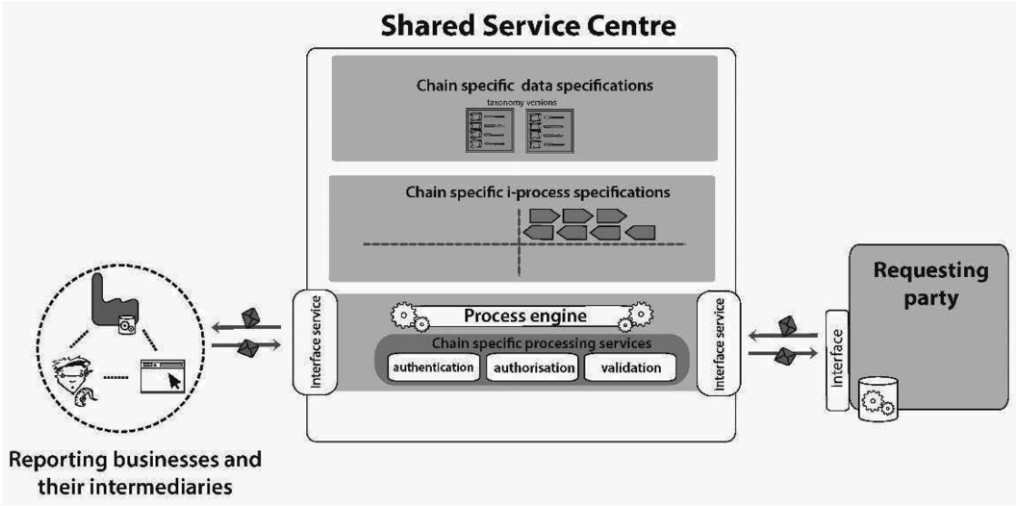


Figure 1.8 – Horizontal harmonisation: the requesting party steers the chain setup and further alignment

When it comes to horizontal harmonisation, the requesting parties are in the lead. They determine how the harmonisation should take place. As a SSC, Logius provides connection support for SBR, even though the commissioning requesting party determines how and when it wishes to utilise this service for its chain. This approach to control is shown in figure 1.8.

2. Vertical harmonisation with the SSC

Vertical chain integration also requires a specific form of harmonisation. As the common receiving parties of Logius, the requesting parties (such as the Chamber of Commerce, the Tax and Customs Administration and Statistics Netherlands) must deal with a SSC. The way that this SSC operates, how it provides its services and how the services develop further all need to be coordinated. Figure 1.9 illustrates this form of vertical harmonisation.

When an SBR domain is under development, it is only natural that the policy-making agencies (the commissioning parties) should also be involved in vertical harmonisation.

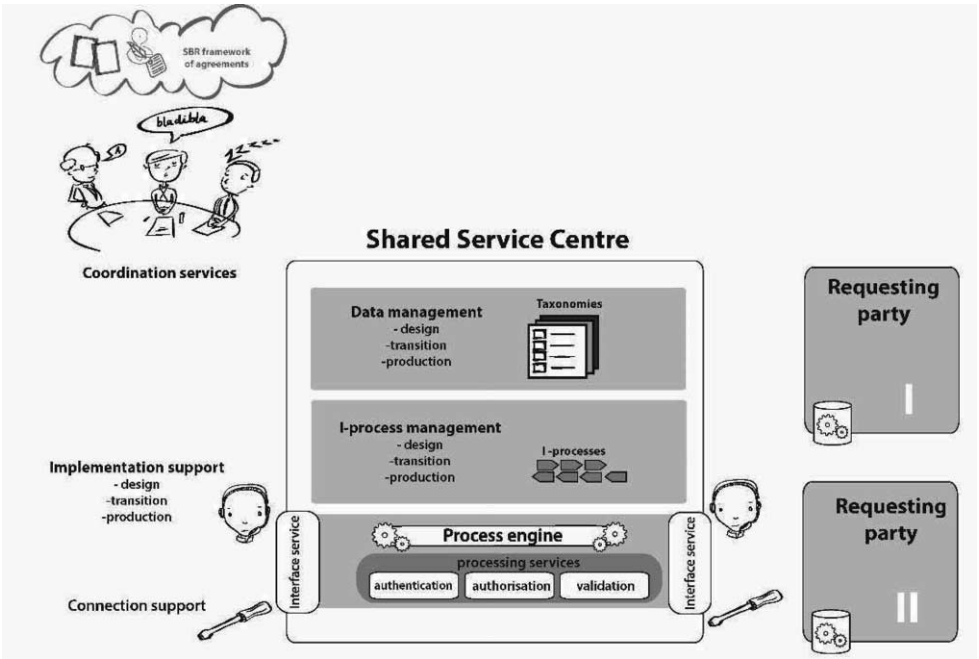


Figure 1.9 – Vertical harmonisation: harmonisation of the service delivery by the SSC with the requesting parties

3. Harmonisation of the framework of agreements at the network level

Finally, the framework of agreements must also be applicable to other B2B reporting chains. To encourage compliance to the SBR framework of agreements, it is important that the framework is aligned with the practice and needs of the private reporting chains. Harmonisation at network level is thus required. Figure 1.10 illustrates the components that require harmonisation at the network level.

4. The organisational challenge

Because of the chain integration associated with SBR, creating these forms of harmonisation and maintaining them remains necessary. This organisational component is therefore an important part of the SBR solution. The fact that the forms of mutual integration are highly coherent can be seen from the example in the following text box. The central position of the SSC (in this case, Logius) actually makes it the only party with the ability to facilitate and coordinate the harmonisation of content. Of course, this is done on the instructions of the receiving parties (administrative authorities) and policy-making government agencies.

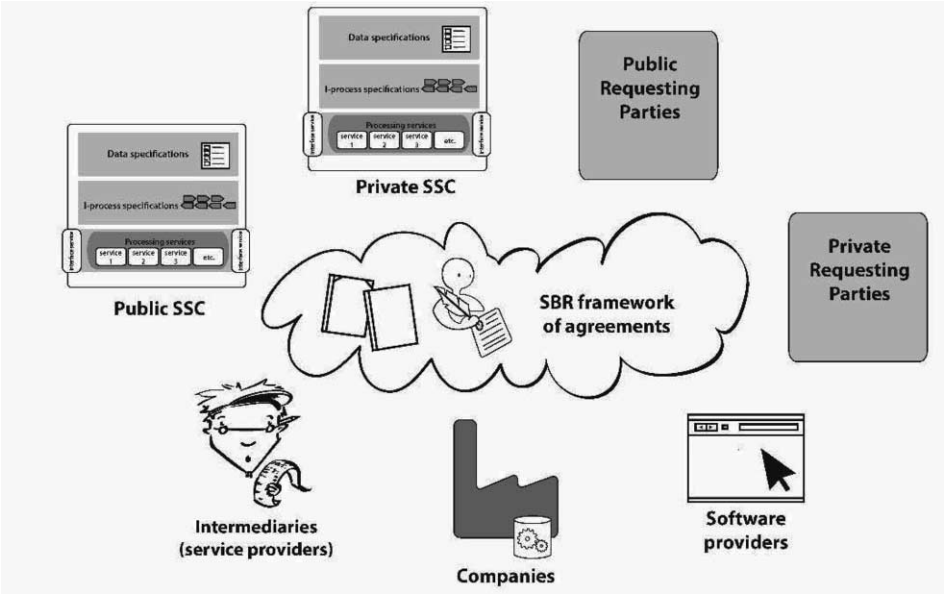


Figure 1.10 – Harmonisation at the network level: harmonisation between private and public parties regarding the scope of the SBR framework of agreements

Coherence of integration forms

The following example is a step-by-step illustration of the coherence between the various forms of integration.

i. Dissatisfaction with one requesting party in a reporting chain regarding its performance in processing complex messages demands a different process setup. This presents a problem for the horizontal integration.

ii. The change requires modifying the message specifications/syntax, or the dimensional setup of the messages. The change must therefore be supported by the architecture of the Netherlands Taxonomy.

iii. The requisite setup of messages does not fit in with the agreements, so the agreements must be changed. The parties decide to stick with the standardisation requirement, as they expect that increased messaging in the future will drive the switch to a dimensional taxonomy. They therefore want to create an architecture for the taxonomy that enforces use of the dimensional form. The cooperative agreement must be adjusted to suit this change.

iv. As a consequence, the message specifications of the other parties must also be set up in accordance with the dimensional architecture from now on. This change is now affecting all horizontally integrated reporting chains.

v. The situation also requires technical changes in the generation and validation of messages by all requesting parties.

vi. The requesting parties that had no problems with processing may now have to change their processing system after all.

As the SSC, Logius must modify its taxonomy development service in order to accommodate the new architecture. Costs will be incurred to do this. Because of their vertical integration, Logius's receiving parties must try to reach an agreement about who will be responsible for these costs. Should the financial burden be on the requesting party that wanted to switch to the dimensional taxonomy, or on all requesting parties?

In the course of the SBR implementation, it turned out that Logius needed to play a more significant and more complex role in terms of content than had originally been expected. In addition to maintaining the exchange of messages, managing the common SBR components requires orchestrating the developments at various levels of integration. In retrospect, we can say that the SBR challenge was amplified because actors underestimated the importance of designing a proper chain governance and coordinating its implementation.

1.6 Readers' guide

This book is divided into two parts: Part A and Part B. In the following summaries, we will briefly explain the essence of the chapters of both parts.

1.6.1 *Part A – SBR as a challenge for information chains*

Chapter 2 – Information chains
This chapter focuses on the central object of this book: the information chain. A chain is a powerful metaphor that underlines the interdependencies between organisations and systems. Drawing on the available literature, this chapter starts by decomposing the concept of a chain. Depending on the so-called flow element – the transaction between organisations – various types of chains exist in practice. Examples include production chains and information chains. Next, this chapter examines the various drivers that lead to the creation of a chain. In business-to-business chains, the ability to generate value is often the main driver for the formation of inter-organisational linkages. In business-to-government chains, legalisation is usually the main driver. Government agencies request information from businesses primarily based on legislation. For the requesting parties, legislation can be both empowering and constraining. Having discussed some drivers, the chapter then focuses on the general characteristics of chains, particularly information chains. Here, we deal with the soft yet crucial elements such as trust and power. Finally, the chain metaphor is explained in detail by decomposing a typical SBR chain.

Chapter 3 – Change management in information chains
This chapter was written from a change management perspective. The perspective could be that of a person – a change manager – or a change organisation (a programme or a department) that several people are involved in. What change management challenges are faced when redeveloping information chains? The chapter describes the intrinsic resistance of information chains and gives an extensive description of the strategic behaviours that can occur within chains. The SBR case is used to illustrate the shape this behaviour has taken in practice, what consequences it has had and what measures have been enacted to deal with the behaviour. One of the core questions that this chapter deals with is the nature of the change methods available for modifying information chains. This issue is addressed from four perspectives, namely (1) direct change management, (2) process management, (3) changing the chain conditions and (4) dilemma management. Depending on the situation, change managers can adopt what they see

as the most appealing perspective; hybrid forms (sequential or for certain components) are also a possibility. The SBR case is used once again to illustrate the theory in detail based on practical experience.

Chapter 4 – Steering change in chain information systems
Drawing on the concepts and insights provided in the previous chapters, Chapter 4 addresses the change steering question: how should a specific type of change be steered (referring to which change strategy and steering instruments to use) and by who (which change agents)? Finding accurate answers to the steering question was a substantial challenge during the launch of SBR in the Netherlands. Studies have shown that this question is also relevant for other types of information chains, yet that there is a dearth of available guidance for addressing this problem (e.g., Tiwana et al. 2010, Markus & Bui, 2012). The main issues include the diverse range of possible changes that can occur within chain information systems and the complexity of accurately identifying the specific change object and the required steering instrument. Popular steering instruments include programmes, projects and procedures. However, incorrect calculation of the necessary steering instrument leads to resistance, stagnation, higher costs and even failure. Often, the market's enthusiasm for selling technology encourages miscalculation. How many times have we read recommendations for technologies that are 'plug & play' or can be applied 'with one flick of a switch,' only for the technology to turn out less mature than we had been led to believe? The urge of managers and policy-makers to realise technological innovations within a short timeframe also plays a role, of course. The objective of chapter 4 is to offer readers a guide for addressing the question of who and how to steer change. To do this, we first consider the available research on steering change in multi-actor environments. This will allow us to define the concepts and relationships involved. Painting this background with the challenges faced during the launch of SBR, we deduce some guidelines for addressing the change steering question.

1.6.2 *Part B – SBR as a solution for information chains*

Chapter 5 – Managing data in information chains
This chapter zooms in on the main object in information chains: information itself. Information can be defined and structured in many ways. However, this can complicate the efficient and automated processing of information. This chapter looks into the challenges and solutions for managing data in information chains. In the SBR context, the challenge was to safeguard that various parties can directly utilise financial and non-financial data from their bookkeeping software for internal and external reporting. For this purpose, the actors chose to employ XBRL. XBRL is a standard for recording business data and presenting it to various parties in a uniform manner. Because the syntax – the way that something is written down – is standardised, anyone receiving the data can indicate what data classification (definition) is relevant to them, using their own semantics (meanings). Within the SBR context, the requesting parties use a shared taxonomy: the Netherlands Taxonomy (NT). This allows a business to generate reports quickly and easily from its own administrative systems in accordance with the

definitions and information requirements of the Tax and Customs Administration or any other requesting party. This standardisation of syntax and semantics makes it easy to collect, process and exchange data, which results in considerable cost savings. Such saving applies both to those who are sending the information, as the various business reports that need to be completed and sent independently from one another are no longer required, and those who receive this information. This chapter also describes the other concepts that are important for the data exchange, such as normalisation, harmonisation, data quality, taxonomy design and data management. The SBR case is used to add detail to these concepts and to clarify their relationships for the reader. Finally, relevant developments in the field are presented and reflected upon.

Chapter 6 – I-processes
Actors perform processes in order to achieve their goals. Process-oriented thinking is widely encouraged, but what constitutes a good process? How can we model processes unequivocally? What are the specific requirements imposed on processes in SBR chains? This chapter covers some basic concepts and methods that allow for the proper conceptualisation of processes when reengineering information chains. We start with the general characteristics of processes, followed by an elaboration of what constitutes a good process. Next, we discuss some popular process management/improvement philosophies. The SBR case is used to illustrate how these general philosophies can be converted into specific and structured process implementations. When doing so, special attention is paid to information processes (I-processes). The subject of these I-processes is the XBRL instance (an XBRL based business report) which can be handled automatically. This chapter also provides some guidelines on modelling I-processes using the Business Process Management Notation. The chapter concludes with some specific requirements imposed on I-processes in SBR chains.

Chapter 7 – Technical foundations of SBR
The SSC provides a generic platform – including services and an generic infrastructure – for multiple information chains. Chapter 7 focuses on the generic infrastructure components. From a conceptual perspective, the generic infrastructure stands between the sending party and the requesting party. The information infrastructure facilitates the automated handling of messages based on standards for data models, process standards and technical standards. Note that the term 'messages' refers not only to business reports, but also to technical or status notifications. The chapter consists of three parts. The first part focuses on the typical B2G interactions and the question of what technical infrastructure setup is suitable for SBR. The second part focuses primarily on relevant technical standards for the exchange of messages. In particular, we describe developments regarding interfaces, web services and service-oriented architecture for the flexible support of I-processes, which as we know are described using BPMN. The third part of this chapter presents the architecture of the information infrastructure and describes how it works. Specific attention is paid to the interfaces, processes and web services it uses. The chapter concludes with a reflection on the challenges that have been resolved thus far.

Chapter 8 – Information chain security
Business reporting using SBR involves the automated exchange and processing of confidential information. The law imposes several requirements when it comes to information exchange with government agencies and even prescribes how this information should be processed. Such requirements include information availability, integrity, authenticity, confidentiality, transparency and non-repudiation. Moreover, the legislation also points to some possible measures that can be taken in order to satisfy such requirements. Measures include user identification, authentication (verifying the claimed identity) and authorisation (verifying access/processing rights) by means of digital certificates and encryption. Led by the SSC, partners in SBR have taken several steps to strengthen information security and continue to collaborate on future measures. Chapter 8 does not cover all the measures, but focuses on specific risks, legal requirements and measures that are currently common in SBR chains. The chapter is divided in three parts. The first part describes the relevant risks as well as the requirements posed by the legislation. The second part briefly discusses the enabling technologies for information security. The third part discusses how these technologies are used in SBR chains. We pay particular attention to how identification, authentication and authorisation is handled for the I-processes. Special attention is also given to the use of the governmental public key infrastructure, digital certificates and an authorisation facility.

Chapter 9 – Governance and service management
SBR involves three forms of integration of inter-organisational information systems: network integration, horizontal integration and vertical integration. These various forms of integration lead to numerous dependencies, necessitating overall management and shared implementation. Each form of integration is based on different principles. This chapter describes the governance aspects that are relevant to the various forms of integration. It also provides the principles for chain governance within SBR. The chapter describes how governance is currently set up within SBR and how this relates to the various forms of integration. This chapter should be read in conjunction with Chapter 1. Because Logius is a SSC and can therefore specialise in all matters surrounding the provision and maintenance of services, and because it is responsible for the SBR building blocks, Logius is a particularly suitable candidate for controlling the complex playing field. The chapter describes with the management organisation set up to allow Logius to carry out this orchestrating role. It describes the management triangle model, with a central role for architecture as the focal point between the various forms of integration.

Chapter 10 – Reporting chain reengineering methodology for the implementation of SBR
This chapter provides a systematic approach for getting from a candidate chain – with partners interested in SBR – to an SBR chain. It describes a chain reengineering methodology with guidance on analysing, designing and transitioning towards an SBR chain. The prescribed methodology is rooted in the experiences gained from the previous realisations of SBR chains. The chain reengineering process starts with the candidate chain partner's interest in SBR and ends with a fully functioning SBR chain. The technical, political or administrative, historical, legal and organisational features of the candidate chain must be considered throughout the entire process. That is why the methodology leaves room for adjustments, allowing the candidate chain actors to determine the appropriate path to take. Nevertheless, the methodology does prescribe four stages that identify go/no-go decision moments for each phase, ensuring that chain parties can guarantee the quality of the progress at various checkpoints. The chain reengineering methodology also provides a content-based guideline that the parties can use as they go through the stages. Do's and don'ts are provided for each stage.

Chapter 11 – Final conclusion
This final chapter gives the reader a concluding perspective on the entire SBR solution. It discusses the strengths of the SBR concept, as well as the weaknesses of the current implementation in the Netherlands. Finally, we consider the possibilities that still lie ahead for the SBR solution and which barriers it may face along the way.

1.6.3 *Appendices*

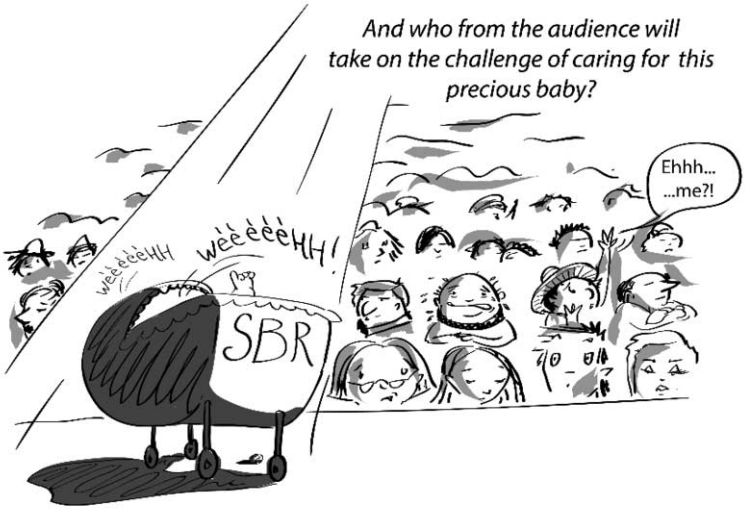
Appendix A – A brief history of SBR in the Netherlands
Appendix A contains an extensive analysis of SBR from a historical perspective. This description gives the reader an understanding of the background that is needed in order to understand the central theme of the book. The description provides insights into SBR's history and the underlying policy objectives. This appendix is particularly relevant for readers who are not familiar with SBR.

Appendix B – Supporting work
Appendix B summarises the research activities that were carried out in the creation of this book.

Appendix C – Glossary and abbreviations
Appendix C summarises the core concepts and abbreviations that are used in the various chapters.

Part A

SBR as a challenge for information chains



2 Information Chains

Chapter highlights

- Grasping the concept of an information chain
- Understanding what drives the creation of chains
- Examining the characteristics of information chains

2.1 Introduction

This chapter introduces the concept of a 'chain' and discusses the drivers behind the formation of chains. In addition, the general characteristics of chains will be discussed. The focus of this chapter then turns to the characteristics of information chains and business reporting chains in particular: What makes are the specific characteristics of these type of chains? These characteristics form the basis by which we present SBR as a challenge for information chains.

The remainder of this chapter proceeds as follows:

- **Section 2.2** explores the notion of a chain by highlighting actors and flow elements. It also discusses different types of chains.
- **Section 2.3** focusses on the factors driving the formation of chains. It is important to understand these factors when looking to effectively modify the components in a chain.
- **Section 2.4** discusses the general characteristics of chains. Together with the factors mentioned in the previous section, these general characteristics help pinpoint potential accelerators or barriers for chain reengineering (subject of Chapter 10).
- **Section 2.5** presents the more specific characteristics of information chains. Drawing on the basic setup of SBR chains, this section introduces the actors in roles in information chains.
- **Section 2.6** concludes this chapter with a brief reflection and outlook to the next two chapters.

2.2 What is a chain?

Chains link together actors and activities that serve one or more goals, depending on the type of chain. A chain actor, often referred to as a 'link' or 'stage,' can be a private organisation, public agency or department within a larger organisation that is responsible for one or more activities (tasks) in the chain. The definition of activities depends on the flow element that is transferred between the chain actors and activities. It can be a tangible product, a person or a piece of information, for instance, in the form of a business report. Each activity must add value to the flow element. When considering the production of a consumer good, such as a television, activities could involve its assemblage, production, inspection, packaging, transport and storage. These kinds of activities require inputs—human resources and raw materials—which are employed to add value and transport the flow elements to the next actor (or stage) in the chain. When the flow element is information, activities often include registration, production, processing and decision-making. Figure 2.1 illustrates the actors and flow elements within a chain.

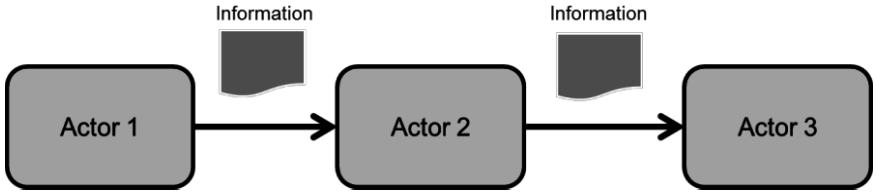


Figure 2.1 – Actors and information as flow elements within a chain

In Figure 2.1, each actor provides the goods or services that are required to create added value within the chain. The simple representation of the chain in the figure shows the interdependencies between the actors in a chain, where the functioning of an actor depends on preceding and subsequent actors. When one actor does not function well, the whole chain is affected and will feel the consequences. In this context, it is often stated that the strength of a chain depends on its 'weakest link' (see Chapter 6). Therefore, the interdependencies between these actors are an important aspect of a chain.

Some additional factors also determine the interdependencies existing between actors in chains. Van Dalen (2000) provides a brief summary of these factors:

- The size of an actor: size of staff, distribution across the country, turnover or capital of an actor.
- Special technological competencies of an actor: special niche products, network knowledge or network relationships.
- The prevailing laws and regulations (applied or enforced by administrative authorities)

As mentioned in the introduction of this chapter, a concept that is often related to chains is the concept of networks. A 'network' comprises a dynamic group of actors and their mutual relationships, which emphasises, to a greater extent than a chain, the heterogeneity and mutual interdependencies of the actors (De

Bruijn & Ten Heuvelhof, 2008). Here, network refers to the idea that all elements within a network are connected to each other. Each actor enters a network voluntarily, based on the expectation to possibly profit from the network. A 'chain,' on the other hand, emphasises the sequence of processes and the dependencies between actors that result from this sequence. The relationships between actors in chains also have a more formal, long-term and stable character compared to the more dynamic relationships between actors in networks. Moreover, in some specific chains, the participation of certain actors is mandated by law. For example, in tax reporting chains, certain actors are obliged by law to file their tax returns. A chain can thus be part of a network, where the chain consists of a specific, predefined set of connections within the network. This book focuses solely on chains.

There are various types of chains, all with different actors and/or flow elements. Examples of chain types include:

- Production chains, in which each actor is a part of a sequential production process. The flow elements are the products that are being produced. Each link provides added value by further developing the product.
- Passenger transport chains, in which travellers are the flow elements that each have their own chain. In this case, the actors are the means of transport. Each actor provides added value by transferring people further towards their destinations.
- Information chains, in which information is the flow element. The actors are the organisations that share the information, for instance by means of business reports. A further distinction can be made when looking at the value of information. On one hand, value is added by improving the processability and quality of information to be delivered to the end-user (the requesting party). Depending on the requesting party, the exchanged information may then be used for its own processes such as risk assessment, decision-making and policy-making.
- Policy chains, in which the flow element is a policy being created and the actors are the organisations associated with the policy. Added value is provided by moving the policy idea further towards implementation. When a distinction is made between policy and implementation, one can refer to implementation chains and policy chains.

The examples above show that chains can vary with respect to the types of actors and flow elements they comprise. A chain's goals will therefore vary depending on the type of chain and its characteristics. For example, the goal of a production chain would be to deliver a finished product whereas the goal of a policy chain would be to implement a well-considered policy.

In information chains, the exchange of information is a means to fulfil the goals of the chain's actors, although these goals may differ between the various actors. We can however, identify some general goals of chains. These include:

- Achieving efficient processing of the flow elements between actors in the chain.
- Adding value to the flow element.

The following section explores the drivers that constitute the formation of chains.

2.3 Drivers of a chain

We have discussed the chain concept and its goals. But what are the factors driving the formation of chains? The answer to this question differs depending on the type of chain. For B2B (Business-to-Business) chains, the goals to be achieved are the most important drivers, and actors can improve efficiency and add value by participating in the chain. However, for B2G (Business-to-Government) chains, legislation is the most important driver behind the chain's creation. According to the legislation, businesses are required to submit information to certain government agencies, thus necessitating the chain's existence. The same applies to SBR business reporting chains.

Now that it is clear why chains come into existence, the question that remains is why organisations want to participate in chains? After all, participation in a chain is associated with various costs, in terms of:

- Money (contributions / subscriptions)
- Transaction costs (time spent on coordination between the actors)
- Loss of autonomy

Despite these costs, there are both collective interests and individual motives that drive participation in a chain. Examples of these motives can include improvements in efficiency, increased quality, sustainability and safety. Legislation is another important motive. While these drivers are all important, the collective and individual motives of individual actors within a chain may come into conflict if one actor places more value on a particular motive than does another. Such differences between the collective and individual motives can complicate chain coordination and expose the dependencies between actors. Thus, actors must search for an optimal balance between autonomy and interdependence within a chain.

It should be noted that there is an important difference between demand-driven and supply-driven chains (this will be discussed in Section 2.4), and that the drivers of participation in these chains are not the same. The incentives for chain participation will also differ between business cases from the market, in which guarantees have monetary worth, and cases from the government, where guarantees cost money. Thus, participation in a chain depends on the type and characteristics of the chain. The following section will elaborate on the general characteristics of chains.

2.4 General characteristics of chains

Each chain involves multiple actors that have various roles. These actors can be a part of the chain but can also operate in the context of the chain without actually being a part of it. Due to this variety of actors, there can exist large differences between chain and their characteristics. In this respect, the following variables play an important role:

- Demand-driven vs. supply-driven chain
- Absorptive capacity
- Vertical and horizontal integration/disintegration
- Vertical and horizontal collaboration
- Intertwinement
- Distribution of power
- Trust
- Distribution of benefits
- Soft variables

Demand-driven vs. supply-driven chain

Chains can be either primarily supply-driven or demand-driven, and this orientation affects the way a chain is coordinated. Traditional, supply-driven chains are often coordinated based on the business objectives and demand forecasts set by suppliers. They tend to display considerable latency related to long production times, lead times, inconsistent transportation and other inefficiencies. This latency can lead to the 'bullwhip effect,' a concept that was discovered by P&G in the 1980s (Lee et al, 1997). The effect implies a trend of increasing swings in inventory for upstream actors in the chain in response to changes in consumer demand. These types of supply chains are also called 'push' chains, as they build products and send them to the market based not on actual demand, but on forecasts. These forecasts rely on historical performance and market performance predictions.

Demand- or consumer-driven chains—think Airbnb and Uber—align their planning, procurement, and replenishment activities with actual consumption. These types of chains focus on ways to better capture the demand signal closer to the source, analyse the demand to sense the latest and most accurate demand signal, and shape the demand by executing and tracking strategies (e.g., promotions) to steer demand in line with business objectives. The key in these chains is to eliminate information latency (via integration) and unnecessary interaction, thereby reducing operating costs and improving profitability and customer service. This type of chain is also called a "pull" chain. Popular examples of chains that have changed from push to pull can be found in all industries (e.g., Dell in the PC industry).

Due to the rise of ICT, chains that were traditionally supply driven (e.g., retail stores) were able collect more information on customer behaviour (i.e. demand) and incorporate this information into their chain coordination, becoming more demand-driven in the process. Studies have shown that demand-driven chains

are particularly difficult to coordinate and that the distinction between completely supply-driven and completely demand-driven chains is purely theoretical. As we shall see, this theoretical distinction does, however, provide valuable insights into business reporting chains.

Absorptive capacity

Major chain transformations like SBR require a moderate to high absorptive capacity amongst stakeholders. Researchers have used the absorptive capacity construct to explain various organizational phenomena. Cohen and Levinthal (1990) offered the most widely cited definition of absorptive capacity, viewing it as the firm's ability to value, assimilate, and apply new knowledge and technical skill. Mowery and Oxley (1995) offered a second definition of absorptive capacity, as a broad set of skills needed to deal with the tacit component of transferred knowledge and the need to modify this imported knowledge. Kim (1997) offered yet another definition of absorptive capacity as the capacity to learn and solve problems. Regardless of which definition is used, chains exhibit varying levels of absorptive capacity amongst the linked organisations. Absorptive capacity differs between organisations due to differences in knowledge, expertise and available capacity. While there is some agreement that a similar or equally high absorptive capacity amongst partners can have a positive effect on the implementation of transformations, no universal steps have been recognized that can align organisations on this dimension. As will be discussed in Chapter 10, change agents should understand the absorptive capacity of their partners and act accordingly, since it will determine the possible magnitude and success of the transformation.

Vertical and horizontal integration/disintegration

Chains can be subject to integration or disintegration. Integration implies that some actors acquire and control multiple activities within a chain, so that the activities in the chain are performed by less actors than before. This can either occur in the form of vertical integration (actors acquire and integrate subsequent actors or stages in the chain) and horizontal integration (actors acquire similar—either complementary or competitive—actors within a chain). Note that the integration of actors can occur with respect to both actors and activities (as discussed in Section 2.2).

An example of vertical integration with respect to SBR can be seen with the shared service centre (SSC). The SSC offers a shared service in which the information is pre-processed before being forwarded to the requesting parties. Therefore, the SSC takes over certain tasks that were previously performed by the requesting parties themselves, an example of vertical integration. It should be noted, however, that from the perspective of the requesting parties, this could be seen as horizontal disintegration. An example of horizontal integration can be seen in the accounting business. While the past accounting market consisted of multiple small accountancy firms, it was subsequently transformed into a market in which only four large accounting firms are dominant. These few powerful players now perform all of the activities that were previously performed by the

multiple smaller firms. On the other hand, disintegration (either vertical or horizontal) implies that some links (actors or activities) are disposed of by an actor within the chain. One form of disintegration is specialization, where tasks within a chain are separated and divided over multiple actors. Here, an actor specializes in the activity for which it has a comparative advantage. An example of vertical disintegration can be seen with the Tax and Customs Administration. In the past, this party was responsible for conducting basic fiscal checks, whereas nowadays these basic checks are integrated into software packages. That is, software developers began to produce software packages that are suitable to perform these basic checks, thus making Tax and Customs Administration's checks unnecessary and causing disintegration in the chain.

An important remark must be made with respect to the horizontal and vertical S2S integration discussed in Chapter 1. It must be noted that these types of integration are fundamentally different from the supply chain integration/disintegration being discussed here. With S2S integration, which was made possible due to the application of open standards, changes can occur within chains as they become more flexible by means of loose coupling. This implies, for example, relocating actors or activities within a chain, which changes the chain's configuration. Barriers can be eliminated between actors and between different activities within a supply chain, which can, in turn, lead to specialisation (a form of vertical disintegration, as discussed above), in which certain activities are transferred to and performed by specialised actors. Thus, the flexibility of chains due to S2S integration can affect supply chains. And while the actual consequences of S2S integration for supply chains cannot be determined beforehand, the potential for major changes can be expected.

Vertical and horizontal collaboration
Chains may also be subject to vertical and horizontal collaboration. Vertical collaboration refers to collaboration between suppliers and customers within a chain. For example, accountants collaborate with software developers in the creation of accounting software. Accountants prefer such software, which meets their needs to a greater extent than other software, thus benefitting both parties. Horizontal collaboration refers to collaboration with competitors and other actors within in a chain, for instance, by sharing resources. An example of horizontal collaboration is the SBR direct initiative in the Dutch banking industry. Using an online submission portal, businesses can submit credit reports to the connected banks that take part in the financial reporting cooperative.

Intertwinement
Chain intertwinement can occur when multiple actors use a SSC for the interorganisational exchange of information. For example, the fiscal reporting chain and the annual reporting chain become intertwined through the use of the same chain information system components, referring to the interface service and data specifications.

Distribution of power

The distribution of power between actors in a chain is an important characteristic of a chain and a central issue from a political perspective. Power is the ability to enforce decisions upon other parties. In this respect, the sequential dependency among organisations in a chain determines the exchange and negotiation relationships between organisations. These relationships are characterised by unequal access to—and the distribution and use of—scarce resources such as expertise (Bekkers, 2000). Collaboration between the organisations is not self-evident due to the unequal distribution of power, although it is necessary due to the sequential dependencies among organisations within the chain.

There are various sources of power within a chain. These include:

- Formal authority: Government parties can have formal authority over a chain. This can occur when the requesting parties are governmental bodies for which the requested information will fulfil specific legislative requirements. Moreover, when the governmental body plays a supervising role, it can exercise its power over the entire chain.
- Monopoly on added value: When there is only one party within a chain that can add value to a flow element, the monopoly power of this party can have a large influence on the chain's result. Even though a 'pure monopoly' is rare nowadays, one very powerful player can be found in almost every chain. In e-commerce, the presence of a single powerful party has been considered to be a factor that contributes to the success of a chain (Monczka, Petersen, Handfield, & Ragatz, 1998). For example, Walmart can be considered as a very powerful actor in the American food chain. Similar is Tesco's position in the British food chain. These powerful actors are major contributors to the success of the food chain.
- Allocating actor: An allocating actor can choose between various products or services that are offered by successive actors. Allocating actors can thus affect the extent of divergence in a chain. They also shape the course of the processes for the subsequent actors. Moreover, allocating actors are less dependent on a single successive actor because they have alternatives (De Bruijn & Ten Heuvelhof, 2008). These alternatives give allocating actors a certain power over the subsequent actor.
- Selecting actor: A selecting actor in a chain can choose between the various products or services resulting from the activities of the preceding actors. An illustration of this is given in Figure 2.2. Such a choice may considerably influence the processes of subsequent actors. In addition, selective actors become an important partner for the preceding actors, whose products or services may or may not be selected. This creates a powerful position for selective actors (De Bruijn & Ten Heuvelhof, 2008).

Powerful actors can thus determine the function of a chain. For instance, they can determine the social structure of the chain and can impose standards on other parties in the chain. Moreover, they can control the distribution of costs and benefits within the chain. A powerful actor is likely to enjoy more of the chain's benefits compared to a less powerful actor.

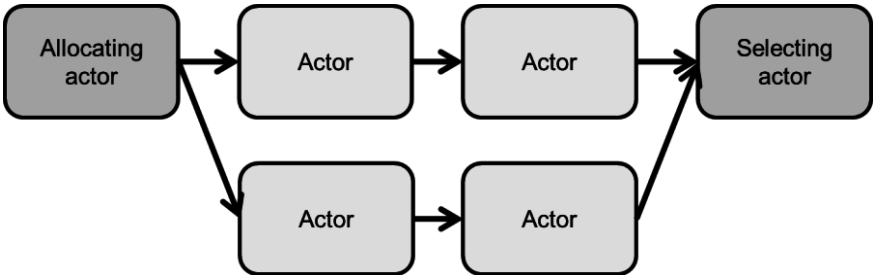


Figure 2.2 - Selecting and allocating actors within a chain

Power can be concentrated in one powerful actor or be more evenly distributed between the actors in the chain. Dispersed power within a chain, however, can create difficulties with respect to chain coordination. For example, it may be difficult to implement one rule for the entire chain, as the rule might not be easily applicable to each actor in the chain. In addition, when there is no authority at all within a chain, there exist mutually dependent relationships between parties for which collaboration is required. However, this collaboration may not always be realised. Finally, with a lack of authority within a chain, coordination problems may arise as some parties simply do not want to be steered towards a certain direction.

Trust

Trust is an important condition for participation in a chain. Chains cannot survive unless the various actors are confident about a mutually beneficial and evenly distributed result. According to Van Dalen (2000), a distinction can be made between two forms of trust:

- Organised trust. This is the most visible form of trust. It is recorded in pricing agreements, contracts, formal rules and procedures, and certificates. The formal character of these agreements provides a solid basis for confidence in a good collaboration between actors in the chain. Organisational trust stimulates parties to enter chains. In addition, it provides certain guarantees despite parties not having worked together before.
- Emergent trust. This type of trust is created through collaboration between parties. Directly seeing the behaviour of other chain parties can strengthen mutual trust. Do the partners keep their promises? Do they have similar ideas about meeting obligations and exercising rights?

These two forms of trust are not mutually exclusive. Formal measures, for instance, provide sufficient certainty for parties to start a collaboration. When this leads to good results, the emergent trust between partners is strengthened. In this way, one form of trust can facilitate the other (Das & Teng, 1998).

Distribution of benefits
The benefits within chains can be unevenly distributed among actors, therefore raising the question of who will benefit from investments made in the chain. Will the main investor (e.g., a requesting party) be the only beneficiary of the investment? If so, this may have consequences for the willingness of the other parties (e.g., intermediaries and software providers) to invest in the necessary means for information exchange (Meijer, 2009; Teece, 1998). In addition, investment revenues do not only end up with the various actors in the chain; the actual payoffs can often be spread over time to new entrants (e.g., start-ups without any technical legacy). In this way, other parties may profit from investments made by a specific actor.

Soft variables
There are some soft variables that affect the structure of a chain. Why do actors in one chain collaborate without any problems, while collaboration in other chains is marked by political conflict? Such a divergence is associated with the social structure of the chain (Meijer, 2009; Uzzi, 1997). Some related factors affecting such dynamics are the culture of the sector, the proximity of chain partners and the wealth/scarcity present in the chain (Duivenboden, Veldhuizen & Twist, 2000).

The above-mentioned chain variables are useful in analysing chains. There are also basic characteristics that can help understand a chain, such as the sector characteristics, the type of information system that is used, and—for reporting chains in particular—the type of government task supported by the chain (e.g. tax declarations, inspections, declarations on imported goods, etc.).

2.5 Specific characteristics of information chains

Now that the concept of a chain and its general characteristics have been presented, our focus will shift towards information chains in particular. While the variables mentioned in the preceding section are also applicable to this type of chain, information chains have some specific characteristics that deserve special attention. We will first focus on the characteristics that pertain to the particular flow element of these chains: information. The focus will then shift to SBR reporting chains in particular, for which the parties involved and the specific actions taken will be discussed.

First, information as a flow element makes information chains special for the following reasons:

- Information is a particularly volatile and rapid flow element.
- Information appears in all forms, shapes and sizes.
- Information is subject to various interpretations and is therefore more subjective than, for example, goods.
- Information is often 'intangible.'
- The flow of information is endless and can always be copied.

Second, the number and types of parties involved in an information chain differs between chains. However, as mentioned before, this book is mainly focused on SBR reporting chains—information chains in which the business information of public and private organisations is the flow element. At least two parties are involved in a reporting chain, namely the reporting party, which provides the information and the requesting party:

- Requesting parties: These actors request and should receive business information from the reporting parties. The requesting parties impose requirements on the information and its method of delivery (e.g. what information is expected, when and how often the information is expected, and to what extent the information must be reliable). When the requesting party is public (a government agency), the information requirements are primarily based on legislation. Moreover, the authority of a public requesting party is legally bound. For example, the Tax and Customs Administration must specify in advance what information it will request from businesses.
- Reporting parties: These parties provide the requested business information to the requesting parties. In most countries, the majority of companies do not prepare and file business information themselves. Rather they employ the services of specialised service providers – intermediaries – such as bookkeepers, accounting firms and tax consultants. The extent to which the services of intermediaries are employed ranges from managing the entire administration to only supporting the message submission/filing process. Throughout the various processes, multiple software providers can be involved. For the purpose of simplification, this book uses the more intuitive distinction between reporting party and requesting party, unless a specific process is involved for which we need to clarify the role of the intermediary or software provider.

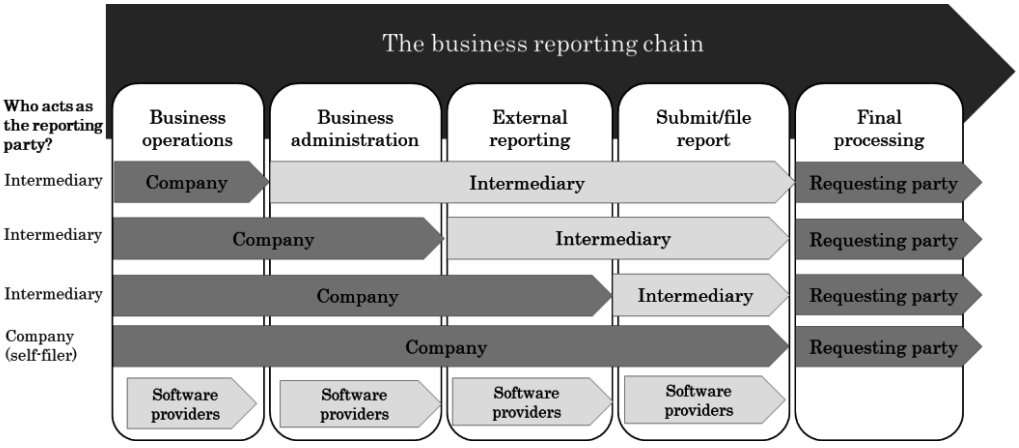


Figure 2.3 – Various actors in business reporting chains

Third, an SBR information chain is characterised by the following basic set of recurring actions:

- Registration: the reporting party registers information about its business operations.
- Composition: the reporting party draws up a business report based on the registered information.
- Transporting: the reporting party sends the information to the requesting party.
- Acceptance: the requesting party determines whether the business reports satisfy the processing requirements.
- Evaluation: the requesting party evaluates the content of the information.
- Decisions: the content-based assessment leads to a formal decision by the requesting party, although this does not apply to all requesting parties. For example, the Tax and Customs Administration draws up a decision whereas The Chamber of Commerce and Statistics Netherlands may only issue a notification that a report has been received.
- Notification: the requesting party informs the reporting party of its decision. With respect to VAT, the Tax and Customs Administration does not provide any feedback information if the declared and paid amounts are equal (and both were submitted in time).
- Taking note: the reporting party takes note of the decision.

Figure 2.4 illustrates the various actions of a business reporting chain.

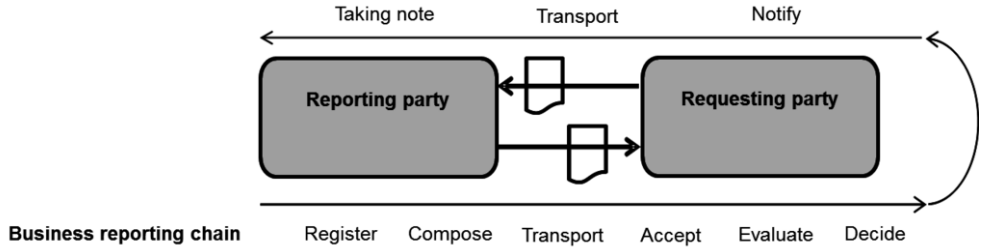


Figure 2.4 - Actions in a simplified reporting chain

Some additional remarks must be made with respect to Figure 2.4. First, it should be noted that the reporting party may need to act based on the decision made by the requesting party. For example, in the case of a tax return filing, the tax assessment by the requesting party is usually followed by a payment from the reporting party. The reporting chain is therefore part of a longer information chain. Second, it should be noted that the figure only shows what is known as the 'happy flow, an information chain in which no errors occur and all messages are processed as planned.'

In practice, the process can result in various outcomes. For instance, an error may occur if a tax declaration turns out to be incomplete and is therefore not able to be processed. In such cases, the involved parties would intervene (either

in a predetermined way or otherwise) in order to achieve the required outcome. This is also known as 'error handling.' In practice, many activities in a chain are concerned with error handling.

Requests for postponement
Reporting parties may file a request for postponement regarding the provision of business information. This affects the processes within a reporting chain. For example, organisations may request postponement with respect to the value added tax or the submitting of financial statements to the Trade Register of the Chamber of Commerce. Intermediaries may also submit these requests on behalf of the organisations. When postponement is awarded by the requesting party, the reporting party can spread out the amount of work done with respect to the business reports over a longer period of time. Figure 2.4 thus merely illustrates simplified representation of actions in the chain, and these actions can be affected by multiple factors, depending on the type of chain.

The parties involved in reporting chains aim to ensure a cost-effective reporting process. When possible, they automate activities in order to improve the efficiency and effectiveness of these activities. Chapter 1 explained the benefits of automation, especially S2S integration. Outsourcing tasks to third parties is also a possibility for improving cost-effectiveness within a chain and involves changing the chain. It is crucial to pay attention to the concept of change, since information chains feature unrelenting change—all the time and in every conceivable way. About the only constant of information chains is that every component of the chain is subject to change. And after it changes, it will probably change again and again. Such changes can range from reengineering an entire chain to modifying an element in a taxonomy. In fact, all of the various components that constitute an information chain are subject to adjustment. For example, chains may change due to the availability of better/more robust technology or due to changes in organisations (actors) within a chain. Triggers for change may also come from the outside, such as modified or new legislation.

Due to the many interdependencies between actors and system components, changes can have far reaching implications. As such, the efficient and effective implementation of change requires the involvement of subject matter experts, who first conduct a chain analysis in order to map the required change and its possible effects. The questions provided in Table 2.2. can be used for this purpose.

Table 2.2 – Some questions for information chain analysis

Questions for an existing chain • Who is responsible for what in the chain? • How are decision rights allocated within the chain? • Who pays for what? • How do these decision rights and payments affect the distribution of power and future developments within the chain? • Who takes the initiative on change?
Questions for change management • Where can the driver of change be found? • How is power distributed between actors within a chain, given the chain's structure, formal authority and formal competencies? • Which behaviours can be expected in the chain?
Questions for a new actors (entrants) within a chain • Which activities are performed? • Where are these activities performed within the chain? • What are the existing relationships in the chain? • What power does the new actor have within the chain? • Will old relations be broken down?

Changes within a chain can lead to added value for the chain, not only in terms of 'financial worth' but also in terms of user-friendliness and the clarity of the reporting chain. In addition, improved accessibility and availability of information, pleasant collaborations, or increased transparency and trust between chain actors can add value. Finally, improving the reporting experience adds value as information is managed and reported in a well-arranged and standardised manner (the 'store-once-report-many' concept, see Chapter 7).

2.6 Chapter conclusion

This chapter has explained the concept of a chain, the reasons why chains are formed and the characteristics of chains in general. The special characteristics of information chains and SBR reporting chains in particular were presented. Chains appear complex due to the diversity of flow elements, actors and activities within the chains. Moreover, making changes to a chain is also complex task due to these characteristics. With respect to chains, change is a broad concept that can refer to changes to the entire chain or changes in individual organisations or actors within the chain. Managing change in a chain therefore requires the specialised knowledge of experts. Chapter 3 will elaborate on the issue of change and the challenge of managing change.

3 Change Management in Information Chains

Chapter highlights

- Acknowledging that changes are unavoidable and should be managed
- Exposing the obstacles and challenges with regards to change in chains
- Figuring out how to deal with change

3.1 The issue of change

The previous chapter introduced the characteristics of chains, both in general and for business reporting chains in particular. An important observation from this previous chapter was that with business reporting, there exists a high level of interdependence among chain parties. The consequences of this interdependence are particularly noticeable when something requires modification or adjustment, or in other words, when something needs to change. The chain actors need each other's' support to effectuate the change, or, at the very least, should be willing not to impede or obstruct the change. Managing change is a complex process that has been widely studied under many banners—e.g., strategic reorientation, total quality management, reengineering, right sizing and turnaround. Under these banners, the reason for change can vary, just like the subject of change. Such reasons can come spring from a variety of variables, such as higher performance ambitions, changed market conditions, advanced technological capabilities or new legalisation. The subject of change can range from governance issues (e.g., who decides on what) to more technology-related aspects (e.g., interface specifications). Chapter 4 provides additional detail on the subjects of

change. As precursor to Chapter 4, the present chapter introduces the change management concepts, challenges and control instruments that are relevant to reporting chains. The goal of this information is to help the actors pursuing the change – the change agents – to pinpoint and address obstacles and related challenges. Accordingly, the remainder of this chapter is structured as follows:

- **Section 3.2** discusses obstacles for realising change and how these obstacles can be addressed.
- **Section 3.3** elaborates on the conceptual challenge of changes in reporting chains.
- **Section 3.4** highlights the importance of 'acceptance' for the implementation of change in reporting chains.
- **Section 3.5** elaborates on two opposing change management approaches: direct and indirect change management, including some guidance on when to use each approach.
- **Section 3.6** presents some control instruments that can be used to steer change management processes.
- **Section 3.7** concludes this chapter with a brief reflection and outlook to the final chapter in part A of this book.

3.2 Obstacles for realising change

Janssen et al. (2010) studied the development and application of ICT-based solutions for managing environmental permits, and observed multiple practical obstacles that emerge when change is pursued. These obstacles include the following:

1. Legislation, policy and technology become intertwined to such an extent that a delay in one area leads to a delay in the others. This creates a 'catch-22' loop, in which those who should adopt new technology wait until the legislation has been passed, but the legislation is not passed because actors have not adopted the new technology yet and policy makers feel they should not force actors to do so.
2. The project's level of ambition changes continuously and may even increase, resulting in a project that becomes too complex and/or too costly. In addition, administrative requirements and commitments from software providers may increase the level of ambition excessively, causing the project to become never-ending.
3. In practice, it is difficult to focus on technology and the business while also maintaining support for the changing project. The main goal of the change (in the case of the study, ICT support for environmental licences) may be forgotten, whereas the secondary goals (e.g., the technology, the organisation, obtaining support) may become the main goals.
4. Stakeholders, who feel their core values being challenged by the radical changes in the roles and processes of chain parties, are reluctant to participate. This resistance can be expressed through lobbying and administrative forums, both of which can be highly effective in obstructing for the entire change process.

It is not easy to define and implement a balanced package of measures in order to overcome these obstacles. Particularly when these issues occur simultaneously and in ways that cannot be anticipated, there is a tendency to respond in an *ad-hoc* manner. Consequently, projects are perceived as being managed as a series of incidents that keep popping up.

With regards to the SBR programme, when the responsible parties recognised the manifestation of all four obstacles to change at the end of 2009, they intervened with the following measures:

- A compliance working group was installed to address the first obstacle in particular. Technical and legal experts from the various public agencies participated in this team. The legal experts' assignment was to test the legal feasibility of the SBR Programme's ambitions in terms of development, implementation and change (both from a technical and functional viewpoint). They found that for most cases, the relevant laws and regulations did not contain obstructions to the realisation of the SBR programme objectives, provided that some preconditions were met such as following the right procedures (good governance) and publishing supplementary documents. To ensure compliance, well-timed communication of implementation issues with the various stakeholders was important. Another critical success factor for the working group was the collaboration between legal experts knowledgeable on technology and technicians acquainted with legislation and politics. The working group format has proved useful, as legal experts and technicians have been committed to SBR from an early stage, parallel with the programme's other activities. Because of this commitment, the working group has been motivated to seek out technical and legal possibilities rather than thinking in terms of impossibilities. The role of compliance, including the compliance of processes, will be discussed in detail in Chapter 6 (I-Processes).
- The Netherlands Taxonomy Project (the predecessor of SBR) started by storing the data definitions and requirements of important governmental organisations (Statistics Netherlands, the Chamber of Commerce and the Tax and Customs Administration) in an unambiguous way. The programme soon had to deal with additional ambitions, which included:
    - A multi-sided platform for shared ICT services provided by the government (including the generic infrastructure – see Chapter 7)
    - New forms of monitoring (a link between SBR and 'horizontal monitoring' by the Tax and Customs Administration, including the implementation of the simplified 'profit declaration' – see Chapter 1)
    - Reliability in terms of content from the beginning of the chain, achieved by applying Simplified Validation Rules
    - Business-to-business application of SBR

  At the start of 2010, the government focused on implementing the basic components solely for SBR chains. Therefore, the link between SBR and

horizontal monitoring was given less attention. In addition, the Simplified Validation Rules had been removed from the shared services provision. All parties were focused on achieving a stable reporting chain, in particular for the purpose of sending information to administrative authorities. When this basic feature was operationalised and stable, some important SBR issues requiring attention reappeared on the agenda. However, the advantage was that these issues could now be built on a stable platform.

- The involved parties understood that government influence over one of the SBR's most significant policy goals—reduction of administrative burden—was initially limited. Reduction of the administrative burden required mass adoption of SBR that would result in the creation of economies of scale. The path to adoption has thus been split into several successive steps. The first goal was to provide policy makers and sceptics with a 'proof of concept' presenting the feasibility of a functional reporting chain based on SBR. In 2010, all participating public organisations created a joint roadmap for scaling up the usage of the SBR reporting chain. Project managers were assigned to each SBR partner. and were responsible for the realisation of an operational delivery chain. The project managers focused on the relevant topics (technology, organisational change and support) and assured that a credible solution was well defined and documented. This proof-of-concept chain provided the stakeholders with sufficient confidence to continue on with the next step. This next step would be to gradually implement SBR as the sole method for system-to-system reporting from 2013 onwards. This proof-of-concept approach has provided a huge push towards market adoption and, as a result, the original policy objectives have become attainable.
- In 2010, an altered marketing strategy for SBR was launched, focusing on parties who were reluctant to adopt SBR for a variety of reasons. The programme communication took on a different, more empathic, tone, changing its message from 'you must be out of your mind if you don't understand this' to 'we would be very pleased if you would join us.' Furthermore, region-specific information sessions for interested parties were set up and continue to be held today as opportunities for opponents and critics to ask questions and have their concerns addressed. The programme focus switched to a much more friendly and accessible strategy, changing the atmosphere from an 'us vs. them' (leading vs. lagging party) approach to a more cooperative one. This led to a much less polarised playing field. The programme benefited greatly from this more empathic approach.

These above measures demonstrate that a carefully drafted change management process is vital in solving substantial implementation issues. We will now discuss a couple of the conceptual challenges of managing change in reporting chains.

3.3 The conceptual challenges when managing change in reporting chains

When redesigning reporting chains, the change management agent will deal with a variety of challenges. This section will elaborate on:

- The intrinsic resistance of reporting chains
- Strategic behaviour
- Trade-offs and choices in chains

3.3.1 *The intrinsic resistance in reporting chains*

Chapter 2 discussed a number of reporting chain characteristics that may complicate the effectuation of changes to those chains. Let us briefly review some of the most important characteristics:

- Reporting chains consist of multiple actors, each of which may have different and conflicting interests. In addition, chain parties may have different ICT architectures that do not necessarily fit together. Often, these architectures are difficult and costly to integrate. Furthermore, changes impose risks that may be deemed unacceptable by the other parties affected by the change. Mitigating these risks can entail huge costs (e.g., setting up a parallel infrastructure). Taken together, these situational factors may cause parties to resist the proposed change or even veto the change entirely.
- Reporting chains are dynamic systems in several respects. First, the operations are dynamic: billions of bits and bytes from one organisation to another each second. Secondly, the technology is dynamic: new technical opportunities emerge at a quick pace, followed inevitably by frequent updates for the ICT users. This dynamic character implies that organisations must change continuously 'by default'. Therefore, they may lack enthusiasm to implement additional changes required by other partners in the reporting chain.

Schekkerman (2000) adds two additional characteristics to this list:

- Dependency: when more and more business processes are handled by inter-organisational information systems, chain partners become dependent on those systems. Dependency necessitates tougher demands on various ICT-related aspects such as continuity, availability, reliability and security. In some cases, actors, often unwillingly, must cede their autonomy.
- Complexity: changes to inter-organisational information systems or to a standard (e.g., the taxonomy) may have considerable implications for chain parties. Complications are likely to occur, and when combined with a high impact, can potentially lead to significant business risk. Furthermore, not only do the systems need to be changed, but employees, for instance, require instruction and training. New organisational procedures and routines may also be necessary. In other words, interoperability needs be created—semantically, technically and organisationally.

These characteristics make change management in reporting chains even more challenging than may be expected in the case of 'normal' organisational changes. Taken together, these characteristics can create a change environment with a high degree of resistance to the change itself. Strategic behaviour can shape this resistance.

3.3.2 *Strategic behaviour*

The fundamental difficulty of managing change in reporting chains is dealing with inertia and resistance to change. Such behaviour can be understood based on the characteristics of reporting chains described above. The idea of introducing standards for business reporting would ostensibly be an attractive idea for all types of actors. Yet, even if the potential overall advantages are obvious, it is not immediately clear whether each individual actor will benefit from these changes. This uncertainty can result in resistance and/or inertia and involved parties might be reluctant to fully commit to new systems and programmes such as SBR. While full commitment would benefit the change agent, actors may instead choose to behave strategically, weighing each step against their own organisational goals. This is called 'strategic behaviour.' Two frequently occurring forms of strategic behaviour are:

- *Wait and see*. For instance, there might be multiple reporting parties, software providers and intermediaries showing interest in developments and participating in working groups and meetings organised by the government. However, these actors might wait until SBR is clearly a '*fait accompli*' before making substantial investments.
- *Free-riding*. Reporting parties might wait until the key investments have been made and the standards have been fixed. Until then, these actors do not contribute to the change in any way. The 'free-rider' can thus benefit from the investments that other parties have made. The other parties might thus become reluctant to make investments, mainly out of the fear of a competitive disadvantage compared to the free-rider.

The key to success is the ability of change management agents to deal with the challenges described. In particular, the change management agent must anticipate the various forms of strategic behaviour and 'free-riding.' The following section discusses the trade-offs that change management agents need to identify and overcome before a practical approach to change can be realised.

3.3.3 *Trade-offs*

Van Twist et al. (1998), highlight the context of change and propose '*thinking in dilemmas*' when changing an organisation. The authors present a methodology for organisational change, providing guidelines for change management agents to use in determining the proper mix of change instruments. When speaking of this process, we prefer the term '*dealing with trade-offs.'* A trade-off is a choice between two competing values, in which both values have positive and negative

implications (see also Quinn, 1998). Choosing either will thus have both advantages and disadvantages.

Trade-offs capture the interdependence of problems and solutions in complex organisations and chains. If trade-offs are not recognised, there is a danger that organisations or chains will continue to modify their choices again and again, creating a cyclical process. Consider the following example (Van Eeten, De Bruijn, Van der Voort and Van Bueren, 2000):

- Change management agents choose Option X because of its advantages.
- After some time, the disadvantages of Option X start to outweigh its advantages.
- Given this newly attained insight, Option Y and its advantages appears to be more attractive.
- Option X is abandoned and everything is changed in order to pursue Option Y.
- After some time, the disadvantages of Option Y start to outweigh its advantages.
- The process starts all over again.

It is of key importance to make choices on different trade-offs based on the available information, and equally important to stick with these choices. This enables the transparent accounting for possible disadvantages while maintaining a steady course. Nevertheless, switching between trade-offs during a change process is not necessarily wrong, the precondition being that the new direction is a well-considered and conscious decision. In changing a chain, the challenge is to find an arrangement that fits the chain's characteristics. This makes it imperative that decisions be made only when a high level of detail is known. For example, when initiating a top-down change, a change manager should leave room for parties to steer the change from the bottom up as well. Such a consideration applies not only to the (technical) design (as in a 'coarse/fine cycle'), but also applies to the change implementation process.

In order to clarify the concept of 'identifying trade-offs,' we will present two typical trade-offs that appear when making changes to reporting chains.

A high or low level of ambition for the change process?

The level of ambition for a change process can be high or low. A high level of ambition focuses on large changes with high potential benefits and generally attracts considerable attention. Given the large scale of such a change process, it generates support from the executive level. The drawback of a high level of ambition is a significantly higher risk of failure. Doing more and involving more actors implies that more aspects need to fall into place in order to realise the benefits. A low level of ambition, on the other hand, involves goals that are easier to attain. As there are less potential benefits, executives may not be as enthusiastic for the change process. In spite of this downside, however, there is considerably more certainty that the intended goals will be reached. The trade-off can thus be identified as follows: Greater benefits but a higher risk of failure with a

high level of ambition, versus lesser benefits but a higher certainty of success with a low level of ambition.

Focusing on early adopters or followers?
Another trade-off involves the choice between focusing on early adopters or on followers. It is a strategic choice about how best to achieve economies of scale in a new chain (or channel within a chain). Early adopters make it possible to learn a great deal about the best way to set up the new chain. In addition, if successful, these early adopters can be used as an example for other parties. However, focusing too much (or one-sidedly) on this group may lead to the situation in which followers end up lagging behind considerably. They are either unable to keep up with the pace, as too much attention is paid to early adopters, or lose interest after time and exercise strategic behaviour). In addition, a sense of 'us versus them' may arise, with the risk of the early adopters losing contact with the stragglers. Such a situation may also create 'groupthink' (Janis, 1972). Focusing on the followers, on the other hand, guarantees that the group of users will remain together. However, a disadvantage is that the pace of development can only be as high as the slowest straggler. The risk from this option is that little or no change will occur.

3.4 The paramount importance of acceptance

The conceptual challenges described above show that while the cooperation of chain partners is essential for the realising change, assuming that actors will automatically cooperate is risky. In order to steer change under such conditions, it is important to understand the concept of acceptance and the means by which it can be obtained. We define acceptance as the '*demonstrable willingness of a chain party to support and realise changes.'* Acceptance is by no means a given. Changes in reporting chains take place in a dynamic, multi-actor context. As a result, there are a number of possible causes for a lack of acceptance:

- Chain parties have different organisational objectives. To optimise the achievement of their own goals, chain parties will have different preferences with regard to a change.
- Chain parties may have different starting positions, for instance, in terms of the degree to which they already work with automated systems. This may cause differences in the impact of the change, and consequently in change preferences.
- One chain party may face expenses in implementing the change, while the benefits accrue to another chain party.

If one or more chain parties are not willing to accept the change (perhaps due to one of the causes listed above), it may be desirable to provide incentives to stimulate acceptance. The various change strategies and control mechanisms described later in this chapter all utilize incentives to achieve acceptance.

A large number of factors can influence acceptance or rejection of changes. These may factors that concern the characteristics of the change, such as the advantages for the chain party, the interoperability, the scope for experimentation,

and reversibility (Rogers, 2003). However, factors such as perceived risks, trust (in the forum and in the control instrument) and communication about the change can play a role as well (Clark, Cavanaugh, Brown and Sambamurthy, 1997). Understanding the influence of these factors and their change-specific nature, can help to determine how to encourage acceptance.

3.4.1 *The conceptual framework for acceptance*

Based on the work of Merchant and Van der Stede (2003), we have developed a conceptual framework that can provide guidance on determining the root-cause for a lack of acceptance. With this knowledge, the change management agent will be equipped to create successful interventions to encourage acceptance. Merchant and Van der Stede (2003) distinguish three control and management problems, namely lack of direction ('knowledge'), lack of competence ('ability') and lack of motivation. Table 3.4 applies these concepts to a change in a reporting chain.

Table 3.4 – Knowledge, ability and motivation

	Definition
Knowledge	The extent to which a chain party is certain about the internal conditions and impact of the proposed changes in its individual context.
Ability	The extent to which the chain party is convinced that it possesses the competence and has the instruments necessary to implement the change.
Motivation	The extent to which the chain party is convinced that the proposed change contributes to the cost-effective achievement of its own targets.

The chain party's position when evaluating the ability and motivation aspects is based on the knowledge aspect. With respect to ability, a lack of skills and resources may create obstructions to the realisation of a change. Motivation is the key driving force behind acceptance. If the chain actor is convinced that the change will contribute to its own goals, accepting the change will be easier. The idea or belief that a change may not lead to (or may even be counterproductive to) its goals, will lead to a low level of acceptance. In this context, Metselaar and Cozijnsen (2005) also refer to the 'willingness to change.' The above conceptual framework can also be used in the dialogue regarding the change, as a way to uncover the causes of any lack of acceptance.

The changes themselves may relate to a combination of dimensions, including processes, technology, organisation (structure and culture) or collaborative agreements. A chain party that is not accepting of a proposed change can therefore make clear which of the dimensions of the change it does accept. Using the three aspects (knowledge, ability and motivation), the chain party can explain whether the impact of the change is not clear in its individual context, whether it believes it does not have the required skills and/or instruments to make the change, and/or whether it lacks the motivation to implement the change.

3.4.2 *Changing the chain conditions*

An important aspect when dealing with acceptance is changing the chain conditions. Kurt Lewin (1951), one of the pioneers of change theory, developed three steps that involved the concepts of unfreezing – moving – freezing. Unfreezing refers to preparing the organisation's employees for the change by 'unfreezing' their minds. The move is the change itself, and the freezing is the internalisation of the change.

Lewin's concept is aimed very specifically at addressing resistance coming from individual employees in an organisation. However, while the process he describes is different from the process of change in reporting chains, the idea of exerting influence on the circumstances of a change remains applicable. To this effect, strategic communication can be employed.

Strategic communication
Strategic communication uses proven means of communication, both inside and outside the programme, to influence the way actors perceive the change. Close attention is paid to the connotations associated with concepts. Communication regarding the concept of 'chains' is an example of this.

Reporting chains are only 'visible' on paper. They are, in fact, nothing else but a structure of ideas—a metaphor for the way that processes actually run, or ought to run, according to a specific party. However, the concept of the chain remains a very powerful metaphor that makes it possible to explain complex processes in a relatively simple way to people who have not studied these processes in detail. Such is sometimes the case at the executive levels. This strength, however, may also be a weakness, as the conceptualisation of a chain can soon result in other processes (especially those that are not integral to the chain) being moved to the background (Van Duivenboden, Van Twist and Veldhuizen, 2000). People will see, so to speak, nothing but the chain. Of course, whether the metaphor of the chain is a strength or a weakness depends on the question of how the metaphor is used for communication.

Over recent years, the literature in economics and public administration has paid a great deal of attention to deliberately exerting influence on the choices made by others by means of strategic communication. Thaler and Sunstein (2008) refer to this as *nudging*, while other literature refers to it as '*framing'* (De Bruijn, 2011; Korsten, 1988). The way in which a problem or solution is expressed in language (or 'framed'), has a strong influence on the mental picture created. Framing a problem or solution (either yours or someone else's) is therefore extremely important as an instrument for indirectly influencing decisions.

Many examples of framing and their influence on decisions can be found in contemporary socio-political debate. A striking example was the successful campaign by the animal welfare organisation WakkerDier to term cheap meat products from the farming industry as '*kiloknallers*,' emphasising the low prices for

large quantities. Another example of framing is the interpretation of energy savings. Consider two campaigns, the first stating, "If you take energy-saving measures, you will save 350 euros," and the second stating, "If you do not take energy-saving measures, it will cost you 350 euros." Research has shown that the second campaign will be much more effective than the first[5], since people tend to be more responsive to the possibility of losing money than gaining the same amount. SBR, for instance, was sold politically as a reduction in the administrative burdens for businesses, whereas it is certainly also about reducing the implementation burden on the public side and increasing the quality of data.

Framing has its flip side too. Especially in the public arena, certain terms and mantras can suddenly be used by everyone, or become unfashionable. An example is the negative image acquired by the 'Electronic Medical File' case in the Netherlands, which is actually not a 'file,' but an infrastructure for exchanging medical data between medical professionals. Although the file is virtual, it is possible that the term 'electronic medical file' gave rise to privacy concerns regarding the confidentiality of the data. The result might have been different if the same system had been announced as 'a communication solution to promote cooperation among physicians and pharmacists, thus preventing errors.' In that case, the reliability and accessibility of the patient data would probably have been highlighted and not the confidentiality issue.

These examples show that strategic communication is a useful tool for gaining increased acceptance. It is possible to highlight or downplay certain details, so that a change appears to be more in line with an actor's business goal. The right presentation of facts may therefore be necessary to create acceptance.

Now that we have discussed the complexity of change within chains, the following section provides insights into different change management approaches and control instruments for dealing with this complexity.

3.5 Two opposing change management approaches

To manage change in information chains, we identify two distinct approaches: direct and indirect change management. While both approaches may employ the same type of instruments (e.g., procedures, projects and programmes) for steering change, the build on opposing assumptions regarding the understanding of Situation A (the starting point) and Situation B (the desired outcome). Chapter 4 explores the characteristics of both situations in more detail. We proceed with an elaboration on the direct and indirect change management approaches.

[5]The example was taken from Thaler and Sunstein (2008:40)

3.5.1 *Direct change management*

Direct change management assumes that the change agent and the other chain partners have a clear understanding of Situation A and Situation B beforehand and that Situation B is preferred to Situation. Moreover, it assumes that the change agent has the authority (either formal or informal) to launch a change. The main question in direct change management is how the chain should move from A to B in a sequential manner. In the direct approach, there is a strong tendency towards top-down coordination due to the possibility for extensive planning and direct steering. Knowing the details about A and B allows for blueprint based planning in which the roles, tasks, outputs and schedules can clearly be defined.

The business case for direct change management
A business case based on direct change management focuses on working backwards from a known situation B. The activities necessary to achieve B are well defined and each activity can be priced and the total costs calculated. The financial benefits of B are known, which creates a more or less certain image of the costs and returns for executives. A business case for indirect change management is based on multiple possible scenarios and a consequently unknown number of activities. There is less clarity in what and how many activities must be carried out and how much effort these activities will require. Consequentially, it is difficult to calculate the exact costs, making the business case and thus the justification for the change a difficult task for the change agent. Executives are often averse to this kind of uncertainty. Therefore, they have a tendency to prefer the seemingly more predictable direct change approach to the indirect one, even though the latter might be more suitable and less risky overall.

3.5.2 *Indirect change management*

Situations A and B are not always easy to specify in practice. As we shall see in Chapter 10, there are numerous questions that need be answered in order to accurately depict the current and desired state of a chain. When A and B are ambiguous, following the path of direct change management can be risky and may create a fundamental resistance to realising change. Indirect change management assumes that neither Situation A or B can be known in advance. Moreover, it assumes that the change agent has no means or authority (either formal or informal) to launch a change. When choosing the path of indirect change management, the starting point, Situation A and the desired outcome, Situation B are being determined along the way. In many cases, it takes time, extensive research and the work of many individuals before a problem can be discussed in terms of courses of action, preferences and choices. One well-known image of the relationship between problems, solutions and actors, and the likelihood that they will be linked to each other at the proper time and in the proper way is the metaphor of the garbage can (Cohen, March and Olsen, 1972). According to this model, actors deposit their problems and solutions in the 'garbage can' of a decision-making process. For the change management to be successful, the actors must combine all solutions and all problems in the same garbage can at the same time. The indirect approach requires that the change agent specifies precondi-

tions (time, budget, agenda, etc.), while the actual content of the change is conceived from the bottom up. While the path of indirect change may require coalition building, a common misunderstanding about indirect change management is the assumption that the primary goal is to involve as many actors as possible and make the process as open as possible. Such not the case, as the involvement of too many actors often leads to indecisiveness and weak compromises.

3.5.3 *Direct change management vs. indirect change management*

A direct change management approach presumes that the change agent directs actors towards a desired goal that has been set beforehand. Such a supposition is not always achievable in information chains. Roughly speaking, the greater the complexity (number of actors and the interactions between them), the smaller the chance of identifying a commonly supported Situation B. Therefore, the indirect approach is more viable in such a case. However, indirect change management is known for its difficulty in reaching closures. Such difficulty especially applies to moments in which an unambiguous decision must be made, since an indirect approach lacks the top-down hierarchy for decision making. To manage the threat of divergent visions with regard to Situation B, direct and indirect change management approaches should somehow be combined. The ideal setting is one that ensures an open enough change to utilize the interests and knowledge of all the actors and ensure that technical experts and management parties both have an appropriate role. At some point, a decision must be made on a definitive course from A to B. This implies that an indirect approach aimed at creating a common image of A and B will gradually become more direct and aimed at getting from A to B as A and B are determined. A combined approach needs to pay considerable attention to the shifting balance between top-down and bottom-up steering. Especially when shifting from the bottom-up initiation phase to the direct, top-down phase, the legitimacy of the hierarchical direction must be reinstated. Three examples of how to combine the direct and indirect management approaches are presented as follows (see e.g., Bharosa et al., 2011; Koffijberg, 2005).

1. Hierarchical intervention, while assuring leeway for steering by others than the change agent at the same time. While a direct 'engineering approach' provides direction, it is vulnerable when it does not sufficiently reflect the interests of the actors. Resistance may cause serious problems for the change agent, especially when the interests of the actors conflict. In addition, an engineering approach is unsuited to deal with the progressive insights of the actors. Leaving sufficient leeway for steering by others than the change agent, therefore, can reduce resistance and make sure that expertise is utilised at the same time. One example of providing such leeway is steering towards the achievement of particular goals rather than controlling the process. Time, costs, and quality standards are strictly formulated and enforced, but the way that actors operate within those pre-set conditions is left open to discussion and decentralised decision-making.

2. Timing and hierarchy. Decision-making processes in information chains can require precise timing. Problems and solutions may appear and disappear, preferences may come and go, and political pressure may increase and decrease over the duration of these processes. Thus, there is a time for hierarchical intervention as well as a time for cooperation and tolerance of diversity. What is the right time for hierarchical intervention? When will a hierarchical intervention have enough legitimacy to be accepted? Legitimate conditions for an intervention could include when an urgent decision needs to be reached, when earlier attempts to reach a consensus have failed, or a situation in which the majority is convinced but a minority still resists. In the last situation, the change management agent will need enough legitimacy to persuade the minority to agree and, if necessary, can compensate them.
3. Imposing a process hierarchically. This is a variant of 'hierarchical intervention while assuring leeway' that involves top-down implementation of decision-making rules. Such rules may involve the question of who will participate in making decisions and what role technical experts will have in the process. Within such rules, there can be room for a more agile approach (Boehm, 2002).

3.6 Control instruments for steering the change management process

A large collection of literature in areas such as project management, programmes and procedures has addressed control instruments that can be used for change management. Several best practices (e.g., Prince2 and Managing Successful Programmes) are available to guide change agents in the use of these instruments. Control instruments usually represent a group of techniques and tools that can be used either to mobilise parties towards a specific goal or to encourage them to undertake a desired action. In some cases, control instruments can also be used to do the opposite, for example, prohibiting actors from acting in a way that does not serve the established goals. We will discuss four types of instruments that are often used to steer change:

- Procedures
- Projects
- Programmes
- Process steering

Similar to the change management approaches discussed in the previous section, an assessment of the current situation A and the desired situation B (if known) determines the choice of instrument. Procedures and projects tend to be more suited to situations where B is relatively well defined. Programmes and process steering tend to be used when B is at least somewhat uncertain. Chapter 4 provides additional details on matching instruments to the characteristics of situations A and B. The scope of the present chapter is limited to an introduction to these instruments.

3.6.1 *Procedures*

The first control instrument is the 'procedure.' Procedures are characterized by pre-determined phases, which may have a minimum or maximum duration, and by a well-defined order of activities. Procedures are part of an organisational or policy framework; deviation from procedures may cause major damage. The procedure is the most rigid control instrument and the one that gives the clearest directives and instructions. Its objective is to ensure implementation of a change in the most efficient and effective way possible. It assumes that clear and specific agreements about applying the procedure at the chain level have already been made. Procedures are as tangible and concise as possible in order to avoid 'noise'—i.e. misconceptions and wrong information. Procedures are often derived from experiences. A procedure can only be used if it is clear what the effect of an action or product will be on a specific variable. This control instrument can be used 'off the shelf' and often contains an addendum giving a detailed description of the process logic (cause and effect), the steps that must be taken, the possible side effects, and how to mitigate them.

3.6.2 *Projects*

The second control instrument that is often used in implementing changes in chains is the 'project.' PRINCE2, a commonly used project management method, defines projects as: *"a temporary organization that is created for the purpose of delivering one or more business products according to an agreed Business Case*." According to this definition, a project is a non-routine, non-repetitive, one-off activity with a defined beginning and a defined end. There is a clearly defined goal with clear performance objectives, defined costs and a set duration. Each of these factors is associated with various risks. The identification of risks is important, as there is still some uncertainty about the activities to be undertaken. Compared to a procedure, this control instrument allows for a higher degree of freedom in the execution.

3.6.3 *Programmes*

The third control instrument is the 'programme.' Hedeman and Vis van Heemst (2011) define a programme as "*the whole of the coherent projects and activities in a temporary organisation aiming to realise one or more objectives that have been defined beforehand and which are of strategic significance*" (p. 163).

Two points from this definition should be noted: (1) multiple projects are involved in a programme and (2) the programme is aimed at realising strategic objectives. We explain both points next.

First, multiple coherent projects are involved in a programme. The outcomes of these coherent projects are generally required if the objectives of the programme are to be realised. The duration of a programme will therefore be longer than the duration of each individual project and some consecutive projects rely on the outcomes of the previous project in the programme. Considerable effort should be put into the coordination of the different projects, in order to avoid diverging and

incompatible project outcomes. This dependency on project results makes it difficult to determine beforehand when a programme will be completed. As a result, the parties involved must assess to extent the costs of changing the chain are justified by the benefits to be gained.

A second noteworthy point regarding programmes is their scope, which includes a focus on strategic objectives. These objectives are often recorded in a vision document and translated into a 'blueprint' of the desired situation. As was explained earlier in this chapter, the realisation of strategic objectives is often associated with radical changes in the chain, implying that various change variables are likely to be affected during the course of a programme.

3.6.4 *Process steering*

The fourth instrument, process steering, is a different approach to change compared with the others. The focus in process steering is on reaching consensus, either on a vision for the desired situation B or on the means to achieve situation B. In principle, process steering aims to address the array of interests and/or different perceptions of the involved actors. This means that goals, objectives, costs and/or process duration are not clearly defined, contrary to projects and programmes. Furthermore, bringing disagreement to light might be the actual objective of process steering.

Two types of process steering can be distinguished: direct process steering and indirect process steering. Direct process steering is an instrument that is used when A and B are known, but when there is no unified idea about how to get from A to B. Organising interactive processes makes it possible to agree on a series of incremental moves towards B and to reach consensus on the desired goal attainment strategy. These are two distinct yet complementary aspects of direct process steering, the first being a short-term course of action and the second a long-term strategy orientation. Figure 3.1. depicts the use of direct and indirect process steering in relation to the unfreeze-move-freeze model of change by Kurt Lewin (1951).

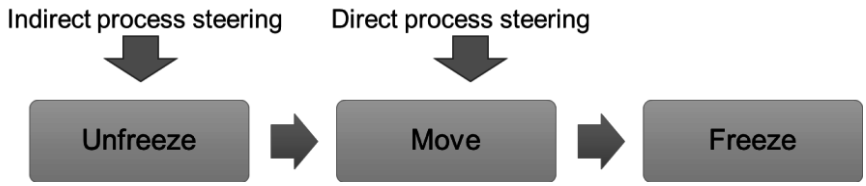


Figure 3.1 – Process steering approaches in relation to the unfreeze-move-freeze model of change

Indirect process steering, on the other hand, is an instrument used to reach consensus when a final target has to be defined. It is aimed at designing and managing a process that enables interaction between actors regarding their interests and proposed solutions. It stimulates the process such that new, common problems are revealed and joint solutions are found. De Bruijn et al. (2010) point out

the important learning effects of such interactive processes. Actors can acquire insights by jointly looking at the details of a problem. Such interaction also helps actors to understand the behaviour and interests of other actors. As a bonus, interaction reveals and solves the issue of jargon. Like specialists in so many other fields, those working on chain information systems are prone to use jargon. Jargon is a serious issue in information chains. Whenever different types of organisations collaborate the jargon issue is sure to surface. As discussed in the Chapter 1 of this book, the SBR solution introduces a lot of jargon such as taxonomy, generic infrastructure and interface service that are not obvious for all parties in information chains. In fact, jargon, under the best of circumstances, can make the SSC's intent unclear on first reading — and under the worst of circumstances, can discourage acceptance amongst actors. While clear documentation can help deal with the jargon issue, interaction between chain partners is key for addressing the jargon issue. Finally, interaction shapes bonds and helps create trust amongst chain partners, yielding a long-lasting commitment to change initiatives. When successful, process steering enables the use of more simple instruments like projects and procedures to realise change, which may have not been previously possible due to a lack of consensus.

3.7 Chapter conclusion

This chapter has offered some insights into the complexity of realising change in chains and has presented steering instruments that can be used to address this complexity. Given the interdependencies and the range of interests of actors within chains, it is typical and even likely that one or more chain parties will resist the change. This may lead to a situation in which reluctance to accept the change becomes a challenge, if not a threat of total non-acceptance. While we have underlined the paramount importance of acceptance in the change process, we have not discussed what needs be accepted (i.e. the change object), what factors influence acceptance, and what type of control is required.

Chapter 4 will discuss these important aspects in greater detail. In the introduction of this chapter, it was stated that Chapters 3 and 4 should be taken together. These chapters offer insights and present steering instruments to be used in addressing change management issues in information chains. Equipped with these tools, it is possible to better assess the situation and select the most suitable situation-dependent steering instruments to manage the change and meet the stated goals.

4 Steering Change in Chain Information Systems

Chapter highlights

- Why you should care about the interplay between technology and governance
- Mastering steering change for specific types of change in chain information systems
- Meeting the guy in the swamp

4.1 Introduction

The previous chapters have provided insight into information chains, their actors and their interdependencies. These interdependencies become particularly evident when changes are implemented in the underlying inter-organisational information system (or chain information system). This chapter deals with steering change in the chain information system. We define a change as a deliberate and purposeful action by one or more chain actors, meant to achieve a goal through the modification of one or more elements in a chain information system. As discussed in Chapter 2, there are several potential drivers for change—for example, enhanced performance goals, the desire to simplify or augment interaction between chain actors or changes in laws and regulations. Thus, chain information systems must cope with change on a continuous basis. There are sev-

eral types of change. Using the example of the SBR solution introduced in Chapter 1, changes can range from minor upgrades in the reporting software to the release of a new version of the national taxonomy.
Drawing on the concepts and insights provided in the previous chapters, Chapter 4 addresses the change steering question: how should a specific type of change be steered (referring to which change strategy and steering instruments to use) and by who (which change agents)?

Finding accurate answers to the change steering question was a substantial challenge faced by the actors tasked with implementing SBR in the Netherlands. Studies have shown that this question is also relevant for other types of information chains, but that there is a dearth of available guidance for addressing this problem (e.g., Tiwana et al. 2010, Markus & Bui, 2012). The main issues are the diverse range of possible changes that can occur within chain information systems and the difficulty in accurately identifying a specific change in practice due to the complexity of such a system.

A review of the literature reveals that the change steering question is not discussed in an integrated and comprehensive manner for chain information systems. While several research strands have indirectly considered the steering of changes across multiple public and private organisations, none have directly focused on it. Furthermore, despite an abundance of literature on underlying topics such as change management and IT management (Thiadens, 2008; Weil and Ross, 2005), their scope has primarily been limited to a single organisation. On the other hand, studies on inter-organisational information systems have generally focused on the drivers for such systems, system performance, and underlying components/technologies (Tuunainen, 1999; Kauremaa, Kärkkäinen and Ala-Risku, 2009). The literature regarding information chains (Grijpink, 2010) and chain management (Duivenboden et al., 2000) may provide food for thought, but fails to provide concrete guidance about what agreements should be made when making changes to the chain information system. Moreover, while best practices for IT management (e.g., ITIL, ASL and BiSL) and IT governance (e.g., COBIT, ISO/IEC 38500, CMM) are valuable, they often assume that the question of who should be involved in steering the change has already been answered.

The objective of this chapter is to offer readers a guide for addressing the question of who and how to steer change. To do this, we first consider the available research on steering change in a multi-actor environment. This will allow us to define the concepts and relationships involved. Supplementing this background with the challenges faced in the SBR case, we deduce some basic guidance for addressing the change steering question. This chapter is structured as follows.

- **Section 4.2** discusses the object(s) of change in chain information systems. Here, two dimensions of change—technology and governance—are acknowledged. This is important, as oftentimes only the technological dimension of a change is addressed while the necessary changes to the governance of the chain are ignored.

- **Section 4.3** highlights some essential questions on steering different types of change. To provide a simplified argument, we consider two end-points: Situation A (prior the change) and Situation B (after the change). We find that knowing Situation B and the dimensions involved in the change (i.e. technology and/or chain governance) determine how the change should be steered. Curious readers might want to skip forward to Figure 4.3.
- **Section 4.4** addresses the change steering question for changes in which the Situation B is known.
- **Section 4.5** addresses the change steering question for changes in which the Situation B unknown.
- **Section 4.6** includes a discussion of our guide for addressing the change steering question.
- **Section 4.7** closes the chapter by connecting the findings of this chapter to the SBR case.

This chapter introduces the main concepts behind steering change and instruments used to do it. While we use the SBR case to explain some of the complexities of the topic, Chapter 9 covers the SBR case in greater detail, revealing the current governance model for SBR in the Netherlands and how it addresses the change steering question. The governance model presented in Chapter 9 leans on the insights provided in the current chapter.

4.2 The interplay between governance and technology

As was repeatedly expressed in Chapters 2 and 3, chains are representations of the interdependencies between actors. Extensive coverage of this concept, both as a dependent and independent variable, can be found in the literature. One of the theories found in the literature is the 'contingency theory' (Donaldson, 2001; Galbraith, 1973; Gresov, 1989), which focuses on identifying contingents, i.e. factors that are fluid and affect one another. Two of the contingents identified for information systems are governance and technology[6] (Brooks, 2006; Sambamurthy and Zmud, 1999). We will first present these two contingents as separate, isolated dimensions, followed by a reflection on the interplay between the dimensions and what it means for steering change.

6 We sometimes refer to the architecture—or the structural blueprint—of a technology. However, references are also made to the architecture of a governance system (e.g. Gulati and Singh, 1998). In both cases, architecture refers to the structure of the design and will be used when we are referring specifically to the design of governance or technology configurations.

4.2.1 *Governance*

Governance is a 'coffee-table' concept, which in the literature is increasingly used to indicate a broad range of actions and structures. Because of the strong intuitive appeal of the governance concept, precise definitions are generally thought to be unnecessary (Lee, 2003). Politicians, board members, managers, architects, auditors and others, for example, all embrace this elusive concept of governance. As a result, when we identify governance as important factor in realising collective goals, it can remain unclear whether the reference is being made to organizational structures, administrative processes, systems of incentives and rules, procedures or philosophies. As we will be returning a number of times to this concept, it is important to accurately define the term governance. The approach we have chosen is a pragmatic one. We start with a brief review of some of the definitions found in the literature that capture the essential characteristics of governance and their importance. We then define the notion of chain governance and proceed with a discussion on what it means for steering change in chain information systems. Since our focus is on governance as it relates to information systems and information management, we refrain from discussing the generic, context independent explanations of the concept. For such an explanation, the reader can, for instance, consult Brown and Grant (2005) and Stoker (1998).

In the literature on governance in information systems, Peter Weill is often quoted. Weill (2004) provides the following definition for IT governance: "*specifying the framework for decision rights and accountabilities to encourage desirable behaviour in the use of IT*" (p. 3). This definition emphasises two key aspects of governance:

1. Specification of tasks and decision rights (as recorded in agreements) are crucial.
2. Governance must encourage the desired behaviour.

A study by Weill and Ross (2005) looking at hundreds of businesses in more than twenty countries concluded that governance is key aspect in gaining benefits from IT investments. The authors state: "the best-performing businesses stand out because of their carefully designed governance." Without formal governance, individuals are left to resolve isolated issues as they arise. Left un-steered, those individual actions often come into conflict, which can lead to problems.

Governance is clearly important, but what scope is appropriate? Markus and Bui (2012) discuss the scope of governance, stating that "*governance can address both mundane operational coordination (e.g., how open source software developers 'check in' new code) and high-level strategic coordination (e.g., where investment capital will come from, who owns the intellectual property, and the role of board members and senior executives in IT decision-making).*" (p. 164). This definition of governance covers a range of agenda items such as performance, resources, risks, compliance, value delivery and alignment. A common denominator for these items is that various mutually-dependent actors are involved.

Another approach to defining the scope of IT governance is to compare it to the scope of IT management. According to Weil (2004), "*IT governance is not about what specific decisions are made. That is management. Rather, governance is about systematically determining who makes each type of decision (a decision right), who has input to a decision (an input right) and how these people (or groups) are held accountable for their role*" (p. 3). In short, governance is about who makes the decisions, while management is about making and implementing the decisions. The well-known one-liner, "*steering, not rowing*" (Osborne and Gaebler, 1992), depicts the difference between governance and management.

Weill and Ross (2005) assert that effective IT governance always answers three questions:

1. What decisions must be made?
2. Who should make these decisions?
3. How are they made and monitored?

Once the types of decisions and the structure for making those decisions are mapped out, an enterprise must design and implement a coordinated set of governance mechanisms that managers will work with on a daily basis. Enterprises generally design three kinds of governance mechanisms:

(1) Decision-making structures – the organisational bodies and roles that locate decision-making responsibilities
(2) Alignment processes – management techniques for securing widespread and effective involvement in governance decisions and their implementation
(3) Formal communications – a clear understanding about how decisions are made, what processes are being implemented and what the desired outcomes are

The consensus view is that well-designed, well-understood and transparent governance mechanisms promote desirable IT behaviours and individual accountability. The research by Weil & Ross (2005) provides a framework by which to design governance mechanisms within a single organization. However, when looking at the inter-organisational governance of chain information systems, far less guidance is available in the literature. This does not mean that previous research has neglected the importance of clear inter-organisational decision-making structures. Indeed, previous work has often focused on shaping collaboration through information systems. However, it has, to a large extent, assumed that actors keep full autonomy over processes and shared systems.

In using chain information systems, autonomy is in part replaced by interdependence. Interdependence is laid down in agreements. In general, private actors in supply chains come to an agreement about how the chain information systems will be used. These agreements can be informal (implicit) and undocumented, or formal and documented. The informal approach is called 'virtual chain management,' as opposed to the explicit 'formal chain management' approach (Wit, Rademakers and Brouwer, 2000). As discussed in Chapter 2, the

use of inter-organisational information systems implies the loss of some degree of autonomy, at least when it comes to the decisions surrounding the design, application and adjustment of shared system components. In cases like SBR, where thousands of actors are depending on the chain information systems, informal agreements are not sufficient. Moreover, general administrative law dictates good governance by the public agencies that employ the chain information systems. For example, risks must be continually assessed and system outages cannot be permitted. Such a situation is where the change steering question arises.

So far, we can define chain governance as *the explicit agreements between actors about how to decide on the aspects*[7] *of the chain information systems that create interdependency between these actors*. Thus, the change steering question—which change agents should steer a specific change in a chain information system and which change strategy and steering instruments should they use? — essentially concerns the design of the chain governance. Chapter 9 will provide a comprehensive answer to this question. However, to fully understand the question and the answer, we need to first address a second contingent in chain information systems: the technology.

4.2.2 *Technology*

This section narrows in on the concept of technology as one of the dimensions of change in chain information systems. A number of scholars (Berg, 1998; Lamb and Kling, 2003) have asked the question: what is technology? The answers they provide are more different than one might expect, as there are a number of different schools of thought on this topic. For example, students from the school of 'technological determinism' view technology as an exogenous and autonomous development that shapes organisations and relationships (Fleck and Howells, 2001). They follow a narrow definition and reductionist view on technology, presuming that a society's technology drives the development of its social structure and cultural values (Zuurmond, 1994). On the other hand, supporters of 'structuration theory' (Brooks, 1997; Orlikowski, 1992) take a broad and holistic view on technology. The 'pervasiveness of technology'—the intertwining of technology with socio-political structures and processes—is one of the key ideas in this school. The school states that technology only has meaning if we consider its interaction with humans.

The following quote provides a view into this school's conceptualisation of technology.

---

[7]Elements of a chain information system that affect multiple actors such as the Netherlands Taxonomy, other chain specifications on the message level, process specifications, and the configuration of interface services.

> *"Technology is the product of human action, while it also assumes structural properties. That is, technology is physically constructed by actors working in a given social context, and technology is socially constructed by actors through the different meanings they attach to it and the various features they emphasise and use. However, it is also the case that once developed and deployed, technology tends to become reified and institutionalised, losing its connection with the human agents that constructed it or gave it meaning, and it appears to be part of the objective, structural properties of the organisations" (Orlikowski, 1992, p. 406).*

The intrinsic challenge in this debate is that it is not referring to a single technology that was created twenty years ago and evolved into what it is now, but about a stockpile of technologies, some of which date back several decades while others are brand new. Figure 4.1 presents definitions of technology from narrow to broad.

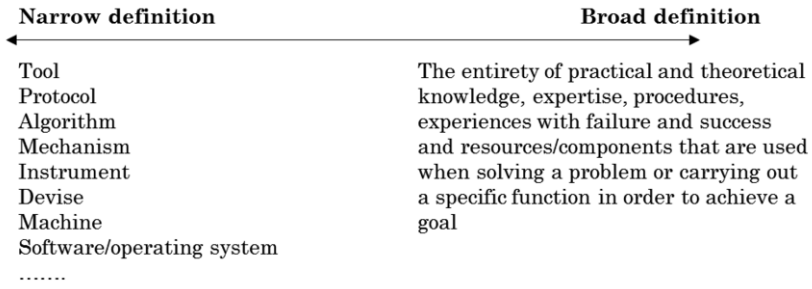


Figure 4.1 – Definitions of technology range from narrow to broad

As can be seen from these various schools of thought regarding technology, there is a certain degree of subjectivity about what technology is (Fountain, 2001). Perceptions of technology are based on a certain pattern of standards and values. Technology acquires meaning—in other words, its meaning is constructed—within that perspective.

Our purpose here is not to enrich the debate on what technology is. Instead, we will focus on the elements, or variables, of technology, allowing us to understand the object of change. Based on our experience with changes in chain information systems in the context of SBR, we have adopted a position closer to structuration theory, which recommends a broad view on technology, thus ensuring that pitfalls or key factors are not overlooked (Bruijn and Herder, 2009). The implementation of technology might not be successful if we fail to take into account the non-technological factors, including experience with the technology, knowledge of its operation, proficiency in using the technology, and its associated processes (Bauer and Herder, 2009; Clegg, 2000).

Against this background, we define technology broadly as *the entirety of practical and theoretical knowledge, expertise, procedures, experiences with failure and success, and resources/components that are used when solving a problem or carrying out a specific function in order to achieve a goal.*

4.2.3 *The notion of 'fit'*

The previous sections discussed two contingents of a chain information system: chain governance and technology. Staying in the theoretical framework of contingency theory, we presume that these contingents interact over time, influencing one other. This interaction is not without triggers and consequences. To understand the interaction and its consequences, we first need to understand the notion of 'fit.'

Nadler and Tushman (1980) provide the following general definition of 'fit': *"the degree to which the needs, demands, goals, objectives and/or structure of one component are consistent with the needs, demands, goals, objectives and/or structure of another component."* In this definition, 'components' are synonymous with 'contingents.'

Why is fit between contingents important? Scholars have extensively studied the notion of fit and its necessity (Galbraith, 1973; Gresov, 1989; Mintzberg, 1992). Most studies agree that a 'fit' between governance and technology is crucial, while a 'misfit' will lead to problems. Misfits can result in reduced effectiveness, reduced efficiency, non-compliance, or dissatisfaction in the users of the technology. Misfits often become apparent when modifying the components of an organisation or system. To avoid the negative consequences of a misfit, several scholars have presented mechanisms for 'fit-finding,' such as alignment, balancing, coordination, linkage and harmony. Over time, multiple models have been presented for fit-finding, including the strategic alignment model (Henderson and Venkatraman, 1993) and the so-called 'nine-cell model' (Maes, 2003).

A thought-provoking conclusion from the fit-finding literature is that finding a 'fit' is not a one-off exercise but a continuous process (Kooiman, 1993; Ashby, 1956). After all, information systems are continuously affected by changes in the technology and/or governance dimensions. Thus, maintaining fit within an information chain is a permanent challenge.

4.2.4 *Changes in technology can affect chain governance*

Technological changes can impact the dependencies within a chain. The introduction, for example, of a national taxonomy or a shared service centre will have implications for how decisions are made within a chain. If the existing chain governance is not suited to deal with these implications—which may be the case more often than recognised—this creates a misfit in the chain information system. Effective and efficient control of the 'new' technology might require modifications to the existing decision-making structure.

Figure 4.2 provides a simple representation of this interaction between chain governance and technology. In the diagram on the left of the figure, the chain governance triggers the need for change in the technology dimension. The right-hand diagram depicts the same situation, but where the change in technology, in turn, requires a change in the chain governance in order to preserve the fit.

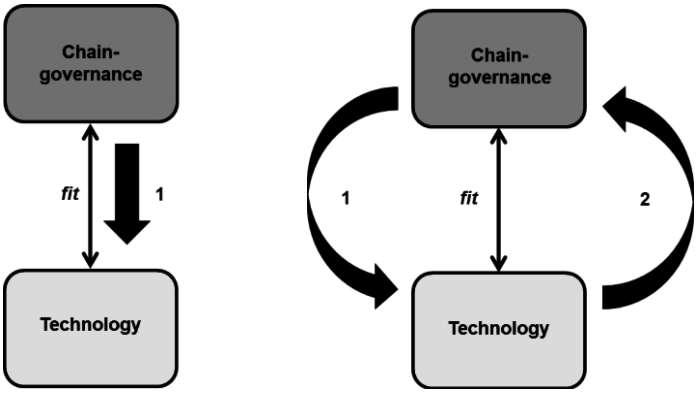


Figure 4.2 – A change may involve the technology (left) but may also require a change in the chain governance in order to preserve the 'fit' (right).

In the light of the interaction between technology and chain governance, we conceptualise the object of change—the chain information system—along two dimensions: technology and chain governance. Sometimes only the technology or the chain governance will be changed, but a change could also involve both dimensions. For instance, the introduction of a shared service centre by the Dutch government in 2009 represented a change in technology. However, it also meant that there was a new actor in the chain, thus creating new and altered dependencies among actors. Such dependencies are managed through agreements (Malone and Crowston, 1994), and the stronger the horizontal collaboration and vertical integration (due to the use of a shared service centre), the more important these agreements become. That is why the decision to use shared services for information delivery and pre-processing not only triggered a technology change, but a change in the chain governance as well.

It should be noted that aiming to create 'fit' also suggests some of the features of an appropriate chain governance. Chapter 1 stated that information chains with heterogeneous actors and information flows require flexible technology for shared facilities. Preserving 'fit' thus means that chain governance must also be appropriately flexible. In the context of SBR we have observed that aiming to preserve 'fit' is a continuous process of alignment that requires periodic evaluations to determine whether the chain governance remains adequate.

4.3 A closer look at two categories of changes

Drawing on Chapter 3, we consider a change as a movement from Situation A to Situation B. In the IT context, the terms often used are 'IST' and 'SOLL' (German for "is" and "should be," respectively). In the previous section, we described how a change involves at least two dimensions: technology and governance. Implementing the change requires steering on the part of the change agent. Determining *who*—which change agents—must steer a specific change and *how*—which change strategy and steering instruments should be used—was presented as the 'change steering question.' We will now discuss the two essential questions that determine who steers the change and how it should be done.

The first question is: what does Situation B look like? From Section 4.2, we can infer that this question entails looking at both the technology and chain governance dimensions of Situation B. Note that we have adopted a broad definition of technology. Factors such as practical and theoretical knowledge, as well as technical resources, thus play a role due to the requisite applications, infrastructure, functionality, architecture and specifications. Situation B, from the chain governance perspective, involves future agreements between actors. Thus, governance covers who will be involved in decisions on aspects that determine the relationships within the chain and how they will be involved. Situation B will either be known or unknown. Knowing 'B' means that:

- There is a clear picture of the technology that will be used.
- There is a clear picture of the future chain governance.
- Chain actors each have a similar picture in mind.

The second question is: which chain actors will be impacted by the change? Generally, a change within a chain information system will not affect all chain actors. The actors who are impacted are the ones needed to control the change. Thus, the chain governance in Situation B must always be reflected in the control of the change. There is a substantial correlation between the question of what 'B' will look like and the ability to answer which chain actors will be impacted by the change.

If Situation B is known forehand, the above pair of questions can be properly answered. Indeed, those actors who will experience an impact from the change are known and will at least be involved in controlling the change. Since B is known, each party will be able to determine the magnitude of the impact. In short, if Situation B is known, answering the change steering question is not necessarily a complex matter.

However, if Situation B is unknown, answering the second essential question—which chain actors will be impacted—is much more difficult. After all, it is not even clear which chain actors will be interacting with each other in Situation B. If Situation B is unknown, it is therefore difficult to offer chain actors—who may experience an impact—any degree of certainty about how much Situation B will resolve specific problems or contribute to their goals. Motivation to control the

change might therefore be low. In this situation, answering the change steering question can prove exceedingly difficult.

We therefore divide changes into two categories in terms of how the change is controlled. The first category is characterised by a known Situation B; the change steering question can be answered properly. The second category is characterised by an unknown Situation B. Answering the change steering question is tricky in this case, as there is no final state in mind, the actors that will be involved are partially unknown, and there is thus no clear path to get to Situation B. Such a situation has implications in how the change should be controlled. The dichotomy can be presented in a tree structure that we can use to classify changes. The second relevant distinction involves the two dimensions of change presented in Section 4.2, namely technology and/or chain governance. Finally, it is relevant to know whether or not the change is anticipated and repetitive. Together, this categorisation of changes yields the tree structure shown in Figure 4.3.

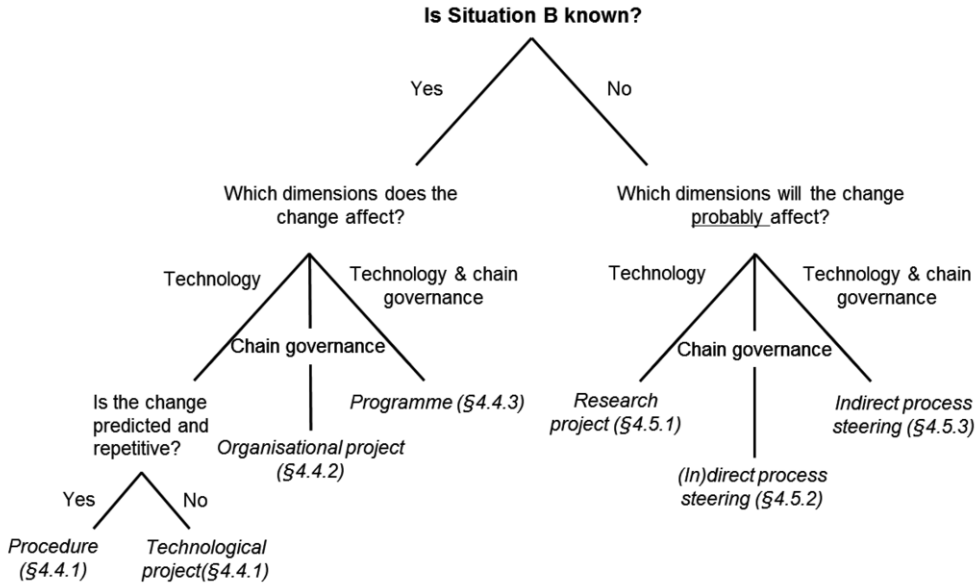


Figure 4.3 – Categorisation of changes using three questions to determine how the changes should be controlled.

As the tree structure depicts, the dimensions affected by the change cannot be established with absolute certainty when Situation B is unknown. Because of the need for fit between the technology and chain governance, the need for a change in the chain governance may only come about during a technological change. Similarly, the need for a change in the technology may only come to the fore during a change in the chain governance. We therefore state that a change will probably involve technology, governance, or both.

With the above categorisation of changes, we propose a guide for pinpointing the kind of change strategy and instruments needed for controlling a change. The following sections discuss each of the branches of the tree structure in Figure 4.3 in greater detail. In Section 4.4, we will deal with the category of a known Situation B, and how the change steering question might be answered in that case. In Section 4.5, we will deal with the unknown Situation B. Since addressing the change steering question is far more challenging in this case, we provide some guidance for doing so.

4.4 Answering the change steering question for a known Situation B

In the previous section, we deduced that a distinction should be made in terms of steering change between cases where Situation B is known and where it is not. This section focuses on controlling change in the first change category, i.e. where 'B' is known, and discusses the change steering question for this case. Changes are discussed in terms of their characteristics, the appropriate change strategy, suitable steering instruments, and the involvement of chain actors. Based on SBR, we will also give examples of the types of change concerned. We will also discuss acceptance of the change, expanding on the information presented in Chapter 3. The criteria for steering instruments and change strategies presented in that chapter will be applied to the changes features discussed here, yielding an appropriate change strategy and suitable steering instruments.

The changes discussed in this chapter include a foreseen and repetitive change in the technology, an unforeseen and/or infrequent change in the technology, a change in the chain governance, and a change in both the technology and chain governance. This section concludes with a number of points of attention for the changes discussed.

4.4.1 *Foreseen and repetitive changes in the technology*

Changes in the category of a known Situation B usually only involve the technology: the change is envisaged (e.g., in terms of frequency, moment and impact) and is repetitive in nature. These are also referred to as 'standard changes.' An example of a foreseen and repetitive change is the annual update of the Netherlands Taxonomy (NT). Every year, the government actors in SBR publish a new version that contains the data to be requested and the data definitions, which may have been, for instance, adapted to suit amendments to legislation and regulations.

The actors controlling the change apply direct change management as a change strategy. They want to take the chain from a known Situation A to a known Situation B. Expected changes must be implemented by means of a procedure, which includes highly concrete agreements about the process that must be completed to ensure a certain result. That is why a procedure—provided it has been set up properly—guarantees efficient handling of the change. The characteristics of this steering instrument were discussed in further detail in Chapter 3.

Which chain actors are involved and how, should be set forth in the procedure prior to the change. Officials at the operational level will always be involved in foreseen technological changes, as most likely will people at the tactical level. The division of tasks, responsibilities and authorisations is set out in the procedure. The procedure is embedded in the 'line organisation.' Unless there are escalations when the procedure is carried out, the strategic level does not need to be involved in the implementation of the change. Expertise will particularly come from actors in the technology field, including IT service managers, technical managers, application managers, data architects, process architects and/or people charged with information security, supervised by a change coordinator, if necessary.

As soon as B is known, acceptance and implementation can proceed more or less sequentially, in accordance with the procedure. A change process from the ITIL best practices can be a useful guideline for this step. The degree of complexity in the acceptance and implementation stages, and the duration of the process, depends on the impact of the change. Regardless of the impact of the change, the actors should be prepared for the change and be able to carry out the change thoroughly and in a standardised manner. The actors controlling the change can, as part of their daily jobs, work to obtain acceptance in accordance with the procedure and manage the final implementation of the change. The actors can start the implementation as soon as there is sufficient acceptance in the forum that functions as a change advisory board. If the responsible officials fail to achieve acceptance within a reasonable period, where the problems lie must be investigated and measures must be taken to remove barriers. In such a case, the issue of acceptance must be escalated to the higher level in the line organisation. The question that should be asked immediately is why the change is not in line with the expectations of the actors or why the actors are not prepared to bear the impact. There is probably more going on than meets the eye, which is what the relevant actors must discuss at a higher level.

4.4.2 *Unforeseen and/or infrequent changes in the technology*

Changes of this type only apply to technology and include unforeseen and/or one-off changes. This type of change is also referred to as 'non-standard changes.' An example of an infrequent technological change is the replacement of certificates, a technology that enables systems of sending and requesting parties to unambiguously identify the Digital Gateway. As security standards are continuously under development, replacement of certificates is required over time. One example was the replacement of SHA-1 certificates with SHA-2 certificates a number of years ago. Another example was the transition to a 'dimensional taxonomy,' which resulted from the decision to use the XBRL dimension specifications—a module of the international XBRL specification—for the Netherlands Taxonomy. The reason for this change was that the requesting actors needed to more precisely specify certain elements of a request (e.g., the turnover per region and per product). The change to the dimensional taxonomy enabled the actors involved to meet this requirement.

The actors controlling this type of change apply direct change management. They migrate the chain from a known Situation A to a known Situation B. Changes that fall within this categorisation should be handled using a technological project as the steering instrument. A project, in general, is defined as a one-off, temporary activity aimed at realising a clearly defined goal. The project is tailored to the characteristics of the change in question, thus incorporating the required degree of flexibility. The characteristics of this steering instrument were discussed in detail in Chapter 3.

The chain actors who will be affected by the change should be involved in the control of that change. The allocation of tasks, responsibilities and authorisations in technical projects is tailored to suit the project environment. The project governance setup depends on the actors that are affected by the change. It also remains within the framework of the current chain governance, since this type of change does not modify the existing chain dependencies. The project is controlled by a steering group and carried out by a project team. The tactical and, if deemed necessary, strategic levels, are represented in the steering group. The operational level is involved in the project team and likely the tactical level as well. The expertise within the project team is primarily technological in nature. It can include IT service managers, technical managers, application managers, data architects, process architects and/or information security staff. Most likely, a project manager or change coordinator supervises the project.

As the change is unforeseen, it is possible to encounter a lack of acceptance up front. This particularly applies when the scope of the implementation is wider than the business reporting chain where the problem resides. It is the project team's responsibility to ensure targeted handling of this acceptance problem. They need to find the specific obstacles in the knowledge-ability-motivation areas of the chain actors involved. The key is to examine how the project can obtain sufficient support for the change. The project team must understand the limits of their authority. On the other hand, they must take the liberty to conduct wider research. To assure actors that a solution is in everyone's interest, changes can sometimes be 'swapped' between the actors involved: 'if you scratch my back, I'll scratch yours.' The project team must discuss any proposal for such tactical steps at a level of control that is higher than the concerned problems. Giving serious thought to the implementation stage during the acceptance stage—as implementation follows acceptance—may help in gaining the support of the actors, for instance, by offering proper support during the implementation steps. If, despite all feasible actions taken, a change is not accepted, the project team should promptly return the assignment to the steering group and ask them to find a way to escape the deadlock. It may turn out that the proposed Situation B is not the solution. In that case, B can no longer be seen as a known situation.

4.4.3 *Changes in chain governance*

A change solely the in chain governance may occur because of external influences (a call for reorganisation, for instance) or to create a better fit between the technology and the chain governance (see Section 4.2). That is why this change type is characterised by one-off changes that are unique and focused on a specific result. At the time of this book's writing, one example of this type of change was the shift of SBR from a programme to a department (i.e. line activity) of Logius. A blueprint was already available that could be considered as the known Situation B. The technology used by SBR did not change. However, new forms of consultation were set up, in which requesting actors would meet with Logius and its supplier. In addition, there were more standardised documents with agreements between actors, and the professionals from the Logius line became more intensively involved in the SBR forums.

Actors can apply direct change management and the implementation of changes as change strategies. Given the one-off, innovative and finite character of a change in the chain governance, it should be controlled by an organisational project that is supplemented by process steering, if necessary. The characteristics of this steering instrument were discussed in Chapter 3.

The division of tasks, responsibilities and decision rights in organisational projects are tailored to meet the project's set objectives. As the existing chain dependencies are changing, the chain governance in Situation B (and in particular, the actors involved in it) should be sufficiently reflected in the control of the change. In other words, the actors that are going to control the change are not only those that are leaving but also those that will be involved in the future situation. Compared with Situation A ,it is possible that no changes in chain actors will be involved. However, it is likely that actors will be given other tasks, responsibilities and authorisations. It is also possible that new chain actors will come into sight and/or other actors will disappear.

The project is controlled by a steering group and carried out by a project team. In the steering group, the strategic level may be represented, while the tactical level surely is. In the project team, the tactical level is involved and likely the operational level as well. The staff involved in the project team and the steering group must have expertise in chain governance and organisational advising. They can be governance experts, enterprise architects and/or policy and organisational consultants.

The quickest way to achieve acceptance and implementation is to operate using the new roles that are aligned with the temporary project structure. However, it is important that the participating individuals are well trained for the roles they must perform.

4.4.4 *Changes to both the technology and the chain governance*

Changes of this type involve both the technology and the chain governance. An example of a change in both the technology and the chain governance is the use of generic building blocks in an information chain that before did not make use of SBR (a change in the technology). This means that the public and private parties of the information chain are also involved as a new SBR actor (a change in chain governance). Chapter 10 will elaborate further on this type of change by presenting the methodology for chain reengineering.

Combining direct and indirect change management is a suitable change strategy for this type. Refer to Chapter 3 for further detail regarding this strategy. A programme is a suitable steering instrument for this type of change. A programme consists of multiple coherent projects. Again, refer to Chapter 3 for a discussion of how a programme can be employed as a steering instrument. In a chain reengineering process, the programme may include a project to develop a taxonomy for the domain or a project to change the processes of the reporting and receiving actors. In addition, the participation of the new chain party in the SBR governance (see Chapter 9) will need to be realised. Along with the changes, the fit between technology and chain governance in Situation B must be guaranteed. Direct process control could be an additional change strategy for involving all the organisations and responsible officials involved in the transition to Situation B.

The allocation of tasks, responsibilities and authorisations in a programme are tailored to meet the specific needs of the chain parties. Because the existing chain dependencies are being shifted, it is important to ensure that the new chain governance (and in particular, the actors involved in it) will be reflected in the steering of the change. The programme is controlled by a steering group, in which the strategic level is inevitably represented (Hedeman and Vis van Heemst, 2011). The strategic, tactical and operational levels may be involved in the programme team. Involvement of the strategic and tactical levels is important in view of the input required for chain governance. In addition, technological expertise must also be brought in. Examples of such experts were provided for the previous change types. Programme managers and change managers are likely to be deployed as well.

Acceptance and implementation are tasks for the programme's subprojects. It should be noted that resistance from one project might interfere with another. Actors that have difficulties with the new governance may raise objections to the technology, as they may believe there is a bigger chance to win their case on the technology dimension. The programme management must analyse such problems to determine what is causing the actual resistance. Modelling arguments based on the knowledge-ability-motivation areas might prove helpful. It is also important for members of the steering group to sufficiently understand the technical and organisational components of the change. Otherwise, understanding any interference between projects and working towards acceptance will be chal-

lenging. Dependencies exist between the various projects in terms of implementation tasks. If one of the projects stagnates for some reason, changes to the other projects may be needed. The biggest possible pitfall is focusing too sharply on the technology and then failing to ensure closure of the organisational component. One strategy could be to successfully implement the accepted technology, thereby ensuring acceptance of the new governance. However, the concomitant risk to this strategy can be substantial, since the acceptance of the technology does not guarantee the acceptance of governance. Changing the chain conditions (see Chapter 3) might also be fruitful in achieving acceptance in the absence of an accepted governance.

4.4.5 *Points of attention when Situation B is known*

There are a number of points of attention for the changes discussed above. Firstly, various building blocks can be identified for any chain information system. Chain actors should be able to accurately determine which elements will be impacted by the proposed change in technology. Such a determination often proves difficult.

Secondly, this chapter makes a distinction between changes in technology and changes chain governance, or both together. Although it sounds entirely logical on paper, it can be extremely difficult to recognize such a distinction in practice. Thus, it is important for chain actors to continually reassess whether the chain governance remains unchanged as the process of a technological change progresses (particularly when considerable modifications are yet to be implemented). When altering the chain governance, reassessment of the technology aspect is similarly important.

Thirdly, maintaining a fit between the technology and the chain governance (see Section 4.2) under changing circumstances is easier when the actors comply with architectural principles (Bharosa and Janssen, 2010; Dickerson and Mavris, 2010). Architectural principles constrict the options of the actors, therefore leading to a design space in which changes are 'safe' and cannot harm the operation of the system (Clegg, 2000). Architectural principles will be discussed in further detail in Part B of this book.

4.5 Steering change when Situation B is unknown

The previous section discussed the change steering question when Situation B is known. In this section, we will explore the change steering question when Situation B is unknown. Once again, such a change may involve a change in the technology, a change in the chain governance, or both. It must be noted that even if the initial plan is, for example, a change in the technology only, such a result cannot be established with certainty. After all, some unforeseen technological aspect may yet be associated with unforeseen dependencies on the governance. Assuming that a fit between technology and chain governance is required, it may therefore be discovered during the course of the technological change process

that a change in the chain governance is also required. The reverse can also occur if a change in chain governance requires a change in the technology.

Controlling a change when Situation B is unknown is often problematic (see Section 4.3). We will explore the control of this type of change and, based on experiences from the SBR case, will provide some guidance for controlling change in three scenarios.

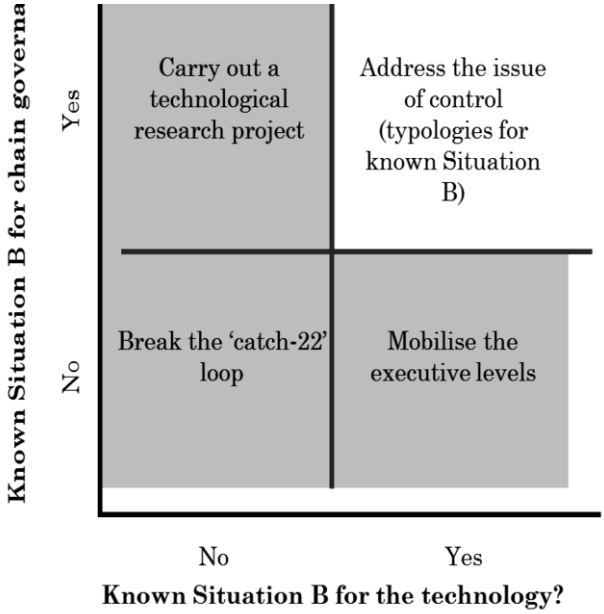


Figure 4.4 – Relationship between the scenarios and categories of change

The first scenario involves a change in the technology but probably not in the chain governance. Our suggestion in such a case is to carry out a technological research project (see Section 4.5.1). The second scenario involves a change in the chain governance but probably not in the technology. Our suggestion is to mobilise the executive level (see Section 4.5.2). The third scenario is a change that probably involves both the technology and the chain governance. Our suggestion is to act to avoid a 'catch-22' loop, where it cannot be determined what is to be changed first—the chain governance or the technology (see Section 4.5.3).

4.5.1 *Technological research project*

The technological research project should be used in cases that are likely to only involve changes to the technology, and where Situation B is unclear and/or not shared by all actors. At the very least, the chain actors should be able to assume that chain governance will not be involved in the change. An example of such a case could be a weakness found in the security protocols used for the interfaces.

Changes that only involve the technology are usually the most controllable of all the types of changes where Situation B in unknown. It is important to note that in this case, the governance in Situation B is known, and thus the steering is determined prior to the change. However, more information about the technology is required. In case of the example of a weakness in security protocols, the chain actors that use the interfaces are able to hold consultations and come up with a solution by investigating what technologies can be used to neutralize the weakness in security protocols.

A permanent point of attention for the research project is to determine whether the chain governance will remain unchanged and whether there remains a clear and shared picture of the chain governance. A combination of the following signals may indicate that a clear, shared picture of chain governance in Situation B no longer exists:

- The dialogue about the chain governance is dynamic and variable.
- Chain actors that are actively involved in the current steering are unaware of the relevance of their involvement or question their involvement.
- Chain actors that are not involved in the chain governance are making themselves heard and are looking for ways to exert an influence.
- Making decisions is virtually impossible, as there seems to be a lack of a joint sense of responsibility.
- There is a lack of follow-up to changes and/or actions that are agreed upon.
- There is a lack of available resources for agreed-upon changes.
- External pressure to change the steering actors arises.

Note that each of the above signals may also be caused by numerous other factors than the lack of a shared view of the change governance. The assessment of whether or not a clear picture of the chain governance still exists therefore depends strongly on the context. Thus, a degree of caution is called for when interpreting these signals.

During the research project, the actors must realise that they are providing a basis for a change that must be accepted by all actors involved and later be implemented. One predictor for a positive outcome is that there is some degree of insight into how acceptable the solution is for the actors and how the solution can be implemented. These criteria can be used to assess alternative B situations. By consulting stakeholders during the assessment of alternative B situations, the research project is already contributing to the achievement of acceptance and implementation, which can follow as soon as B is known.

4.5.2 *Mobilisation of control*

Mobilisation of control is used for changes that are likely only to involve the chain governance and where Situation B is not clear. In this case, there is, however, a clear and shared picture of the current technology, which is not expected to change in Situation B.

In the literature, such a case is known as an 'institutional void.' Hajer (2003) defines the institutional void as where "there are no clear rules and norms according to which politics is to be conducted and policy measures are to be agreed upon. To be more precise, there are no generally accepted rules and norms according to which policy-making and politics are to be conducted" (p. 607).

When translated into the context of change in chain information systems, this means that a change is taking place in a situation where agreements have not yet been made regarding what chain governance will look like in Situation B. An institutional void often occurs during the creation or redesign of chains and networks.

Examples of this can be found in The Netherlands, which is undergoing the decentralisation of national government tasks to municipalities. These tasks include social support, participation and youth care, and the change comprises a considerable modification to the chain governance in these chains. However, some of the technological solutions that are used for the implementation of the various laws (for instance, a law requiring systems that keep track of benefit payments) do not necessarily need to be changed as a consequence of the decentralisation. While it is known that the municipalities will be responsible for the execution of tasks, concrete agreements regarding the involvement of chain actors in decisions have yet to be made.

The key observation with this type of change is that the technology in Situation A and B is known. One example could be a party that wants to use the technology more widely. To effect this change, the party can attempt to mobilise the required support among actors through lobbying and 'selling' the envisaged Situation B. In the literature, such an effort is described as '*mobilisation coordination'* (Ven and Walker, 1984), or activities initiated by a single actor with a certain objective that requires support, collaboration or resources from a number of other organisations. This idea is comparable to the direct process control that was discussed in Chapter 3.

An approach to mobilise coordination is to deploy several acceptance and implementation rounds. The first round is fully focused on determining what Situation B will look like. The actors appoint transition managers who will draw up proposals and try to obtain acceptance for their designs. An ideal Situation B will be created gradually, through trial and error. As B becomes increasingly known, the actors constitute the first steps toward implementation. The programme can be further formalised in the second round as soon as the foundation has been laid and the direction in which actors are heading becomes clear. For the second acceptance and implementation round, steering should cover a broader scope and should be more sequential.

4.5.3 *Breaking the catch-22 loop*

We will next discuss the scenario involving change in which Situation B is unknown, and where the change will likely involve both the technology and governance dimensions. An institutional void and technological uncertainty are characteristic of changes in this type of scenario, which is similar to what is known in literature as a 'wicked problem' (Churchman, 1967).

In a report about the 'learning government', the Scientific Council for Government Policy (WRR) presented a critical discussion of the functioning of the government when solving social issues (WRR, 2006). The report emphasises that in the problems the government is faced with, simple direct control is often unsuitable. The council calls these issues 'wicked problems,' where there is still a great deal of uncertainty in terms of their nature, the resources available for a solution, and the targets to aim for. In addition, much scientific uncertainty exists in most of these problems due to a lack of validated knowledge.

One characteristic of 'wicked problems' is the existence of one or more 'catch-22' loop(s). This term, which comes from the novel *Catch-22* by Joseph Heller (1961), describes a situation in which an individual must perform two mutually dependent actions, with one action starting after the other one has been completed and vice versa. In relation to a change, a catch-22 means the following: A change, for which the technology in Situation B is still unknown, requires control by the chain actors who will be involved in the Situation B's governance, in order to make sure progress is made towards a known technology. However, the potential chain actors in B's chain governance require a known B technology in order to be motivated to set up the appropriate steering mechanisms. The problem of mutual dependency is that it is not possible for both the control of the change and the technology to move towards a known Situation B.

New technological developments—for instance, in information and communication technology (ICT)—are an important source of wicked problems in our society (Hoppe, 2010). Once new developments have taken place, there may still be uncertainty about the possibilities of the technology and there might be no consensus on how to evaluate the possibilities of technology. An example of a wicked problem is realisation of the Dutch Electronic Patient Record System, a nationwide system for exchanging medical records launched in 2008. The House of Representatives supported this system and passed specific laws that enabled its nation-wide implementation. Nonetheless, in 2010, Senate commissioned a shutdown due to the political and social concerns regarding information security, protection of privacy and the misuse of medical records by insurance providers.

The literature does not provide concrete guidelines for addressing wicked problems. For example, the WRR's report only discusses the consequences of these types of problems in relation to political decision-making. According to the council, handling wicked problems politically is not a matter of pushing decisions through, but requires encouraging social learning processes. This demands effort

from a range of involved actors, particularly those outside the government, to find out what exactly the problem looks like and to discover the frameworks from which decisions regarding an issue can be made.

Looking at SBR, the initial development and implementation can be seen to resemble the characteristics of a wicked problem. There was a desire to change, but no picture of the final way that the various chain actors would be involved (i.e. the chain governance). A vision of the technology and a sketch of the architecture quickly became available, but the technology in Situation B was still unknown. That situation was a catch-22, as described above.

In SBR, a breakthrough in the Catch 22 was created by moving towards a known Situation B with regards to the technology. In other words, first the solution moved towards credible (stable) usage, and only then did it progress towards the large-scale and multi-domain usage. The Tax and Customs Administration was able to make the business case for generically applicable system-to-system exchange and provide resources for it. Initially, the actors in the reporting chain started a few separate projects (see Appendix A) with the objective of jointly defining the technical specifications. A number of standards were already in place. Next, the SBR Programme was set up for further development and implementation of the building blocks. This programme also covered projects that focused on experiments or proofs of concept. A limited number of chain actors—a subset of what was finally to become Situation B's chain governance—were able to create the permanent possibility to continue with technological development, even without the final governance in place.

Parallel to this long-term process, which remains quite challenging in the absence of the final governance, a limited number of chain actors—a subset of those who will finally do the steering—have been focusing step by step on increasingly intensive and instruction-driven collaboration and control. This has ensured that the actors could gradually reach comprehensive agreements on how they would steer changes in Situation B. As the technology has matured, the challenge has shifted towards mobilising and setting up the management, as described in Section 4.5.2. Gradually taking the chain governance a step further at key moments has filled the institutional void.

For change steering processes that are similar to wicked problems, we will—with a degree of caution—provide some guidance. Looking at the SBR case, that chain actors were seemingly able to find paths to progress from unknown technology and chain governance for Situation B towards a scenario in which these became more clear. The SBR programme managed do to this by continuously focusing on the development of the technology. In general, defining the chain governance at least provisionally for Situation B situation during an early stage seems to be an alternative method, ensuring that a particular subset of the actors is made responsible for reaching a technological solution. This course is not simple either, as it requires administrative authorities or the policy-making government agencies involved to play a prominent role. An iterative approach between the two

extremes seems possible as well, as long as the chain actors continue to further develop either the technology or the setup of the chain governance for Situation B. The absence of a focus on one of the two dimensions, or the attempt to further the technology and chain governance at the same time, would likely lead to stagnation.

Furthermore, acceptance and implementation need to be handled iteratively. Various rounds of implementation and acceptance are required, in which the jigsaw is re-fitted each time. Meanwhile, pioneers can start implementing and working on acceptance of relevant stakeholders. This acceptance can be boosted by the initial implementations, and the steering can then be adapted to meet requirements. It is important that the actors involved continuously re-evaluate Situation B, as Situation B may change considerably during this process. A roadmap may be used as a focal point in the process. During the process, the actors who have implemented the changes may end up disappointed if Situation B has changed significantly in relation to what they had accepted and implemented earlier. Such may be the case if they had overestimated the benefits of Situation B or had not been aware of other relevant points (e.g., obligations in the new chain governance).

4.6 Discussion

In this chapter, we presented a guide for addressing the change steering question. We acknowledge that a few things have been simplified and other relevant factors have been left out. In addition, the following limitations indicate areas where further research is necessary.

First, we have only considered the change steering question from a contingency theory perspective. This enabled us to zero in on the fit between two important contingents in chain information systems: technology and chain governance. Other theories (including transaction costs theory and agency theory) would likely provide complimentary insights into additional change steering questions. Moreover, contingency theory does not restrict the number of contingents in a system. We have given two particular contingents—governance and technology—a central role in this chapter. Other contingents such as leadership, information position, culture and competencies of the actors involved have not received the attention they deserve.

Second, the relationships between the characteristics of a change and the criteria for applying a steering instrument are predominately based on one empirical case (SBR in the Netherlands). Further research is needed to confirm how effective the match between change types and steering instruments are in practice. Considering the increasing number of chain information systems and the associated volume of changes to be steered, we anticipate that more research—preferably with the goal of providing guidelines—will follow.

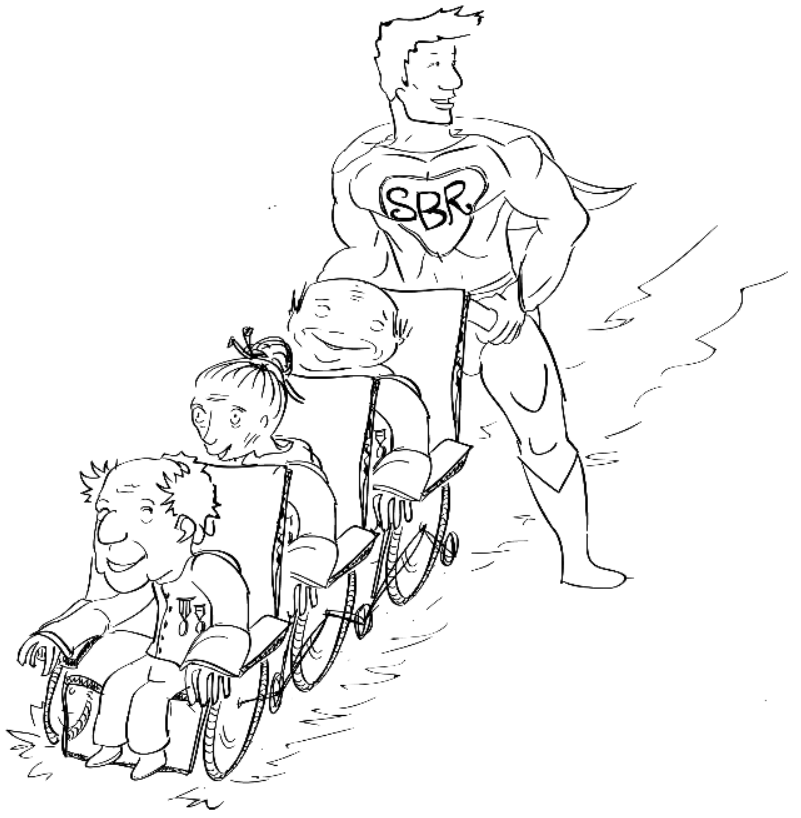
4.7 Chapter conclusion

This chapter provides a theoretically conceived yet empirically constructed guide for addressing the change steering question. Put simply, we argue that ascertaining the appropriate change agent and steering instrument depends on whether or not Situation B is known and on which dimension the change needs to take place (technology, chain governance, or both). Whether or not a change is foreseen and repetitive can play a role as well. These simple heuristics have allowed us to classify four change types and three change scenarios. We have provided answers to the change steering question for each type and scenario.

The SBR case was used to examine the change steering question. The examination of the change steering question using SBR gave insight into the task at hand for the parties involved during the development and realisation of SBR in the Netherlands. Although a vision of the required technology and a sketch of the architecture have been available since 2006, the actors lacked a clear picture of the technology and the chain governance for Situation B. This brings us to the illustration that introduces this chapter. This illustration depicts Baron von Munchausen. *Wunderbare Reisen zu Wasser und zu Lande: Feldzüge und lustige Abenteuer des Freiherrn von Münchhausen* (Bürger, 1923, from *Baron Munchausen's Narrative of his Marvellous Travels and Campaigns in Russia*) tells how Baron von Munchausen saved himself from certain death in a swamp without any help by pulling himself up by his hair. The folk tale symbolises finding a solution for an almost impossible challenge, in the absence of external assistance. In the context of chain information systems, we see that external assistance—in the form of guidance on steering change—is not always available. The SBR programme, for example, was able to pull itself out of 'the swamp' thanks to some actors that were able to provide a technical proof of concept in a reporting chain without an overarching chain governance. Their success helped break the catch-22, allowing them to assist the formation of a chain governance. Thanks to an established chain governance of SBR, and the fact that actors have a clear picture of Situation B, it has become much easier to provide appropriate answers to the recurring change steering question in the context of SBR.

Part B

SBR as a solution for information chains



5 Managing Data in Information Chains

Chapter highlights

- Understanding the difficulties of data specification and exchange
- Familiarise with XBRL
- Mastering the data life cycle

5.1 Introduction

The objective of this chapter is to provide guidance regarding the complexities of managing (i.e. modelling, specifying, exchanging and maintaining) electronic data in information chains. Accordingly, this chapter is divided into three parts that focus on the following topics:

- Part 1 – **Section 5.2** – Approaches to exchanging data. Separation of structure, form and content are addressed.
- Part 2 – **Section 5.3** – Specification of data. This section clarifies the notions of syntax and semantics, and highlights opportunities for their standardization using XBRL. As discussed in Chapter 1, XBRL plays a quintessential role in SBR chains.
- Part 3 – **Section 5.4** – How data specifications are developed and implemented in SBR chains. Focus is placed on the Netherlands Taxonomy and how it promotes compliance in information chains.

The chapter concludes with a brief reflection on what SBR chain actors have achieved in terms of standardisation and the opportunities that lie ahead.

Integrative case: Financial statements of Company B

Many countries have laws and regulations obligating companies to provide a clear look into their financial situation by filing annual financial statements with the business register of the specific country. The business register subsequently disseminates this information to the public. In the Netherlands, the business register is maintained by the Chamber of Commerce. In the course of doing business, companies commonly take great interest in the financial stability of their competitors. Let's say that Company A is interested in the cash position (including cash equivalents) of Company B. Company A can obtain the financial statements of Company B from the Chamber of Commerce. The financial statements will include a balance sheet that might look similar to the one shown in Figure 6.1. As this figure illustrates, the cash and cash equivalents of Company B amount to € 679.000, as of 31 December 2013.

Consolidated balance sheet
Company B Ltd.

	Ref	31 December 2013 *EUR '000*
Property, plant and equipment	5	1.210
Intangible assets	6	1.500
Inventories	7	378
Cash and cash equivalents	8	679
TOTAL ASSETS		**3.767**

Figure 5.1 – Consolidated balance sheet of Company B

Company B must send their financial report to the Chamber of Commerce via the generic infrastructure. The first step in this process is to convert the information on the consolidated balance sheet into digital data. This chapter provides a systematic explanation of how such data is transferred.

5.2 How is data exchanged?

Before discussing various perspectives on data exchange, it is important to make note of the difference between data and information. According to Ackoff (1989), data consists of processed or unprocessed values recorded by a person or organisation for multiple purposes. However, data only becomes meaningful and able to provide additional value when interpreted at the right moment, in the right form, by the right person. When we start interpreting data, it becomes information. In the integrative case in the box above, the value of "679.000" is data. Without any context, this data is useless. On the other hand, an example of information would be: "The cash and cash equivalents of Company B are € 679.000, as of 31 December 2013." The data now has context and can thus be considered as information.

To interpret data in such a way that it becomes information, data should have the following characteristics (McGilvray, 2008):

- Processability: the extent to which the data can be used to achieve the desired business transactions or outcomes;
- Comprehensibility: the extent to which documentation and metadata are available to aid in the correct interpretation of the data.

In this chapter, we consider data as facts that are in a format suited for communication, interpretation and processing into information, either by humans, automated systems, or both.

5.2.1 *Three perspectives on data exchange*

Organisations face numerous obligations to provide data to requesting parties. Requesting parties can be individuals, private organisations or public agencies. Reporting obligations are formed based on three perspectives: the reporting perspective, the transaction perspective and the policy perspective. These perspectives are briefly explained as follow:

1. The **reporting perspective** obligates organisations to provide information to justify their activities to a variety of parties, including supervisory bodies, shareholders, credit providers, and society as a whole. An example would be data requested by the Tax and Customs Administration to determine the amount of income tax to be assessed.
2. The **transaction perspective** obligates organisations to provide information required to complete a transaction. For example, an organisation is obliged to provide its bank account number on an invoice.
3. The **policy perspective** obligates organisations to provide information that allows public agencies to determine the effectiveness of their policies. In most cases, the public agencies request targeted aggregate information, or high-level information that is composed of a multitude or combination of individual pieces of information. For example, Statistics Netherlands requests various statistical reports from a multitude of local organisations in order to prepare a statement on development in the Netherlands as a whole.

Each perspective involves an information chain in which information is exchanged between at least two parties: the reporting party and the requesting party. However, most information chains include multiple parties, each having specific roles in the chain, such as businesses, intermediaries, agents, and requesting parties (i.e. public and private agencies). Figure 5.2 provides a graphical representation of the business information chain. It shows how various kinds of information exchange can take place at multiple aggregation levels, each of which may involve a number of organisations.

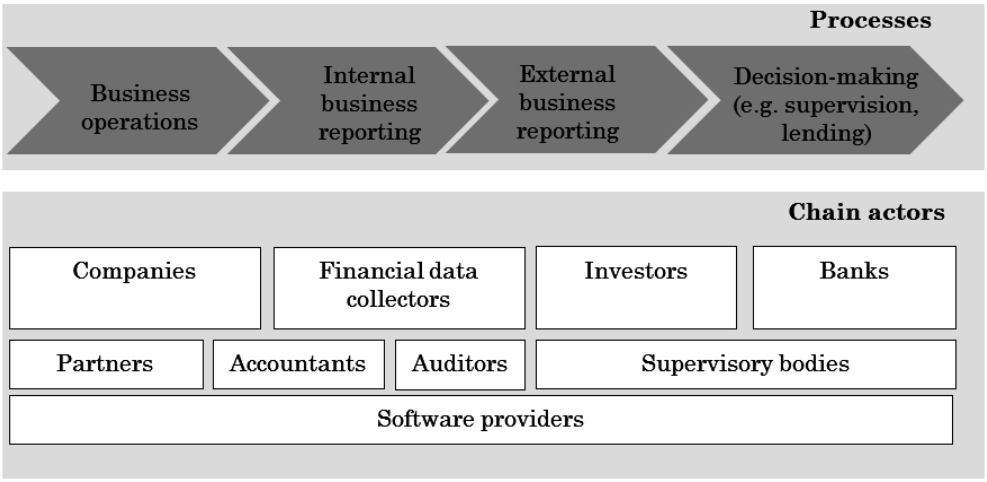


Figure 5.2 – Business information chain (based on Hoffman & Watson, 2010)

An efficient exchange of data includes the request and transfer information for the lowest possible operational cost (Nijsen, 2003). Efficient information chains benefit from the digitisation of data delivery. To achieve efficiency, the data should be obtained only once from the source. This ensures that the same data does not have to be re-entered and that various requesting parties do not need to request the same raw or derived data (or parts thereof) from the organisation more than once. Grijpink (2010) calls this 'chain computerisation,' or the creation of an information infrastructure for automated information exchange and processing between organisations within an information chain.

Organisations may opt for electronic processing of information rather than processing done on paper, via web forms or by other means. According to Arendsen (2008), reasons for the electronic processing of information include the following:

- The short response times required by chain partners.
- The need for a reliable and provable process of exchange/processing.
- The high frequency of message exchange.
- The large number of messages exchanged.

In addition, a few other reasons for electronic processing that can be distinguished:

- Cost savings when creating messages.
- Reduced transaction costs[8] for the information exchange (for a given set of requirements).
- Reduced recording and handling costs (physical archive vs. disks).

[8] Transaction costs are the costs that are incurred for fine-tuning the various links in the production chain (den Butter, 2010).

- An increase in productivity, such as shorter transaction times and improvements in processes.
- Avoiding redundancy in the chain (not entering the same data multiple times).

The above-mentioned benefits are generic and are mainly focused on potential cost savings in processing, storing, transmitting and sharing data. Both the reporting and the requesting parties can achieve these benefits.

Arendsen (2008) argues that there is one critical condition for harvesting the benefits of electronic message exchange: the integration of internal automated information systems. This condition is usually not met in the exchange of 'digital paper,'[9] which we do not believe can be regarded as proper electronic data exchange. In this chapter, we will use the definition of electronic data interchange given by Hansen and Hill (1989): "*the movement of business documents electronically between or within firms (including their agents or intermediaries) in a structured, machine-retrievable data format that permits data to be transferred, without rekeying, from a business application in one location to a business application in another location*" (p. 405).

This definition of electronic data exchange emphasises the significance of 'structured data.' This type of data can be identified as 'structured' since it is organised according to a certain structure. Structured data usually reside in databases, and can include, for example, specific information stored using a methodology of columns and rows. Data expressed in eXtensible Markup Language (XML) documents, which contain highly hierarchical and recursive structures, can also be considered as structured or semi-structured data. Structured data is searchable by data type, can be understood by computers and can be presented efficiently to human readers. Unlike structured data, non-structured data does not have an identifiable structure. In practice, non-structured data is often exchanged by means of 'digital paper.'

5.2.2 *Separation of structure, form and content*

When exchanging data electronically, structure, form and content are often separated. While the content is the key attribute, the data exchange benefits from a standardised structure, and the content's form is mainly useful for human interpretation. This separation has six advantages:

- Efficiency: only data needs to be sent. Sending the structure is not necessary. This is especially beneficial when receiving thousands of reports.
- Fixed data: the requesting party can precisely prescribe which data they want to receive. The reporting party only needs to fill in the data, without

[9]Digital paper can be described as digital files that do not provide any interactive operability. Information in these files cannot be processed by computer systems. For example, files in Microsoft Word or Adobe PDF format that merely contain information, but no connection to other files or systems.

having to modify the structure or add concepts, since the requesting party provides the structure.
- Flexibility: when a requesting party wants to change the structure of a report, the data in the report might not be affected. As a result, software suppliers do not have to adjust their software for every new format.
- Styling: a consistent style can be achieved when content is separated from form (Bodnik, 2013).
- Portability: the data is portable across heterogeneous systems (Oracle, 2014). Reuse of the data is therefore possible in other domains.
- Security: changes in files are difficult to identify when structure, form and content are combined in one document.

Because of the advantages of separating structure, form and content, it is considered a best practice in electronic data exchange. The practice is also a key assumption for the following section, in which we will discuss the theory behind specifying data.

5.3 How is data specified?

Semantic and syntactic interoperability are important preconditions for the digital exchange of data, especially for the purpose of horizontal S2S integration. This section focuses on both semantics and syntax.

5.3.1 *Semantics*

When organisations exchange data, it is important to make sure that the meaning of the data is correctly transferred to and interpreted by the receiving organisation. This requirement is addressed in the concept 'semantics' (Floridi, 2011; McComb, 2003). Semantics is an abstract concept and is therefore subject to various interpretations. In the context of data exchange, we will use the description given by Ouksel and Sheth (1999), who state that semantics attempts to map objects from a model onto the real world. In this context, it focuses on the issues that involve human interpretation and on the meaning and the use of data or information. Therefore, the term 'semantics' is used in situations that involve a potentially large set of expressions whose common objective is to represent some domain of the real world.

In order to map objects onto the real world, definitions of expressions should be provided so that the meaning of the expressions becomes clear. Defining is explaining what an expression means and the definition is the outcome of this explanation (Longworth, 2006). Defining can thus occur in different ways. For example, providing different characteristics of an expression, such as relationships between expressions, is also a way of defining and can help to clarify the meaning of an expression. Furthermore, when the meaning of a concept is transferred to another party, one must also make sure that this concept is used correctly. That is the subject of pragmatics. Semantics explain the meaning of an expression, while pragmatics explains how this expression is used in practice. Carlston (1996) described the difference between semantics and pragmatics as follows:

"the subject matter of semantics is linguistic meaning, that is decoded content, while the domain of pragmatics is all those additional processes which must be carried out in order to arrive at the speaker's intended message" (p. 306). In this chapter, semantics is broadly interpreted to include the pragmatics, as well as all kinds of expression characteristics and relationships between expressions.

Categories of semantics can be differentiated to determine whether systems can exchange and process information automatically According to Uschold (2003, p. 5), three questions about semantics need to be answered to determine the category of semantics:

1. Are the semantics explicit or implicit?
2. Are the semantics expressed formally or informally?
3. Are the semantics intended for human or automated processing?

On the basis of these questions, Uschold (2003, p. 5) categorises semantics into four types:

1. Implicit
2. Explicit and informal
3. Explicit and formal for human processing
4. Explicit and formal for automated processing

These types can be represented in a semantic continuum. At one extreme, there are no explicit semantics at all for the things people have in mind when using certain terminology. The other extreme is a formal and explicit semantics that is fully automated. Figure 5.3 illustrates this continuum. In reality, the boundaries between the categories are not always evident and there can be intermediate forms of semantics within this continuum.

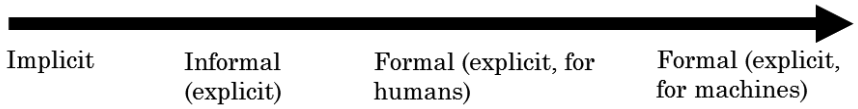


Figure 5.3 – The semantic continuum (Uschold, 2003)

Implicit semantics

In simple cases, semantics are merely implicit. This implies that the meaning of a concept is derived from common concepts for which there is human consensus. However, the exact meaning of a concept is not recorded or stated anywhere. One downside of implicit semantics is ambiguity, which leads to possibility of people having different ideas about the meaning of a concept.

Informal semantics

A little further along the continuum, semantics are explicit and expressed informally, for example by means of a textual description. Like implicit semantics, informal semantics mainly regard human use. After all, machines can only make limited use of informally expressed semantics due to the complexities associated with the human language. The disadvantage of informal semantics is that two different implementations of informal semantics do not necessarily need to be

consistent and congruent, allowing for subtle differences between implementations. This may lead to problems when interoperability is required or when implementations change.

Formal semantics for human processing
Slightly further along the continuum, semantics are made explicit by means of formal language, though this explicit formal language is only intended for processing of information by humans. Examples are formal documents or important formal specifications of certain concept meanings. Formal semantics for human processing help to eliminate ambiguity in concepts. However, errors are still possible because of human involvement.

Formal semantics for automated processing
The final type of semantics is explicit and formally specified, and is intended for automated processing of concepts by computers. When new concepts are identified, their meaning can be derived automatically. In addition, combining data can lead to new information that can be used for a variety of purposes.

In the context of electronic data exchange, we argue that formal and explicit semantics are more suitable than informal and implicit semantics. After all, data processing requires unambiguous interpretation of data, for which explicit and formal semantics is best suited. This means that the data needs to be well organised. The following section discusses various ways to approach the organisation of data to allow for the utilization of explicit and formal semantics.

5.3.2 *Syntax*

Unambiguous interpretation of data requires unambiguous meanings of concepts as well as a common language: the syntax. Syntax can be viewed as the collection of agreements made between parties to specify how data is presented using letters, figures and/or other symbols. Consider, for example, the ISO date notation in which it is agreed upon to format all dates as CCYY-MM-DD, where CC, YY, MM and DD, each consist of two digits indicating the century, the year, the month and the day, respectively.

Syntax focuses on the shape or structure of the data. Here, open exchange formats such as XML play an important role in structuring data. The following requirements are often imposed on a syntax:

- The syntax must use an open standard, which avoids dependence on one or more suppliers.
- The syntax must facilitate semantic standardisation in order to define data in an unambiguous way.
- The syntax must allow users of the data to render the data in any composition they want.
- The syntax must improve the reliability and controllability of data flows and reporting processes.

- The syntax must ensure efficient working methods, for instance by providing data from information systems for checking, analysis, and monitoring.
- The syntax must reduce the costs of manual and automated interfaces between various systems, therefore reducing the total cost of providing information.

From the above requirements, it can be seen that syntax and semantics are two intertwined concepts. If "2012-01-31" represents a date, this is not only syntactically correct—meaning it complies with the agreement to format dates as CCYY-MM-DD —but is also semantically correct: the date exists. A date such as "2012-02-30" would be syntactically correct but semantically incorrect as the 30th of February does not exist.

The requirements imposed on the syntax could also be enhanced to ensure that a row of symbols representing a date will only be syntactically correct if they also represent a meaningful date. The degree of precision in syntactic rules depends directly on the convenience it obtains in automated information processing. If the syntactic agreements are formulated in a precise enough manner, such that any date string can only represent an existing date, and if parties comply with these agreements, no further checks on the compliance of these agreements would be required.

In this text, we use a broader definition of syntax than the common definition: syntax is defined as the collection of agreements made between parties to specify how data is presented through the use of letters, figures, and/or other symbols. In this chapter, syntax also refers to the rules and principles that compose the language structure. Syntax is used as a generic term for all the rules regarding how data is written down in a language. The distinction between semantics and syntax is important when discussing methods for organising data.

5.3.3 *Realisation of semantics: approaches to data organisation*

In the first part Section 6.3, we stated that the unambiguous interpretation of data requires concepts to be defined unambiguously. According to Uschold (2003), there are two methods to accomplish this: (1) the simple method and (2) the specification method. Both methods are explained as follows.

The simple method—and probably the most commonly used method—is to ignore the problem. In this case, the organisation assumes that the terminology used has the same meaning for other organisations. In reality, organisations cannot assume that other organisations use the same terminology. Even when that is the case, it cannot be assumed that concepts will have the same implications. A good example of such a situation is the concept of profit, which is used in corporate income tax declarations and in financial statements. However, the Tax and Customs Administration uses a different definition for 'profit' in corporation tax

declarations than organisations use in their general-purpose financial statements. It is clear that a solution must be found that enables organisations to state exactly how they interpret a concept when communicating information.

The second method mentioned by Uschold (2003) implies that organisations must indicate which concepts they use and how these concepts are interpreted. For this purpose, organisations can use a specification method that organises concepts and their associated relationships. Therefore, the meaning of concepts must be encoded into a formal language, also known as syntax. The meaning of concepts is then modelled based on the relationships and attributes of the concept.

An organisation may use various approaches to organise its concepts and their associated relationships. Possible approaches to organising data are the use of controlled vocabularies, taxonomies, thesauruses and ontologies. These approaches are explained briefly below.

Controlled vocabulary
A controlled vocabulary is a list of explicit terms that is controlled by, and available from, a controlled vocabulary registration authority (Pidcock, 2002). A controlled vocabulary does not necessarily need to specify any definitions. It may just be a set of concepts that the parties have agreed to use, having definitions that are assumed to be known by all parties. However, terms in a controlled vocabulary are generally defined explicitly. The degree of detail of these definitions depends on the nature and scale of the data exchange. The controlled vocabulary registration authority must monitor the definitions of the concepts in a controlled vocabulary and should make sure that they are unambiguous and non-redundant.

Taxonomy
A taxonomy is a collection of controlled dictionary definitions that are organised in a hierarchical structure (Reimer, 2001). Each term in a taxonomy is involved in one or more parent-child relationships with other concepts in the taxonomy. A taxonomy adds meaning to concepts by using hierarchical relationships. A traditional taxonomy often assumes a generalisation/specialisation relationship, which approaches one concept as a specialisation or generalisation of another concept. Nowadays, the word 'taxonomy' is also used to refer to other types of hierarchies with different definitions for the relationships (Pidcock, 2002). When a taxonomy has drawn up a variety of carefully defined definitions for a hierarchical relationship, it can almost be seen as a version of an ontology.

Thesaurus
A thesaurus is a collection of controlled vocabulary concepts represented by a specific network structure. This implies that a thesaurus can contain hierarchical, equivalent and associative relationships (Pidcock, 2002). The semantic expressiveness of the associative relationships in a thesaurus varies widely.

These relationships do not necessarily need to have an explicit meaning, other than that two concepts are related.

Ontology

The term 'ontology' is regularly used to refer to a controlled vocabulary, a taxonomy, a thesaurus or an ontology. This follows from Gruber's (1993) definition of an ontology as "an explicit and formal specification of a conceptualization" (p. 1). This definition was extended by Ehrig (2006) to become: "an explicit, formal specification of a shared conceptualization of a domain of interest" (p. 12). This generic definition can easily lead to confusion, but becomes clearer when split up into multiple parts. In the context of Gruber's paper, a 'conceptualization' is an abstract model of how people think about various aspects of the world (generally limited to a specific subject). An 'explicit specification' implies that the concepts and relationships in the abstract model are given explicit names and definitions. A name is a label for a concept. Definitions are given in the descriptions of the concept meanings or in the relationship between concepts. A 'formal specification' is a concept is expressed in a language with formal characteristics that are properly understood. Formalising these characteristics is an important way to eliminate ambiguity. Finally, 'shared' means that it must be possible for different applications and communities to use an ontology (Uschold, 2003).

An ontology can therefore be considered a controlled vocabulary that is expressed in an ontological representation language. Such language has a grammar to allow vocabulary to be expressed in a meaningful way (Pidcock, 2002). The grammar imposes formal restrictions on the way the vocabulary concepts can be applied together.

In practice, the differences between a controlled vocabulary, taxonomy, thesaurus and ontology are not always easy to determine and depends strongly on the circumstances in which they are used. Pidcock (2002) states that taxonomies and thesauruses link controlled vocabulary concepts to one other using hierarchical, equivalent, and associative relationships. They do not contain explicit grammatical rules about how these controlled vocabulary concepts should express anything meaningful. However, an ontology does.

According to Pidcock (2002) the most important similarities between these approaches are:

- They are methods that help structure, classify, model and represent concepts and their associated relationships for describing a specific topic.
- They aim to create agreement between communities in terms of a mutual terminology and ensure that the terminology is used in the same way.
- There is a set of terms that a community decides to use in order to refer to these terms and relationships.
- The meaning of the terminology is specified to some extent and in some manner.

The key differences between the approaches involve the following:

- The degree of meaning that can be specified for each concept
- The notation or language used to specify the definition
- The purpose for which it is used, as all approaches have different, but overlapping, applications.

An example of the difference between approaches
A controlled vocabulary may, for example, contain the term *Cash and Cash Equivalents*. A taxonomy may state that *Cash and Cash Equivalents* belongs to the genus Current Assets, of which Assets is the parent. A thesaurus may state that *Cash and Cash Equivalents* does not have a synonym, and that 'Bank overdrafts' is the opposite of *Cash and Cash equivalents*. The ontology may state, using a particular grammar, that *Cash and Cash Equivalents* is a compulsory element of the Balance sheet, that cash equivalents have a short-term investment from less than 12 months, and that everything that is cash or easily convertible to cash is included in the term.

For the purpose of electronic message exchange, organising the concepts from a controlled vocabulary is extremely important in order to create formal and explicit semantics. In the context of this book, we will use the term 'taxonomy' because the relationships are, to a large extent, hierarchical. Moreover, we will focus on the organisation of concepts without specifying a language—or syntax—to express the concepts in. In our opinion, an ideal syntax should not impose requirements on the approach adopted for organising the concepts.

The development of a conceptual taxonomy is an activity that models the information needs of requesting parties in a natural manner, without considering the restrictions that are imposed by a syntax or that result from the implementation method. While this concept was deliberately chosen as a starting point, we are aware that it will not always be sustainable in practice.

5.3.4 *Standardisation of syntax: the development of open standards*

Section 5.3.2 states that a syntax focuses on the form or structure of data. The most important developments in this context relate to open standards for data exchange. According to the IDABC (2004), standards are considered to be 'open' if they have the following characteristics:

- They are created by means of a decision-making procedure that is accessible to all interested parties.
- They are controlled by a non-profit organisation.
- They have been published and are freely available.
- They are royalty-free and there are no restrictions on use.

The use of open standards has numerous benefits, such as a considerable choice of supporting software, a broader sales market, and a reduced likelihood of vendor lock-in, where a customer is dependent on one vendor's services and not able to switch.

Electronic messages are the containers of the data that is exchanged. This data must be defined in a structured manner and must be recorded to ensure that it can be exchanged independent of internal data format. Two well-known international standards are available for structuring data and messages:

- EDIFACT, the Electronic Data Interchange for Administration, Commerce and Transport, is a formalised and machine-readable language that has been used by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) to standardise a large number of electronic messages. EDIFACT messages are based on international, normalised data elements. They use a syntax that was designed during the '80s to yield the smallest files possible.
- XML, or eXtensible Markup Language, is a standard that was developed at the end of the '90s by the World Wide Web Consortium (W3C) in order to store and send data via the Internet. XML is a markup language that makes it possible to represent structured data as plain text. XML defines a set of rules for encoding documents in a format that can be read by both humans and machines.

From the 1980s onwards, computerised information systems have been increasingly used to support commercial relationships between organisations. Electronic message exchange was initially introduced as an instrument for optimising logistic processes (Arendsen, 2008). As part of the customer-supplier relationship, the ordering process and stock process were often electronically linked by the EDIFACT standard. Given the relatively high complexity and costs of technical infrastructures at the time, the introduction of this form of business-to-business integration (B2Bi) primarily occurred in large organisations (Hofman, 2003).

The Internet, or the worldwide web (WWW), has led to new standards for differentiating the presentation and structure of data, such as the markup languages HTML and XML. As a consequence of the rise of the Internet around 2000, XML became the most frequently used syntax for message exchange. These new standards also had consequences for EDIFACT. The content-based (i.e. semantic) standardisation still applied, but many software applications had problems with the syntax. XML/EDIFACT thus came about, combining the vocabulary and grammar of EDIFACT with the syntax of XML.

The emergence of XML has led to the creation of numerous controlled vocabularies and standard messages based on them. There are various national and international standards, each focusing on a specific area. For example, there are standards that support a specific process, such as the Universal Business Language (UBL), which contains standardised electronic documents for purchasing, transportation and sales processes. Other standards focus on a specific branch of business, such as the Dutch Insurance Data Network.

The choice of appropriate standards is complex because of the large number of options. The area of semantics and the required syntax (based on XML) is very

important when choosing standards. Each standard has its own community and adoption rate, which in turn determines the availability of automated solutions. Policy makers must make sure that their choice is based on the needs of the requesting parties and the availability and support of a suitable standard with the right features to fit into the domain.

Selecting an international open standard is an obvious choice, as they are widely supported by software, knowledge about them is widespread and they are freely available without licensing costs. A local profile such as the one used in the Netherlands, specified for the country's own legislation and regulations, is often created when international standards are applied.

5.3.5 *XBRL – standardisation of both syntax and semantics*

5.3.5.1 Background

The starting point for electronic data exchange was XML (eXtensible Markup Language), a markup language that makes it possible to represent structured data as plain text. XML is suitable for storing and sending data via the Internet. It defines a set of rules for encoding documents in a format that can be read by both humans and machines. XML is an open language, in which data elements can be created.

To facilitate large-scale automatic processing of documents, the flexibility of the structure in an open language needs to be restricted. Otherwise, every reporting party will specify metadata in their own way. For example, Person A might report a value of 20 with the metadata 'euro' and 'without decimals,' while Person B might report a value of 20 with the metadata 'euro' and 'on a specific date.' To ensure that both persons report the relevant characteristics of the value, these characteristics should be part of a framework.

There is thus a need for a framework in the business reporting domain that restricts enough functionality to remain generic, but is flexible enough to allow the creation of specific business reports. This is where XBRL (eXtensible Business Reporting Language) comes in. XBRL enables the publication, exchange and processing of business reports over the Internet. XBRL was developed by XBRL International, a non-profit consortium of over 400 organisations. It is an open standard, which means that any business or software provider can build in XBRL in their software and use the standard free of charge.

5.3.5.2 Structure of XBRL

As depicted by Figure 5.3, XBRL is layered on top of XML. XBRL uses several technologies of XML. The important technologies are XSD (XML schema definition), XPointer and XLink. XSD allows for specifications of the requirements for the structure and data types used, XPointer is used to locate elements, and XLink is used to link elements together. On top of this layer is the XBRL 2.1 layer, which limits some of the possibilities of XML and extends others. Figure 5.3 provides an overview of the different layers of XBRL.

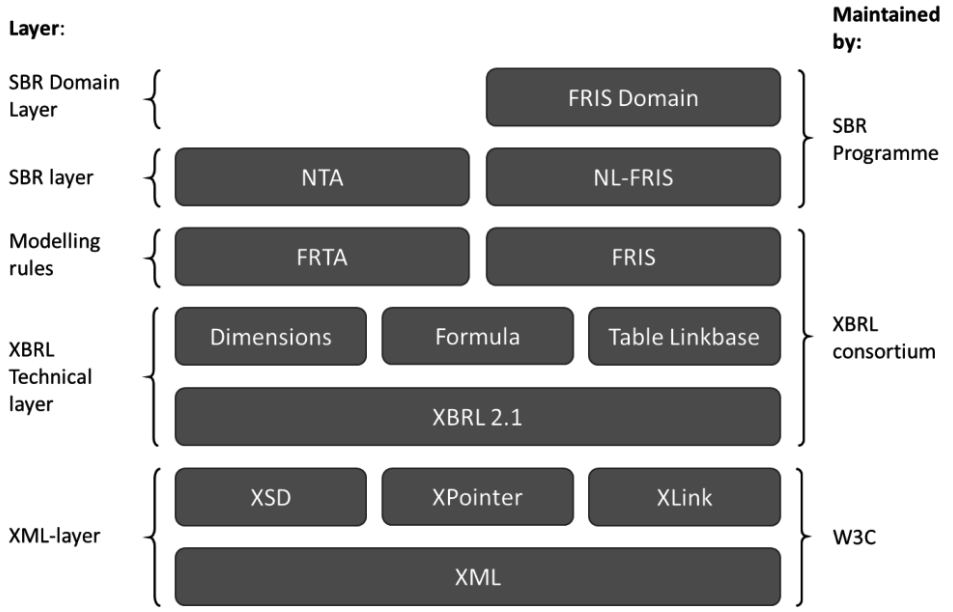


Figure 5.3 – Simplified XBRL structure in the Netherlands

After the release of XBRL 2.1, new XBRL specifications were added to the structure for dimensions, formula, and table linkbase, among others. Dimensions provide the possibility of using the aspect model, allowing reporting parties to define extra aspects to report on. The formula linkbase provides the functionality of adding business rules to a report, for example by calculating items within a report or stating if-then-else rules. Finally, the table linkbase makes it possible to present the dimensions in a table as is specified by the reporting party.

The XBRL specification specifies the requirements of the taxonomy and instance file. Best practices for exchanging business information can be found in the FRTA (Financial Reporting Taxonomy Architecture) and FRIS (Financial Reporting Instance Standard) documents, which contain specific requirements for financial reporting. The next layer includes taxonomy and instance requirements for specific groups. For the Dutch SBR Programme, these requirements are found in the NTA (Netherlands Taxonomy Architecture) and the NL-FRIS documents. The NTA specifies the FRTA even further, and the NL-FRIS specifies the FRIS even further. For example, the NTA specifies that footnotes are not allowed, and the NL-FRIS specifies that Chinese characters cannot be used in the reports. Finally, the specific requirements that government agencies impose are located in the top layer. The three administrative authorities that take part in the SBR Programme have specific requirements: the Tax and Customs Administration, the Chamber of Commerce, and Statistics Netherlands. The entity specification is different in all three cases. Each requesting party wants the re-

porting parties in their chain to electronically identify themselves with the identity number they got from that specific requesting party (for example, the VAT number for the Tax and Customs administration).

All the layers in Figure 5.3 are maintained by different organisations. The XML layer is maintained by the World Wide Web Consortium (W3C). The XBRL is maintained by the XBRL consortium. The two top layers are (in the case of SBR) maintained by the Dutch SBR Programme. Since the layers are stacked on top of each other, a change in a lower layer (for example, XML) will have an impact on all the upper layers. Therefore, older versions of XML (version 1.0) and XBRL (version 2.1) are still used, as newer versions ones would be difficult to implement due to the interdependencies between the layers. Instead, new layers are added to fix issues or add functionality.

5.3.5.3 How does XBRL work?

To provide an overall picture of how XBRL operates, we will look at the example of the integrative case introduced at the beginning of the chapter. Suppose that it was possible to take the actual pages of the financial statements and shake all the numbers off the page. All those loose numbers would now be lying on the floor, utterly meaningless. Did 679 refer to the turnover or salaries? Which financial year does the figure belong to? Are the figures in dollars or euros? Moreover, did the number have a footnote reference? What valuation principle has been used to determine the figure? XBRL makes it possible to associate such contextual data directly with the numbers. While this contextual data is only implicit on paper, XBRL makes it explicit. As seen in Figure 5.4, the information associated with the data item '679' is made explicit by the metadata.

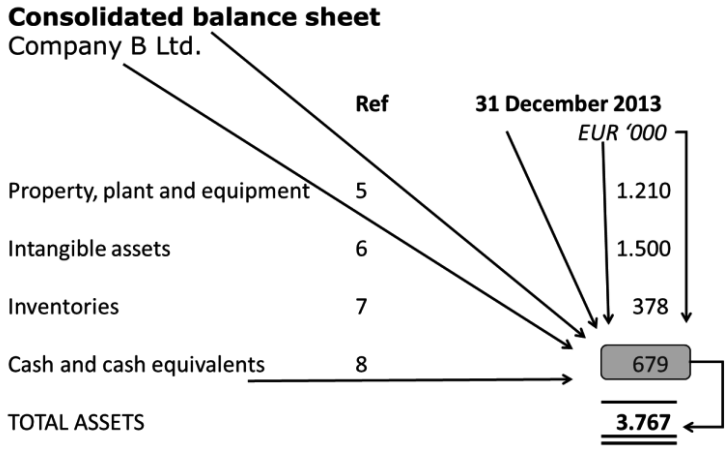


Figure 5.4 - Example of meta information

Making contextual data explicit ensures that the figures are meaningful, independent of the report or the environment that the data is used in. Adding this context ensures correct interpretation of the data in other systems or by other users.

It is important in data exchange that the data are tagged and that these tags refer to unique definitions. The file containing the data is called an XBRL instance document (see §5.3.5.5) and the set of documents that contain the definitions is called a taxonomy. The instance document and the taxonomy are inextricably connected with each other in order to ensure that the data can be read, interpreted and presented independent of the system used (Engel et al., 2003).

An example of a schema, instance and linkbase files based on the integrative case can be found in Appendix B. This example will be elaborated upon below on an abstract level. The elaboration will explain how cash and cash equivalents can be reported in an XBRL format. Although there is additional code in the files that is necessary for the XBRL files to function, it will not be included in the examples and corresponding explanation.

5.3.5.4 Taxonomy

Taxonomies are an essential part of the XBRL standard. An XBRL taxonomy is the place in which the concepts are defined. The taxonomy specifies what type of information the reporting party must enter into the instance document—for example, whether the data item must be a number or a string. A taxonomy is an electronic document containing an explanatory list of concepts and how they fit together. Based on the taxonomy, software programs prepared for XBRL may not only recognize what 'Cash and cash equivalents' refers to, but also that 'Cash and cash equivalents' is a part of 'Total assets.' A taxonomy ensures unambiguous data interpretation by users.

A taxonomy consists of one or more schema files and linkbases. A schema file is an .xsd file that describes elements. A linkbase links elements to one other. The linkbase is explained in further detail in §5.3.5.6.

Schema
In the schema, the element Cash and Cash Equivalents is described as follows:

<xs:element id="sbr_CashAndCashEquivalents" name="CashAndCashEquivalents" type="xbrli:monetaryItemType" substitutionGroup="xbrli:item" xbrli:periodType="instant" xbrli:balance="debit" nillable="false" abstract="false"/>

The different components are explained as follows:

xs:element	Declare new element.
id='sbr_CashandCashEquivalents"	Give ID to element.
name="CashAndCashEquivalents"	Give name to element.
type="xbrli:moneytaryItemtype"	The reported element is a monetary data type, which means that a currency should be reported in the instance file.
substitutionGroup="xbrli:item"	Element is not associated with other elements in the schema, nor is it grouped with other elements in a tuple.
xbrli:periodTyp="Instant"	The element is reported on a specific date (not in a period).
xbrli:balance="debit"	The element is recorded at the debit side of the balance sheet.
nillable="false"	The reported value cannot be empty.
abstract="false"	The element cannot be reported in the instance document

5.3.5.5 Instance document

The instance document contains the actual data that is exchanged. In the instance document, these items look like a list of XBRL 'tags,' each with a specific value and referring to a specific concept in the taxonomy. The instance document thus uses these tags to link the concept to be reported to its associated value. The reporting party must also include additional information, such as the period the data applies to or the data unit of the elements in which it is reported. An example is provided in the following textbox.

Instance document
In the instance document, Cash and Cash Equivalents is given the value 679000 in the following line:
<sbr:CashAndCashEquivalents contextRef="ContextA" unitRef="EUR" decimals="INF">679000</sbr:CashAndCashEquivalents>

The different components of the line are explained as follows:

sbr:CashAndCashEquivalents	A value will be reported for the concept CashAndCashEquivalents, which is declared in the taxonomy.
contextRef="ContextA"	The value will be reported for Context A (see description below).
unitRef="EUR"	The units are defined in euros.
decimals="INF"	The precision of the reported data is infinite (e.g., a reported value of 679000 is exactly 679000 and not 679001)
679000	The value that is reported (fact value).

One important aspect of the different components is the contextRef. Context refers to metadata values that are stored in a separate place in the instance document. In this case, the contextRef is referring to ContextA which can be found in the following lines:

```
<xbrli:context id="ContextA">
        <xbrli:entity>
                <xbrli:identifier scheme="http://www.sbr-nl.nl">12345678</xbrli:identifier>
        </xbrli:entity>
        <xbrli:period>
                <xbrli:instant>2013-12-31</xbrli:instant>
        </xbrli:period>
        <xbrli:scenario>
                <xbrldi:explicitMember
                dimension="sbr:DimensionConsolidatedorSeparate">sbr:ConsolidatedMember
                </xbrldi:explicitMember>
        </xbrli:scenario>
</xbrli:context>
```

This context has an identity (a unique identification number such as a VAT number), period (in this case, it is a specific date) and scenario (in the dimension titled Consolidated).

If Company B wants to report cash and cash equivalents on another date (e.g., 31-12-2012), a new context must be made (e.g., Context B) with a different date value.

An organisation may also make the instance document available on its own website to ensure that analysts, regulators, auditors and other parties can explore the data of the business reports. In theory, XBRL makes it possible to create a digital report with customised content that can be moulded into any required

presentation format—even information coming from multiple reporting parties at the same time, if needed. It is this flexibility that makes XBRL so powerful, and which distinguishes it from other standards for information exchange. If an organisation places the instance document on its website, analysts, regulators, accountants and other parties can use the data however they want without needing to manually process it beforehand to load and translate the data into their own information standards.

5.3.5.6 Linkbases

A linkbase is an XML file in which the links between elements have been defined. Solely recording the concepts is not enough: the concepts also need to be related to other concepts within the taxonomy, as well as to regulations and other resources. These relationships are called links and similar types of links are grouped together into a linkbase. To do this, XML Linking Language (XLink), which is part of XML, is used. XLink makes it possible to define complex relationships. XBRL makes full use of the options of XLink, which also allows the definition of multi-dimensional data models in a taxonomy.

Two types of linkbases can be distinguished, namely those for resources and those for relationships. An example of a resource linkbase is the reference linkbase, which links a resource (e.g., a reference to legislation or a regulation) to a specific concept. Relationship linkbases, on the other hand, serve three main purposes: information validation, inclusion of additional semantic information, or inclusion of information relating to the presentation of the information. Validation is important to guarantee the quality of the information—for example, that the calculations are accurate. The inclusion of additional semantic information may be necessary to give reporting parties sufficient insight into the nature of the concept. Most technically-oriented people see the presentation of information as secondary, but it is important for many business users. The presentation format can also be included in the taxonomy through the use of a linkbase. The characteristics of the various linkbases are summarised in Table 5.1.

Table 5.1 – Overview of linkbases in XBRL

Linkbase	Purpose
Label	A label linkbase contains labels with texts that should be shown to readers to ensure that they can understand and interpret a concept.
Reference	A reference linkbase associates concepts with the source of the request, such as legislation and regulations.
Definition	A definition linkbase is mainly used to record multi-dimensional relationships. It describes the relationships between the tables (hypercubes), axes (dimensions), domains and domain members. In addition to multi-dimensional relationships, the definition linkbase can also describe other relationships required to define an element.
Presentation	A presentation linkbase determines the hierarchical relationship between concepts for data presentation purposes.

Calculation	A calculation linkbase indicates which concepts are added or subtracted to check the correctness of the data items.
Formula	A formula linkbase makes it possible to define calculations that are more complex. It describes the validation rules that are applied to the data items in the instance document.

The following textbox describes the technical aspects of linkbases.

Linkbases
Linkbases are used to either link elements to one other (relationship linkbases) or to link elements to resources (resource linkbases).

Resource linkbases
Resource linkbases always contain a 'locator,' 'arc,' and 'resource.' A locator locates the appropriate element(s) in a taxonomy, while the arc describes the type of relationship that the arc represents. The 'resource' is just that: it is the resource to which the element is linked, such as a label or reference to legislation. In the following example code, the locator refers to the element CashAndCashEquivalents. The arc is a so-called concept-label arc, which means that it is intended to connect a label to a concept. The resource is a label intended for the concept CashAndCashEquivalents.

<link:loc xlink:href="sbr_31122013.xsd#sbr_CashAndCashEquivalents" xlink:label= "CashAndCashEquivalents_loc" xlink:type="locator"/>

<link:labelArc xlink:arcrole="http://www.xbrl.org/2003/arcrole/concept-label" xlink:from="CashAndCashEquivalents_loc" xlink:to="sbr_CashAndCashEquivalents_label" xlink:type="arc"/>

<link:label id="sbr_CashAndCashEquivalents_label" xlink:label="sbr_CashAndCashEquivalents_label" xlink:role="http://www.xbrl.org/2003/role/label" xlink:type="resource" xml:lang="en">Cash and cash equivalents</link:label>

Relationship linkbases
Relationship linkbases are slightly different from resource linkbases. They always contain locators and arcs, and the arcs link the locators together. The following example code illustrates a presentation relationship, where 'Cash and Cash Equivalents' are presented as the fourth item.

<link:loc xlink:href="sbr_31122013.xsd#sbr_CashAndCashEquivalents" xlink:label="CashAndCashEquivalents_loc" xlink:type="locator"/>

<link:loc xlink:href="sbr_31122013.xsd#sbr_AssetsTitle" xlink:label="AssetsTitle_loc" xlink:type="locator"/>

<link:presentationArc xlink:arcrole="http://www.xbrl.org/2003/arcrole/parent-child" xlink:from="sbr_AssetsTitle_loc" xlink:to="sbr_CashAndCashEquivalents_loc" xlink:type="arc" order="4"/>

5.3.5.7 Advantages of using XBRL in information chains

Many books and articles discuss the advantages of XBRL. These advantages can be clustered into three groups: (1) cost reduction, (2) transparency and (3) quality and speed. These clusters will be discussed in detail below.

Cost reduction is the type of advantage. A large proportion of IT costs are not caused by the systems, but by the interfaces between various systems. Systems

and applications often cannot communicate sufficiently with one other without investments in a new module or without inefficient additional actions, such as data transformations. XBRL offers an improvement by harmonising information flows, meaning that it links different systems without the need for customised interfaces (Bergeron, 2003).

In addition to cost reduction, XBRL also increases the transparency of reporting. Preparation of financial statements using the IFRS taxonomy increases transparency and comparability because, in theory, there is no longer any doubt about the interpretation of the figures. Reports can be compared immediately, unambiguously and digitally (Bonsón, Cortijo, & Escobar, 2009). At the receiving end (the analysts, regulators and public agencies), uniformity of data is an important advantage because it improves the comparability of the information. Moreover, manual processing of data in the receivers' own systems is no longer required.

Finally, XBRL provides users access to higher-quality data that is also more quickly available. It creates opportunities, both internal and external, for making better use of that information:

- Analysing the data based on defined business rules may improve internal process control, for instance, by immediately informing the responsible parties about certain discrepancies in general ledger entries.
- External parties can ensure further automation of data monitoring. For example, a bank that has granted a loan to a business can build signals into its own systems for when solvency criteria are exceeded. An analyst can immediately apply the XBRL data received to the required models without performing inefficient actions.
- Improvements in risk management are also possible. Currently, this important activity is usually performed on an *ad hoc* basis in many businesses and/or by means of labour-intensive data collection. XBRL makes it possible to improve the risk management process. It can be used for real-time signalling of risk.

The benefits of XBRL will only become evident when a community of parties who support XBRL arise. These include regulators, governmental bodies, businesses, analysts, etc. The more parties that join in, the greater the benefits of a seamless exchange of information become. The analogy can be applied to other means of communication as well: the advantages of telephone, fax, and e-mail only became truly evident to a wide audience once a large community of users had arisen.

5.3.5.8 Risks associated with the use of XBRL

The preceding section illustrated the advantages of using XBRL. However, there are also risks for all parties involved. In general, those who send and those who receive XBRL instances must adapt to the opportunities to be gained from XBRL over time, and apply the technology in a controlled manner to realise its advantages. A number of risks are described as follows:

- *'GIGO: garbage in, garbage out'*: to many people, the term XBRL is associated with higher-quality data. This is true, but only if the underlying

information systems are reliable, sufficient checks and balances have been built in, and the employees in question are competent in the system's use. Thus, XBRL does not necessarily ensure better-quality data.
- Errors in the taxonomy or the content of the taxonomy may lead to incorrect interpretation of data.
- Errors in reading may lead to incorrect interpretation of data. Incorrect mapping may yield an incorrect instance document that results in incorrect interpretation of data.
- 'Dialects' in the use of XBRL for each country, sector or organisation may lead to incorrect interpretation of data. These 'tinted' taxonomies are a risk to uniformity.
- Because data in XBRL format is less tangible, there is also a chance that an instance document will contain more information than the sender is aware of.

Incorrect data interpretation can have considerable consequences now that XBRL is making it possible to automate some corporate decisions. For example, a bank that uses XBRL data to monitor credit facilities may face problems if it turns out the data is being interpreted incorrectly. The implementation of XBRL is associated with the afore mentioned risks. While the majority of these risks are not new, they do deserve additional attention.

5.4 The data specifications for SBR chains

To describe how the SBR Programme developed data specifications for the exchange and processing of data in information chains, we will cover the following topics:

- The use of XBRL taxonomies within the SBR Programme
- Specific requirements for SBR taxonomies, including organisational requirements such as compliance with the Netherlands Taxonomy Architecture (NTA).
- The taxonomy development process applied for the Netherlands Taxonomy (NT). This process will be analysed in various stages, from the requirements analysis up through the publication stage.
- Relevant developments in XBRL that could provide new opportunities for SBR.

5.4.1 *Background on the use of XBRL taxonomies in the SBR Programme.*

At the beginning of the 21st century, the Dutch Government initiated the SBR Programme's precursor, the Netherlands Taxonomy Project (NTP). Its objective was to apply a shared XBRL taxonomy to various reporting domains. The basic idea was that efficiency advantages could be gained through standardisation of semantics and syntax, determined by the choice of communication standard. To obtain these advantages, data from the internal data administration must be reused for external reports as much as possible.

The objective of the SBR Programme is to realise a generic government solution for system-to-system (S2S) exchange and shared processing of business reports. The XBRL taxonomy is a vocabulary of harmonised data concepts that can be used for reporting to the Dutch government by means of a standardised syntax. As such, it is one of the building blocks of the SBR solution. The taxonomy ensures that organisations can draw up reports more quickly and easily and integrate them into their administrative processes and S2S filing of business reports to the government.

Interestingly, the emergence of the XBRL syntax was the primary reason for starting the SBR Programme. XBRL makes it possible to achieve the semantic standardisation required to define data unambiguously. In addition, this open standard does not create a dependency on a single or a small number of suppliers. As a result, the possibilities associated with using semantic standards became clearer to many parties. Earlier in the chapter, we stated that it would be better from a conceptual point of view if the choice of syntax had been made after the semantic standardisation had taken place. That is because we believe an ideal syntax should not impose any restrictions on the way that the data is modelled, as is the case for XBRL due to the way that the XBRL specification is drawn up. The SBR Programme chose the syntax first, before the required semantic standardisation was realised. Choosing to do it this way (compared to the conceptually correct method) led to considerable delays in cross-domain semantic standardisation.

The implementation of XBRL in the Netherlands illustrates 'the handicap of a head start.' In such a case, making progress in a particular area often creates circumstances in which stimuli are thus lacking for the pursuit of further progress. When the first version of the Netherlands Taxonomy was issued in 2006, the Netherlands was one of the first countries to use XBRL in the business reporting process. As a technique, XBRL was developing rapidly, as shown by the publication of XBRL specifications such as Dimensions 1.0. At that time, the Netherlands decided not to apply new specifications for the time being, as there was insufficient knowledge and experience with the techniques. However, this decision resulted in a situation in which no new XBRL specifications were adopted in the following years, despite the fact that sufficient benefits could have been obtained from doing so. More projects and programmes that applied the latest XBRL specifications subsequently arose at the international level, meaning that the Dutch working method became technologically outdated. Ultimately, the situation was resolved with version 6.0 of the Netherlands Taxonomy, issued in 2011, when the Netherlands Taxonomy adopted newer specifications to become technically comparable to international taxonomies such as IFRS and US-GAAP. The lesson that can be learned from this example is that it is important to keep up with new developments, as long as they are appropriate from a functional point of view.

The design of the SBR Programme also stands out due to the input of market parties in the realisation process of the Netherlands Taxonomy. The SBR Programme has been a public-private collaboration from the start, and is focused on promoting the acceptance and adoption of the Netherlands Taxonomy by market parties. Other countries in comparable situations have often chosen not to set up public-private partnerships, but implement their system as mandatory (Chen, 2012). The SBR Programme did not have the choice to do this in the Netherlands, as mandatory enforcement of a new way of reporting would not fit in with the country's culture of consensus-based economic and social policy making. In recent years, however, the consequences of the non-mandatory nature of the SBR Programme have been seen through the small number of messages received. It has become clear that making SBR mandatory or offering financial incentives are the only ways to make the SBR process successful.

5.4.2 *Specific requirements for SBR taxonomies*

An SBR taxonomy can be classified as a taxonomy that meets the rules set by the SBR Programme. In principle, all parties can realise a more effective and efficient information exchange process by standardising semantics and syntax. However, the objectives behind these standardisation efforts will be different for each situation. The same applies to the implementation method. The government's objective for SBR is to achieve greater efficiency and effectiveness in business reporting. The level of freedom is restricted in order to ensure that all parties that join SBR are aligned with this goal. This restriction prevents critical differences in implementation to as great an extent as possible, enabling reuse of data within an information chain. A number of important requirements have been drawn up in order to realise this restriction. These requirements must be met before an SBR taxonomy can be classified as such.

The requirements for SBR taxonomies can be subdivided into international and national rules. International rules apply to all projects around the world that use the term Standard Business Reporting. One example is Australia, where SBR has already been rolled out successfully. From an international perspective, two important requirements ensure classification as SBR project:

- An SBR taxonomy uses one or more controlled vocabularies containing concepts from collaborating (governmental) organisations, for the purpose of exchanging and processing data within an information chain.
- An SBR taxonomy uses the same syntax throughout the information chain. The financial reporting chain uses the XBRL syntax.

In addition, the following requirements, which are more organisational in nature, can be imposed on data standardisation projects in the Netherlands to allow them to be classified as 'SBR':

- An SBR taxonomy is created under the responsibility of the relevant requesting party.
- An SBR taxonomy is a part of the Netherlands Taxonomy (NT), to the extent that the requesting party is a governmental organisation.

- An SBR taxonomy complies with the requirements imposed on the Netherlands Taxonomy Architecture (NTA).

These items will be explained in the following sections.

5.4.3 *Responsibility of the requesting party*

An SBR taxonomy is drawn up under the responsibility of the requesting party in the relevant chain. For example, the Tax and Customs Administration is the requesting party in the tax domain. In theory, the creation of an XBRL taxonomy can be done in either a centralised or decentralised way. In the centralised form, a single organisation is responsible—at the national level—for the creation of the various domains of a taxonomy. In the decentralised form, each domain is responsible for the creation of a taxonomy or sub-taxonomy.

In the Netherlands, the SBR programme chose the decentralised approach to creating the overall taxonomy. In this approach, the requesting parties are responsible for creating sub-taxonomies. In addition, the SBR Programme plays a small central role by creating a joint sub-taxonomy with common elements. Here the various sub-taxonomies are combined into the Netherlands Taxonomy and tested against the rules in the NTA. SBR chose this decentralised model at the start-up stage of the SBR programme. The sub-taxonomies for the tax and statistics domains are the products of the Tax and Customs Administration and Statistics Netherlands, respectively. These parties take full responsibility for the taxonomies, including management of the products. Thus, another organisation setting up a taxonomy for the tax domain, for example, would not be a possibility.

The advantage of the decentralised approach chosen by SBR is that a requesting party is often the best party to define the required information through a taxonomy. The downside is that cross-domain standardisation and normalisation have become particularly difficult due to the various requesting parties involved. Within this context, many hundreds of architectural rules are needed to ensure a consistent setup of the various domains. In addition, all requesting parties need to make sure their concepts are described in detail in order to be able to determine to which extent the concepts correspond semantically. In addition, they have to use the technology to ensure that the same concepts are actually being used. This would be much easier if everything was handled by just one party than by multiple parties at various locations at different points in time.

5.4.4 *The Netherlands Taxonomy*

The SBR Programme created the Netherlands Taxonomy (NT), in collaboration with a number of requesting parties, for information exchange processing in the financial reporting chain. The NT currently comprises three different reporting domains: taxation, accounting and statistics. The differences between these domains are not only present in the definitions of the concepts used, but also in the way that concepts are defined and communicated to the reporting parties. The purpose of the NT is to provide an unambiguous framework of concepts based on

the applicable legislation and regulations. The normalisation of the framework of concepts is a continuous process, as changes are made to the concepts on an annual cycle. These changes are needed because reports are added, modified or removed from the NT. Reports need to be changed when changes in legislation and regulations occur. In addition, new reports can be added to SBR due to further extension of SBR within existing domains. Of course, further extension is also possible when new domains are added to SBR. The SBR Programme publishes at least one new version of the NT each year to address changes in legislation and regulations. However, this does not mean that major changes in the administrative processes and their underlying information systems are also required every year. Proper implementation of XBRL by software providers would mean that the only alterations needed to facilitate the changes are to the mapping table between the taxonomy and the databases. The mapping method is crucial for the efficiency and effectiveness of reporting.

5.4.5 *Compliance with the Netherlands Taxonomy Architecture*

The architecture determines which elements of the XBRL standard will be used in the relevant taxonomy and how the elements will be used. XBRL International has defined the outline of a syntax that makes it possible to create various taxonomy architectures. In 2005, an XBRL International working group combined a set of agreements (best practices) into the Financial Reporting Taxonomy Architecture (FRTA). The FRTA contains a large number of more or less self-evident rules. For example, it includes the guidelines that each concept should have a unique default label, that a description should be comprehensible and that an element must only occur once. A 'concept' is the term used by XBRL to indicate an element for which a value can be reported. Most XBRL tools have built-in validation functionality to check whether the taxonomy corresponds to the FRTA stipulations.

Because of continued development of the XBRL standard, this standard has become so outdated that large projects cannot rely on it anymore. This situation, together with the numerous options provided by the XBRL specification, has made it necessary to detail the taxonomy architecture at a local level. Within the SBR Programme, the Netherlands Taxonomy Architecture (NTA) was set up with this need in mind. The setup of the NT is based on the NTA. The NTA determines—for the entire NT—which elements of the XBRL standard can be used in the Dutch situation and how they are used. The NTA limits the level of freedom for the various requesting parties in drawing up their sub-taxonomies in order to improve harmonisation.

The setup of the NTA is based on the common principles for the construction of an SBR taxonomy. These construction principles are listed as follows:

- Simplicity of the reporting process.
    - The architecture must focus on the simplest possible mapping and instance document creation.

    - The architecture supports the basic principle of SBR: achieving optimum data reuse.
- Stability.
    - The architecture helps minimise the impact that changes to legislation and regulations will have on information delivery systems (sources).
- Consistency.
    - The architectural framework must be consistent and the taxonomy (and any extensions) based upon it must be covered by these frameworks.
- Compliance with specifications, best practices and related taxonomies.
    - The architecture must differ as little as possible from what has been successfully applied in other projects.
- Maintainability.
    - The architecture lays the foundation for easy maintenance.
- Performance.
    - The use of the architecture must result in other technical advantages, for example, instance documents that are as small as possible and the best possible performance when instances are processed.

These principles guide the taxonomy development process, which will be explained in the following section.

5.4.6 *The taxonomy development process*

Piechocki and Felden (2007) state that the development process for an XBRL taxonomy is different in nature from the development of software systems or knowledge systems. The process requires standardisation of an information chain domain based on standardised metadata. In addition, an XBRL taxonomy is often later implemented in software as a way to define the metadata and as the basis for drawing up reports. Piechocki and Felden (2007) state that "*XBRL taxonomy development can be regarded as a transfer of the domain knowledge from a domain expert into an implemented knowledge base which is encoded within an XBRL taxonomy*" (p. 894).

Based on these ideas, the authors present a model that describes the taxonomy development process (Figure 5.5).

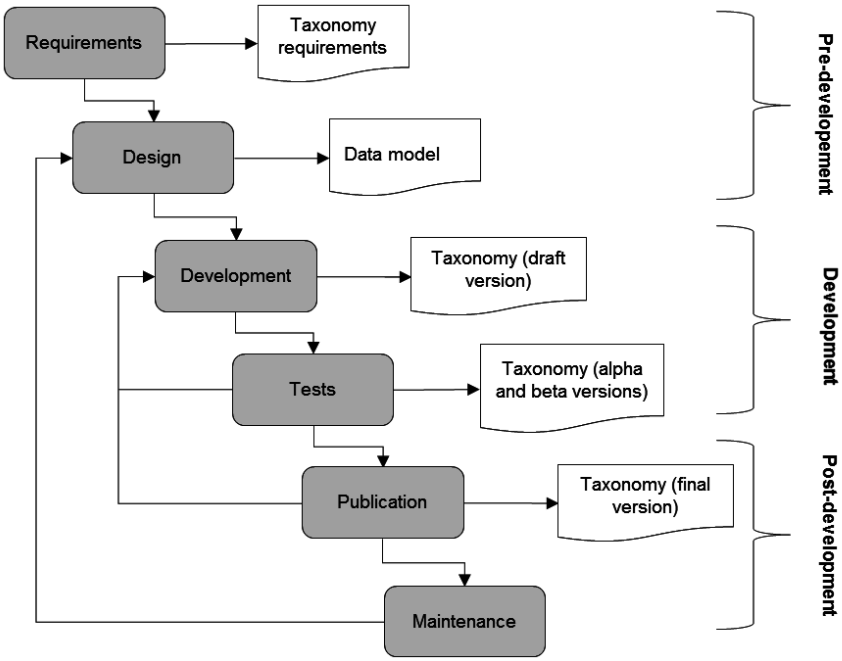


Figure 5.5- Taxonomy development model (based on Piechocki & Felden, 2007)

The taxonomy development model includes clearly defined stages that a taxonomy author will face when developing an SBR taxonomy. The authors used current developments in XBRL projects around the world as the foundation for this model. The development of the SBR taxonomy has the same development process phases and same deliverables at the end of the each phase as in Figure 5.5. These phases are explained in detail in the following sections.

5.4.7 *Requirements phase*

The requirements are examined and defined during the first phase of the taxonomy development process. This stage yields a list of requirements that represent the content of the taxonomy. The information chain plays an important role in defining these requirements, as the requirements that can be imposed on the taxonomy depend strongly on the information chain characteristics summarised in the table below.

Table 5.2 – Characteristics of reporting obligations in a chain

Characteristic	Relevant aspects	Section
1. Type	Domain, flows, aggregation level	5.4.7.1
2. Frequency	Conditioning, cyclical, event based	5.4.7.2
3. Directionality	Duty to provide data, right to obtain data	5.4.7.3
4. Origin	Coercion, interest	5.4.7.4
5. Nature	Open, closed business reporting	5.4.7.5

Next, the five characteristics listed in the table are explained in detail.

5.4.7.1 Type of reporting obligation

The first chain characteristic that is integral to the taxonomy requirements is the type of reporting obligation in the chain, which determines the domain that the taxonomy relates to. A domain is a specific area, often with a specific domain owner, in which one or more types of data are exchanged. Good examples of domains are the tax domain and the accounting domain, which are currently included in the Netherlands Taxonomy. Various different flows can also be distinguished within a domain. A flow is a specific type of reporting, used within the domain in question to exchange information for a specific purpose. For example, the corporate income tax and VAT tax declaration flows within the fiscal domain are quite distinct. The latter focuses on exchanging data that is relevant to the self-calculated amount to be paid, for instance, based on VAT amounts stated on purchase and sales invoices. The corporate income tax flow focuses on data that is relevant in determining the amount of the corporate income tax to be paid, such as the organisation's profit. A domain can therefore have multiple flows. These flows are often included in the Netherlands Taxonomy in separate reports.

A flow may also have different aggregation levels Three different aggregation levels can be seen from a conceptual perspective: the reporting level (highly aggregated), the administrative level (somewhat aggregated) and the transaction level (not aggregated). Within SBR, all flows currently focus on the reporting level, which is the most highly aggregated level, since the reporting obligations in the current SBR domains are at this level. However, this is the only option, as other levels are also possible in other domains.

5.4.7.2 Frequency of exchanges

The second chain characteristic that determines the requirements is the frequency of exchanges. The reporting obligations that can be distinguished within an information chain often differ in their frequencies and the times at which they are submitted. Arendsen (2008) states that reporting obligations can be categorised into conditioning, cyclic and event-driven.

- 'Conditioning' reporting obligations are those in which an organisation enters into a specific legal relationship for the first time, such as taking out a loan. The reporting obligations imposed in this context apply to the legal relationship established at that moment.
- 'Cyclic' reporting obligations for organisations recur periodically. They usually concern the reporting of data for specific periods, such as monthly, quarterly or annual reviews. An example of this type of obligation is the VAT declaration that organisations are required to send in to the Tax and Customs Administration periodically.
- 'Event-driven' reporting obligations depend on the occurrence of specific events within an organisation. A good example is a request by Statistics Netherlands (CBS) to complete a statistical declaration. Not every organisation is requested by CBS to submit information each year. Whether or not an organisation is requested to submit information depends on the sampling procedures applied by CBS.

The Netherlands Taxonomy has placed particular attention on flows that can be seen as cyclic reporting obligations. For requesting and reporting parties, cyclic reporting obligations can benefit most from standardisation. Organisations are more willing to standardise if they can benefit from the reporting recurrently. Such is clearly the case for reporting obligations that are cyclic, but less so for obligations that are conditioning or event-driven, whose incidental nature makes standardisation of the information flows less interesting for many parties. Such a case can currently be seen in the statistics domain, which is lagging behind other domains in terms of the number of business reporting messages received. Because of the event-driven nature of these flows, organisations rarely use these messages for reporting, despite the fact that they can easily send in business reports this way. We can offer two possible solutions for this situation. The first is to change the event-driven character of the reporting into a cyclic one. However, as this means that organisations will have additional reporting obligations, it is not a realistic option. The second possibility is to make SBR the exclusive business reporting standard and discontinue all other options.

5.4.7.3 Directionality of reporting obligations

The third characteristic of the chain that determines the requirements is the directionality of the reporting obligations. Two directions can generally be distinguished: either the organisations have a duty to provide data to a requesting party, or the requesting party has the right to obtain data from the organisations. When organisations must declare data to a requesting party, it is called a duty to provide. Nijsen (2003) also calls this an 'active' reporting obligation. When a requesting party is allowed to obtain data from an organisation, it is called the right to obtain, which is also known as the 'passive' reporting obligation.

The various flows that can currently be distinguished within SBR are all based on the duty to provide. There are good reasons for this directionality, as the flows for a duty to provide are often cyclic and the flows for a right to obtain data are usually event-driven. Standardisation is easier in the first case, as stated earlier. However, in theory, SBR can support both the duty to provide and the right to obtain data. In addition, SBR can support the resulting communications, such as service messages about tax assessments from the Tax and Customs Administration.

5.4.7.4 Origin of the reporting obligation

The fourth chain characteristic that determines the taxonomy requirements concerns the origins of the reporting obligation. Reporting obligations and their related messaging often originate from legislation and regulations (Arendsen, 2008). Legislation and regulations always define the duty of organisations to disclose information to the administrative authorities (also known as business-to-government or B2G reporting obligations). Within the SBR Programme, the reporting obligations for B2G information chains are based on the stipulations laid

down in the legislation and regulations, as can be clearly seen in the three current B2G flows. All three are based on relevant legislation and regulations in their specific fields.

The situation is different for business-to-business (B2B) information chains because these parties cannot rely on applicable legislation and regulations as the basis for their reporting obligations. In the Netherlands, there is currently only one B2B information chain in SBR. It is in the banking domain, where a consortium of three large Dutch banks jointly determines the reporting obligations that organisations must comply with when submitting credit reports using SBR. These reporting obligations are based on the information that the banks' internal systems need in order to make the appropriate risk assessments on their loans.

5.4.7.5 Nature of reporting obligations

The fifth characteristic of the information chain that determines the taxonomy requirements is the nature of the reporting obligations. Two different types of business reporting can be seen in an information chain: open and closed.

In open business reporting, the reporting party is allowed at least some level of freedom in deciding what data it will declare to the requesting party. An example of open business reporting is a financial statement by a large organisation. Legislation and regulations provide a reporting framework, but organisations are allowed a certain amount of freedom regarding what they do and do not wish to explain and include in the financial statements, based on their own assessments. Most organisations choose to adopt a minimalist position and report as little as possible, but this does not mean that they cannot use a different approach.

The data to be supplied in closed business reporting is defined in detail by the requesting party, and the reporting party is not allowed to deviate from it. In this situation, an organisation is not given the freedom to add items, and must only report the items determined by the requesting party. In a paper environment, this would mean that a particular form would be completed. A good example is the VAT declaration, a fixed set of data that organisations must send in to the Tax and Customs Administration and where no deviations from that fixed dataset are allowed.

Reports drawn up based on the Netherlands Taxonomy have been in the 'closed' category. This situation is currently changing, however, as the financial accounting domain wants to provide organisations with considerably more freedom in drawing up the content of their business reports. Initially, the choice to keep the taxonomy for this domain closed was a deliberate one due to the focus of the SBR programme on smaller organisations and the additional complexity associated with open reporting. The assessment was that the reports in the NT were sufficient for small organisations and generally did not require any expansion. However, as the case is different for medium-sized and larger organisations, the option of open business reporting will be added to this domain. For the tax and statistical domains, on the other hand, open business reporting is not a realistic

option in the Netherlands, as the requesting parties have precise requirements about what data they want to receive. Thus, the reporting party is not given any freedom regarding what it reports.

5.4.7.6 Taxonomy framework

As detailed above, the requirements of the taxonomy can be derived from the characteristics of the relevant information chain. An idea of the taxonomy framework must already be in existence in the requirements phase. The taxonomy framework can be described as a method by which various taxonomies are —or are not—combined (Piechocki & Felden, 2007). The framework also indicates whether a basic taxonomy or an extension taxonomy should be developed. A basic taxonomy defines all the concepts independently, whereas an extension taxonomy uses concepts (or a subset of concepts) drawn up by another party.

The NT has its own concepts plus others that have been imported from other international taxonomies. For example, a number of business reports that are an extension to the IFRS (International Financial Reporting Standards) taxonomy are available in the financial accounting domain. IFRS is a reporting standard that must be used by companies listed on stock exchanges in Europe when drawing up their consolidated financial statements. All other businesses in Europe also have the option to use this reporting standard when drawing up their annual financial statements. The International Accounting Standards Board (IASB, the organisation that issues the IFRS) publishes an IFRS taxonomy annually, in addition to issuing a 'bound volume' every year that describes all reporting rules in book form. The IFRS taxonomy is a representation in XBRL format of the reporting options found in the bound volume.

5.4.8 *Design phase*

The development of any taxonomy requires the collaboration of domain experts and technical experts, who jointly combine semantics and syntax into the relevant taxonomy. In the taxonomy development process of Piechocki and Felden (2007), the design phase focuses on semantics. This stage is about using a semantic data model to provide structured insights into the knowledge of domain experts. In our description of this phase, we will deliberately discuss syntax as little as possible because, as stated earlier, semantics should be kept independent of syntax. As a consequence of choosing XBRL as the syntax, however, it should be noted that this stipulation may not be absolutely true in practice, since the XBRL syntax imposes a number of restrictions on the semantics. Nevertheless, we are making this distinction so that the semantics of the semantic data model can be kept as objective as possible. We will discuss the syntax in detail when describing the construction phase. The design phase includes the following steps needed to obtain a semantic data model:

1. Identification of the concepts
2. Normalisation of the concepts
3. Structuring the concepts

5.4.8.1 Identification of the concepts

A domain expert must identify the relevant concepts based on the information needs of the requesting party. When doing so, the domain experts should not rely on the concepts required in the taxonomy, but must ask themselves what business reports need to be provided to the requesting party. They should not take into account any potential technological complications. In practice, requesting parties will often start identifying concepts from the applicable legislation and regulations in the domain concerned, or from the information needs of the internal systems of a requesting party. An analysis by the domain expert will result in a list of concepts that can be requested by a requesting party. The text box provides an example.

Identification of concepts based on legislation
The concepts in the financial accounting domain are based, *inter alia*, on the articles in Title 9 of Book 2 of the Dutch Civil Code (BW2). We will use a random legal article to illustrate how concepts can be identified. This example originates from Section 3, which list regulations for the balance sheet and its explanatory notes.
Article 369:
The following inventory items included in current assets are to be listed separately:

a. raw materials and auxiliary materials;
b. work in progress;
c. finished product and trade goods;
d. advance payments for inventories.

Based on the this article, six concepts can be distinguished that could appear on the balance sheet: 'current assets,' 'inventories,' 'inventories of raw materials and auxiliary materials,' 'inventories of work in progress,' 'inventories of finished product and trade goods,' and 'advance payments for inventories. A domain expert would thus identify these six concepts based on the legal article.

5.4.8.2 Normalisation of the concepts

The normalisation of concepts aims to ensure that concepts are only defined once in a controlled vocabulary within a domain. To do this, a domain expert must have sufficient insight into the definition of the concept involved. In addition, the possibilities for inter-domain normalisation (i.e. across different domains) should also be considered.

Inter-domain normalisation can create complex situations, for instance, if data definitions based on different stipulations do not match up, or if they are illogical given the context in which they are used. The source is often the applicable legislation and regulations, but the relevant laws and rules are not necessarily consistent. Far-reaching normalisation is not possible, or at least not yet, as it would require further harmonisation—i.e. changes to the relevant legislation and regulations to ensure that the definitions are aligned. The laws and regulations are mostly 'owned' by different ministries or departments, so harmonisation can be a lengthy process.

Any differences in definitions within legislation and regulations will cause problems for data reuse. Further standardisation of data definitions across specific legislation and regulations will lead to more general information requests, thus reducing the number of elements in the information request.

The above-mentioned complexities also play a role within the SBR Programme. The legislation and regulations that requesting parties' demands are based on are different for each domain, which leads to variation in the definitions. Concepts that appear to be the same but are not are regularly seen. For example, the tax domain and the financial accounting domain use different definitions of the concept of 'profit.' If the substantive definitions of these concepts are considered, it turns out that there is some degree of difference between them. As a result, these concepts must first be harmonised by changing the legislation and regulations. Such harmonisation, however, is generally beyond the scope of SBR. If further harmonisation is not possible or desirable, it means that there are actually two concepts here. After all, their definitions illustrate that they are not identical. To facilitate further harmonisation, the equivalence of the two concepts can be explicitly recognised in the NT by adding a relationship using definition links.

When new parties join the SBR Programme, they are also obliged to investigate to what extent their data requirements can be covered by the concepts already included in the NT. The reason for this mandatory exercise is that normalisation makes it easier for an organisation to draw up its business reports.

5.4.8.3 Structuring the concepts

Once a list of concepts has been drawn up, structuring of the concepts is done to describe their relevant characteristics, using defined standards. The activities for structuring concepts can be divided into the characterisation of the concepts and the description of the relationships between them. The output of these activities is a semantic data model. Although we are referring to a purely semantic data model here, domain experts are often forced to take into account syntax when structuring the concepts. This is because the syntax may enforce some semantics. An example of this is the inclusion of a 'balanceType' attribute in a concept that is based on the XBRL 2.1 specification. At first, this attribute would not usually be included in a semantic data model, as it is not required for exchanging and processing the data. However, because of the implementation by the syntax, it is ultimately necessary to add this attribute to the semantic data model. From a conceptual point of view, we argue that it would be better if the choice of syntax does not influence the semantic data model, but such situation often proves impossible in practice.

The activities for describing concepts consist of determining the attributes, labels, definitions and references. The activities for describing relationships between the concepts consist mainly of determining the order of concepts, the calculation with concepts, or other kinds of relationships between the concepts. All

of these activities should be carried out by a domain expert with some knowledge of semantics.

Attributes
When determining technical concepts, attributes must be added to the concepts identified (or it should be possible to add them) depending on the chosen syntax. Attributes can be considered as specific characteristics of a certain concept. Various types of attributes are available in the XBRL 2.1 specifications.

Labels
Labels that provide a readable representation of a concept can be linked to declared concepts. To do this, the labels are linked to the technical identification code of concepts. This makes it possible to link different types of labels, for instance, labels in different languages. Labels are also used for what are known as 'preferred labels,' these labels are used in default in the presentation view.

Definitions
It has already been stated that definitions are required when normalising concepts, to guarantee that the concepts are unambiguous. Being able to show these definitions to the users of a taxonomy also has the added value of making sure they are aware of the precise meaning of a specific concept. It is recommended that these definitions be included in the taxonomy as well, for example, by using a documentation label.

References
It is possible to link concepts with references to the relevant legislation and/or regulations. These references can also be seen as a type of definition, as the legislation and regulations probably say something about the concept.

Sequence of concepts
The domain expert will often structure the concepts so that they have a specific sequence that must be displayed to the party drawing up the business reports. In practice, this is usually a sequence that the users are familiar with.

Arithmetic relationships of concepts
In addition to content-based semantic descriptions, relational connections may be used as semantic descriptions. Including an 'arithmetic' relationship in concepts is very interesting for many parties. It makes clear, for example, that adding the value of Concept A to the value of Concept B results in Concept C. However, it should be stated that showing these 'addition' relationships is not the same as validating the relationships. The relationship may be shown based on the taxonomy, but validation confirms whether the values actually add up.

Interconnectedness of concepts
Various detailed relational connections can be distinguished along with the 'addition' relationship described above. A relationship showing a certain degree of interconnectedness between concepts could, for example, be one that shows how

Concept A is a specific case of Concept B. Users may find it useful to know whether and how certain concepts are interconnected. The semantic descriptions of the relationships and content-based aspects are expressed as metadata in the taxonomy. The greater the number of relationships and content-based aspects a requesting party can define, the more metadata will be available to the reporting parties. A large amount of metadata for the reporting concepts should ensure unambiguity of those concepts, making it easier for reporting parties to understand exactly what information the requesting party wants to obtain.

Attempts are made in the SBR context to supply as many useful relationships and content-based aspects of concepts as possible to the reporting parties in the form of metadata. Deciding what metadata is included in a taxonomy is often the result of balancing interests. Trade-offs regularly need to be made between the added value for the reporting parties on one hand and the efforts to create the metadata on the other. This may result in situations where a certain type of metadata is not included, at least provisionally. A good example of such a situation is the arithmetic relationship between concepts. In recent years, SBR chose not to include such elements in the taxonomy. The reason was that the functionality was insufficient, as the technology had not been developed far enough. That development has now been realised, so the inclusion of arithmetic relationships is expected to take place in future.

Despite the trade-offs that sometimes need to be made when providing metadata, it is an essential component of the semantic descriptions. The overall purpose of metadata is to eliminate ambiguity in the meaning of the data exchanged.

5.4.9 *Development phase*

The development phase involves the translation of the semantic data model into its syntactic representation, i.e. a draft version of the taxonomy. One of the major challenges in developing a taxonomy is converting the knowledge and requirements from an expertise domain into syntax that can be interpreted by a computerised system (Claassens, 2007). The technical knowledge required for modelling a semantic data model to produce syntax is so specific that technical expertise is essential.

5.4.9.1 Modelling concepts to produce a data model

Modelling concepts into a data model eventually results in a draft version of the taxonomy being created. These activities are mainly carried out by a technical expert or data modeller. It is very important here that the possibilities offered by an open standard such as XBRL are restricted as much as possible, as it is possible for different experts or data modellers to create completely different taxonomies using the same raw materials. It is therefore desirable to use a specific architecture that restricts such options. In such a situation, the architecture is explicitly intended for the creation of an unambiguous taxonomy.

Another helpful tool for modelling is the use of design templates. A number of different semantic scenarios can be distinguished in a report, and the technical expert or data modeller will use these to identify a pattern in the syntax. The taxonomies become less ambiguous by using a specific method for processing these template patterns with existing syntax options and including that method in the architecture. One example of a pattern is the way that a summary of movements (e.g., opening balance + movements = final balance) must be modelled. Of course, the technical expert or data modeller is free to determine whether these templates will be used.

There are various ways of looking at how to model concepts into a data model (Simsion and Witt, 2005). These include:

- The communication perspective
- The presentation perspective
- The storage perspective

In practice, users often do not distinguish between these perspectives, resulting in unnecessary or undesirable requirements being imposed on the modelling. These perspectives are discussed in further detail below.

5.4.9.2 Communication perspective

The communication perspective is the most important perspective in a data model for electronic message data exchange. This is because communication is the primary task of an electronic message. There are various modelling techniques that ensure the best possible content of the messages, depending on the chosen syntax.

Modelling techniques

The normalised list of concepts needs to be further modelled in a taxonomy. Using XBRL as the syntax makes it possible for the data modeller to model the data in two ways: 1) using a hierarchical modelling method, and 2) using a dimensional modelling method. In hierarchical modelling, data is organised into a tree structure that represents data using parent-child relationships. Each parent may have multiple children, but each child has only one parent (a one-to-many relationship). In this structure, elements of the concept name are reused from the parent concept, creating a 'path' or 'breadcrumb trail' such as *Assets – Current Assets – Cash and cash equivalents*. The hierarchical modelling method is a good method if the concepts are normalised and the syntax only permits a hierarchical model. Figure 5.6 provides a graphical representation of hierarchical modelling.

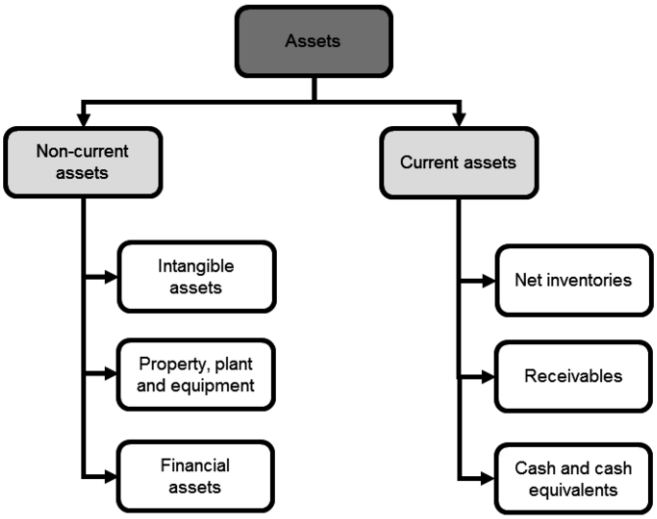


Figure 5.6 – Graphical representation of a hierarchical structure

The second modelling technique uses a dimensional model. Modelling in one or more dimensions makes it possible to reuse concepts by modelling part of the semantics into the dimensions, thus minimising the number of concepts in the taxonomy. The dimensional modelling method is particularly interesting in more complex business reports that require large tables. An example of a more complex report is a case in which similar information is requested for different categories. Table 5.3 provides an illustration of multi-dimensional modelling of turnover broken down by product and country. The various turnover values are reported for the various dimensions.

Table 5.3 – Dimensional structure of turnover broken down by country and product

Turnover	Benelux			France	Spain	Total
	Nether-lands	Belgium	Subtotal			
Turnover of product X	10	2	12	-	-	12
Turnover of product Y	1	-	1	6	8	15
Turnover of product Z	5	3	8	1	2	11
Total	16	5	21	7	10	38

The NT uses both the hierarchical and dimensional modelling methods. However, the complexity of dimensional modelling in the NT remains limited. Various European projects are currently working on several complex XBRL taxonomies that use an extremely large number of dimensions. Using dozens of dimensions at the same time is not uncommon. The methodology for multi-dimensional modelling is known as a 'data point model' (DPM).

Granularity
One aspect that is relevant from the communication perspective is determining the level of granularity of data, i.e. the aggregation level or the level of detail. A good example regarding granularity can be found in the definition of accommodation costs. If one does not want rent subsidy to be part of the accommodation costs, the definition then becomes "accommodation costs, i.e. rent, energy costs, cleaning costs exclusive of housing benefits, etc." Each individual 'granules' or component of accommodation costs must then be identified explicitly. Determining the degree of granularity is a more or less subjective choice by the data modeller. SBR applies the basic principle that legislation and regulations are the guides in determining the degree of granularity. If the legislation and regulations explicitly refer to certain items, the possibility to query those items via a separate concept will also be provided.

Validation
Validating data is relevant from the communication perspective, as it ensures that the data complies with the quality requirements imposed on it. The syntax used, partially determines the possibilities for data validation. For example, by designating specific data types for certain concepts. It is also possible to require specific items to be reported or left out, based on the modelling method used. A third way to validate data is by using specific business rules that can be part of a data model. All three methods are used in SBR.

5.4.9.3 Presentation perspective

The presentation perspective is a less interesting perspective from the data-modelling point of view, as it merely focuses on the presentation (rendering) of the data from the data model. This rendering can be on paper, in a digital document, or in a software that displays XBRL messages on a screen. The essence here is that the presentation of the data does not necessarily have anything to do with the way that the data is included in a data model, it is merely a way to present the data. Business users often find it difficult to understand this essential point, since their focus is virtually always on the presentation perspective. The business user is often accustomed to creating or completing forms or business reporting templates that have a more or less stable presentation. Over the years, this presentation has often been optimised for viewing by humans. The presentation also often reflects implicit relationships (e.g., parent-child) and is thus not generally suited for automated processing, as implicit relationships are incomprehensible to computers. While people are accustomed to the presentation perspective, it should not be forgotten that—both within and outside this perspective—there are numerous other ways to group data consistently using metadata.

We can identify various types of relationships between concepts that are used for presentation. These include the sequence that concepts are presented in, the hierarchical level at which concepts are presented, the tabular format that concepts are presented in, etc. These are all examples of content-based presentation, but it is also possible to present concepts using typographical characteristics. An example might be to present concepts in a certain colour to express a certain

categorisation. Such relationships must also be included in the taxonomy if they are to be used. This is often done using various parent-child relationships. The example in Figure 5.7 shows the assets side of the balance sheet, in which the presentation sequence has been set using parent-child relationships.

Balance sheet [title]	
Assets [title]	
Non-current assets [title]	
Intangible assets	X
Property, plant and equipment	X
Financial assets	X
Non-current assets	X
Assets [title]	
Stocks	X
Receivables	X
Cash and cash equivalents	X
Current assets	X
Total assets	X

Figure 5.7 – The presentation structure of a balance sheet

Presenting concepts in XBRL taxonomies has always been an issue, as only the presentation sequence of reportable concepts could be included. The options offered by modelling in dimensions highlight the limitations of the XBRL approach. Requesting parties that wanted to provide a rendered version of the data often had to implement custom software solutions to do so.

5.4.9.4 Storage perspective

The storage perspective focuses on the use of the taxonomy as a means of storage. In theory, an XML file can also be used as a storage document for data. This can be useful in some situations, but we believe that this methodology has one big disadvantage: its performance. Data can always be retrieved more rapidly from a normalised database than from various XML files or from a native XML database. Therefore, this chapter refrains from discussing XML as a storage format in detail.

From the storage perspective, we will focus on how the taxonomy can be mapped to the databases of the reporting and requesting parties. This 'mapping' is essential for automated generation of business reports by reporting parties based on the latest taxonomy. Reporting parties can often realise this mapping through their own administration. The administration software loads the taxonomy and allows the reporting party to create a mapping between the concepts of the requesting party and the concepts as defined in their own administration. Some administration software even handles this process for customers. A requesting party can often provide a similar mapping, which they use to link the concepts from the taxonomy to the concepts in their internal systems to make sure they can be transferred automatically.

5.4.9.5 Realisation of SBR taxonomies and the role of the NT

The realisation of an SBR taxonomy is associated with a number of special aspects that cannot always be found in other taxonomies. As stated earlier, SBR taxonomies are always created under the responsibility of the relevant requesting parties. Nevertheless, this does not mean that the requesting parties are the owners of all the concepts they use. The requesting party is free to further develop the taxonomy in-house or outsource it to another service provider. The SBR taxonomy is a sub-taxonomy, i.e. a taxonomy for a specific domain included in the NT. All the taxonomies that are part of the NT must comply with the architectural agreements included in the NTA. The tax domain, the financial accounting domain and the statistical domain are the three sub-taxonomies that are currently part of the NT. The characteristics of a sub-taxonomy are that it focuses on a specific domain and that it is included in the NT. Reports that are part of a domain in the NT obtain their concepts from a common set of concepts, if possible. There will always be concepts, however, that only apply to one specific domain. Figure 5.8 provides a graphical representation of this principle.

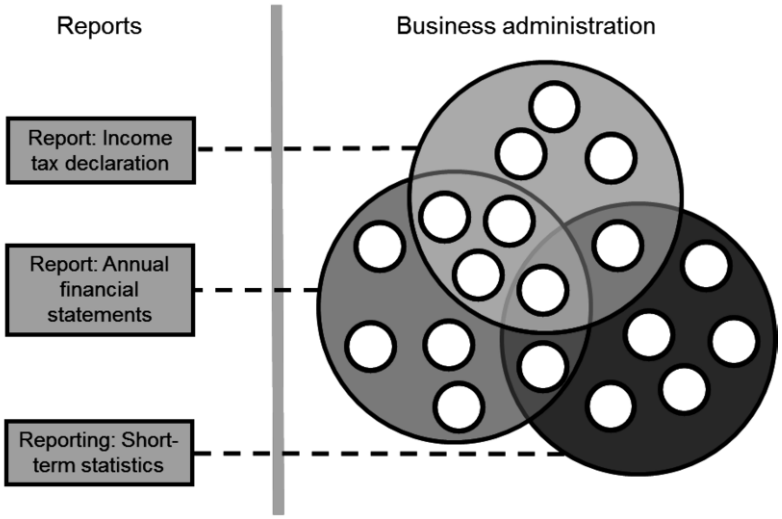


Figure 5.8 – Graphical representation of the structure of the Netherlands Taxonomy

A sub-taxonomy therefore is not the same as an extension taxonomy. An extension taxonomy uses the concepts in the NT for the reporting process, but the requesting party still needs a limited number of other definitions for specific reporting objectives to create the proper reports. A good example of an extension taxonomy is the banking taxonomy used by a consortium of the three largest banks in the Netherlands for exchanging data between businesses and banks relating to loans. The banking taxonomy is an extension of the NT, as it is largely aligned with the financial statements and tax declarations in the NT. The banks defined additional concepts specifically required for credit reporting. The bank

taxonomy is issued as a separate taxonomy and is not part of the NT, but it complies with the architectural agreements included in the NTA.

5.4.10 *Test phase*

A draft version of a taxonomy is subject to an extensive testing stage after it has been delivered. A number of metrics are required to determine the taxonomy's quality. The question that should be asked is to what extent the data model supports the information requirements (Simsion & Witt, 2005). This means that the tests must determine whether the various quality requirements were taken into account in the taxonomy's creation. The quality characteristics specifically defined for data are useful for this. In this chapter, 'quality' refers to being fit for a specific purpose (Juran, 1992). Test activities are carried out during the test phase to determine whether the semantic and syntactic quality requirements have been met.

5.4.10.1 Semantic quality requirements

The semantic quality requirements focus on the quality of the content rendered from a data model. These requirements should be considered when constructing the data model. The literature provides several overviews of data quality requirements. Requirements such as accessibility can be evaluated or measured using one or more indicators. An article by Lee et al. (2002) provides a comprehensive set of quality requirements and indicators (see Table 5.4).

Table 5.4 – Data quality requirements (based on Lee et al., 2002)

Quality requirement	Example of an indicator
Accessibility	This information is easily accessible.
Appropriate amount	This information is of sufficient volume for our needs.
Believability	This information is trustworthy.
Completeness	This information is sufficiently complete for our needs.
Concise representation	The representation of this information is compact and concise.
Consistent representation	This information is consistently presented in the same format.
Ease of operation	This information is easy to manipulate to meet our needs.
Freedom from Error	This information is accurate.
Interpretability	It is easy to interpret what this information means.
Objectivity	This information is based on facts.
Relevancy	This information is useful to our work.
Reputation	This information has a reputation for quality.
Security	This information is protected against unauthorized access.
Timeliness	This information is sufficiently up-to-date for our work.
Understandability	The meaning of this information is easy to understand.

The above table can serve two purposes. On one hand, it can be used as a checklist when modelling data. On the other hand, it comprises the criteria that the data model should be tested against. Although the framework itself does not provide any standards, the quality dimensions summarised above can be used to

formulate the semantic quality requirements. These requirements are often assessed by domain experts who have the requisite knowledge and experience to provide comments on taxonomies for a specific domain. In many cases, such assessment is based on an initial draft version of the taxonomy (Piechocki and Felden, 2007).

5.4.10.2 Syntactic quality requirements

The syntactic quality requirements focus on the correct technical application of the syntax used. Various test activities are performed to this end in order to establish any technical inaccuracies. Various levels of technical testing activities can be identified for SBR, which uses XBRL as its syntax. The first layer is to check whether the taxonomy is 'well-formed XML' and complies with the requirements of the XML schema. The next layer demands that the taxonomy complies with the requirements of the XBRL 2.1 specification, as well as with several additional XBRL specifications.

When a taxonomy is determined to be valid for both XML and XBRL, it will next be examined in greater depth to ensure compliance with architectural rules. As discussed in §5.4.5, two architectural levels can be found within SBR: compliance with the FRTA rules and compliance with the NTA rules. In the SBR context, the NTA rules are seen as more up to date and relevant than the FRTA rules. Compliance of the taxonomy with FRTA and the NTA can mostly be checked using automated systems. In principle, all XBRL tooling has the FRTA requirements built in, so this can be checked easily enough. The SBR Programme has had custom tooling developed, which allows the use of automated systems to check most of the hundreds of rules included in the NTA. In the test phase, each version of a sub-taxonomy is run through this tooling to assess its compliance with the architectural rules. Because of the large number of rules required to limit the level of freedom in reporting, the testing simply cannot be done manually. After testing, the results are evaluated and inaccuracies in the syntactic processing of the taxonomy are resolved, if necessary.

5.4.10.3 External test activities

Consulting the interested market parties such as intermediaries or accounting firms is a method that is frequently used internationally to test the quality of a taxonomy. This practice contributed significantly to the semantic and syntactic quality of taxonomies during the early days of SBR in the Netherlands. However, in recent years it has become clear that mostly unpaid market consultations alone are insufficient to guarantee high-quality taxonomies. The number of responses by interested market parties is often limited to just a few leading parties. In addition, when market parties respond, they only focus on the elements that apply to them. The full taxonomy will therefore never be checked in detail by these parties. Actively approaching specific umbrella organisations to cooperate in such checks does yield higher quality taxonomies, but this testing is primarily aimed at the semantics.

Checking that the syntax is correctly applied has become more difficult over the last few years. The techniques have become more complex and only a limited number of people have sufficient knowledge of XBRL to conduct the checks. In addition, a vast number of taxonomies have been added internationally in recent years, leading to virtually no input from experts to public requests for unpaid comments. It is therefore very important to have the right technical experts available when constructing taxonomies.

5.4.10.4 Testing the Netherlands Taxonomy

The test phase of the NT is similar to what was described in the previous sections. If the draft version of the NT passes the internal validation, that version will be issued as an alpha version for each domain, together with the joint concepts that were previously issued. Multiple alpha versions will therefore be issued, at least one for each of the domains. The alpha versions are published on the SBR website so that they can be consulted by market parties.

Based on comments from market parties, the various requesting parties will provide beta versions of their sub-taxonomies to the SBR Programme. These various sub-taxonomies are then combined into one whole: the Netherlands Taxonomy. This version is known as the beta version and is also published on the SBR website for market consultation. Any responses and comments regarding the beta version of the NT are used by the requesting parties for the final version, which is issued every year. The process of creating the finalised NT is the same process as for the beta version.

5.4.11 *Publication phase*

The information requirements of a requesting party, as included in structured form in a taxonomy, are communicated to the market parties in the publication phase. The taxonomy itself is a technical collection of files that can be provided to the relevant market parties in various ways. For SBR, the NT is made available on the publication date in three form: as a .zip file on the SBR website, as a directly accessible taxonomy on nltaxonomie.nl and through a taxonomy viewing tool (see text box below). The most practical way to understand the structure and setup of the taxonomy is to navigate through the taxonomy using a tool that understands XBRL and has a query function. Reporting parties that want to use the taxonomy do not usually require special XBRL software. Their own administration software loads the taxonomy in the background and allows them to apply the mapping between the concepts of the requesting party and the concepts included in their own administrative data system.

Taxonomy viewing tool
The SBR Programme has made a taxonomy viewing tool available for visualising the NT. The taxonomy viewing tool offers functionality for examining the data types, labels, references and other properties of the information requirements for each type of report. This tool is available at www.taxonomy-viewer.nl.

Additional information is supplied with every new publication of a taxonomy. The parties that issue a taxonomy are required to provide additional documentation with it. For example, the SBR Programme stipulates that each taxonomy release should be accompanied by release notes, FRIS (Financial Reporting Instance Standards) documentation, versioning information, sample instance documents and a manual for drawing up an instance document. The SBR Programme views the issuing of these additional documents as a best practice, as it allows different users to gain familiarity with the setup and structure of the taxonomy, as well as any changes that have been made to it. These additional document types are described briefly as follows.

Release notes
The release notes contain the key differences in architecture and content between the previous version and the current version of the taxonomy. For the NT, a comparison is always drawn between the new version of the taxonomy and the previous finalised version. The release notes provide a brief textual summary of the changes that were made to the taxonomy so that users can quickly identify them.

FRIS documents
A FRIS (Financial Reporting Instance Standards) document describes the requirements that the XBRL instance documents must comply with. These are technical rules that determine whether an instance document is valid. One example might be the requirement for inclusion of at least three contexts in an instance document. Since the requirements imposed on an instance document cannot always be integrated into the taxonomy, these requirements are published in PDF format as additional documents. The documents have a similar format to the sections of the Financial Reporting Instance Standards 1.0 by XBRL International.

The NT has multiple FRIS documents, as illustrated in Figure 5.3. For example, there is an umbrella NL-FRIS document that contains the requirements imposed on the instance documents, which apply to all domains. In addition, each domain has a FRIS domain document of its own that defines a number of specific situations that only apply to the domain in question. The SBR Programme aims to restrict the list of FRIS rules as much as possible, as manual actions are required of parties who want to incorporate these rules into their software. Experiments carried out in 2012 to make the FRIS rules available as XBRL formulas, showed that this was possible. The FRIS document itself continues to record the descriptions of the rules.

Versioning information
Versioning information refers to recording the differences in content between two versions of a report in the taxonomy. This information can be provided in two ways. Firstly, it can be structured in a way that allows it to be read by computers in accordance with the versioning specification by XBRL International.

Secondly, it can be provided in a form that can be read by humans, for instance, in HTML format.

Sample instance documents
Providing sample instance documents gives the user an idea of what an instance document should look like when it is compliant with the requirements of the taxonomy. It should be emphasised that sample instance documents are just examples and therefore not generic templates that can be 'hardcoded' by software providers. The NT provides sample instance documents for each report and makes them available on the SBR website as additional documentation. Sample instance documents are examples of functionally and technically valid instance documents. This contrasts with test instance documents, which may contain deliberate erroneous situations in order to generate error reports. Test instance documents are not made available to the market.

Manual for creating instance documents
Users who have limited experience with XBRL are provided a domain-specific manual that deals with the way instance documents are created for the relevant domain. From 2011 onwards, the SBR Programme has provided a manual for creating reports in the financial accounting domain. The manual explains a range of issues that the user may face when drawing up a report. The SBR Programme aims to explain, in the clearest way possible for each domain, how an instance document should be created.

Administrative data system
From the points of view of uniformity and quality, it would be better to generate taxonomies from an administrative data system rather than creating them manually using specific software or text editors. The administrative data system contains a semantic dataset, including the reporting concepts with definitions, references and other relevant sources, as well as their interrelationships. In addition to supporting a semantic dataset and the required syntax, the data administration must also contain an accurate and transparent working method for making changes. This working method needs to be supported by a workflow component that only allows authorised users to make changes and which logs all changes in detail. Logging is also important for auditing the taxonomy creation process.

The one-off creation of a taxonomy and the associated validation rules are only an initial step in a larger process. After, the taxonomy and the validation rules end up as part of a management process. The taxonomy then needs to be changed periodically (often annually) to reflect the latest changes in legislation and regulations or as a result of new XBRL techniques being introduced in the taxonomy. To realise such change, it is important to maintain a proper data administration that maintains both the semantic and syntactic aspects of the taxonomy.

5.4.12 *Maintenance phase*

Maintaining a taxonomy involves activities that take place after the publication of the finalised version of the taxonomy. These activities are also known as 'operational support' and include answering questions and assessing notifications received about possible errors deriving from the taxonomy. Questions and remarks must be recorded and formally responded to. Reports about possible errors must be evaluated by the front desk, back office or even the development support staff. Domain experts and financial experts will often be included in this third line of support. Generally, notifications of possible errors can lead to the following four scenarios:

1. Unfounded notification, no further action.
2. Correct notification, will be addressed in the next taxonomy version.
3. Correct notification, must be resolved using a quick fix as soon as possible.
4. Correct notification, must be resolved by a new version as soon as possible.

The quick fix is considered a practical solution if only a single file in the taxonomy contains a significant error. As the error only affects a single file, only that file will be replaced. However, if multiple files contain major errors, a new version of the taxonomy will need to be published. The activities in the maintenance stage result in the following outputs: a registry of questions and/or error reports (dealt with or otherwise), a summary of changes to be made in the subsequent version of the taxonomy, and the quick fixes or new taxonomy versions issued, if applicable. The maintenance phase is complete when none of the business reports covered by a taxonomy are operational any longer.

5.4.13 *Relevant developments in data*

Two relevant developments in the data arena concern the validation of the business reports received and the possibilities for rendering or presenting data items in instance documents. Both developments are explained in detail as follows.

5.4.13.1 Validation of the business reports received

Reporting organisations send their business reports to requesting parties based on the information required, as stated in the taxonomy. The underlying idea behind SBR is system-to-system exchange and processing of information without manual intervention. This means that reporting parties can send their business reports to the requesting party in a secure manner. Those reports will then be processed by back office systems of the requesting parties, again automatically. Of course, it is crucial here that the requesting party validates the data from the business report against the various requirements for the data before the data is processed by the underlying information systems. Running validation rules increases the value of information and therefore results in high quality information that is more suitable for the intended purpose. It is important for the reporting organisations that errors are detected at the earliest possible stage. Validation routines can be performed at three levels:

1. the level of the sender (or the reporting party, if the latter is not the same organisation),
2. in the generic infrastructure (see the description of the validation service in Chapter 7) and
3. the level of the requesting party. Depending on the preferences of the requesting parties, multiple validation levels can be applied. Validation can occur directly upon transmission, pre-processing or receipt.

Validations must be performed to ensure that the reporting parties have observed the requirements imposed by the requesting parties. In addition, the reporting parties need confirmation that their submissions have been accepted to show that they have met their legal obligation—something in which validation also plays a key role. Within the SBR Programme, the following validation stages can be identified:

1. Validation of whether the business report is well-formed XML.
2. Validation of whether the business report complies with the XML schema specification.
3. Validation of whether the business report complies with the XBRL 2.1 specification.
4. Validation of whether the business report complies with the XBRL Dimensions 1.0 specification.
5. Validation of whether the business report complies with the international FRIS rules.
6. Validation of whether the business report complies with the NL-FRIS rules.
7. Validation of whether the business report complies with the domain's FRIS rules.
8. Validation of whether the business report complies with the domain-specific FRIS reporting rules.
9. Validation of whether the business report complies with the consistency rules (business rules).

The list above contains the various layers of validation performed as part of SBR. The first layers focus on technical compliance with the relevant standards and aim to determine whether a taxonomy is 'well-formed XML' and complies with the technical requirements of the XML schema. The subsequent layers deal with the technical requirements imposed by XBRL. For example, the taxonomy must comply with the technical requirements of the XBRL 2.1 specification. If the taxonomy contains dimensional structures, it must also comply with the XBRL Dimensional Taxonomies 1.0 (XDT) specification. This is actually a validation action to ensure that the syntactic quality requirements presented in §5.4.10.2 will be met. The following layers involve the correct use of FRIS rules at various levels, namely the NT level, the domain level or the entry point (reporting) level. Finally, consistency checks consider the semantic requirements, focusing on the correctness, completeness and accuracy of the document's content.

Validation rules can be programmed using various formats, but it is recommended that they be developed using an open standard. Since 2009, XBRL has included a specification for setting up validation routines using XBRL formulas. This open standard for creating validation rules focuses entirely on working with taxonomies and instance documents. It makes it possible to check the contents of instance documents for certain aspects that can be found in both the instance and the taxonomy. It is therefore best to create validation rules that apply when validating an instance document based on an existing taxonomy.

5.4.13.2 Rendering instance documents

Rendering instance documents in the same way as their paper equivalents is a requirement of most market parties, although doing so has proved to be quite difficult. In the early years of XBRL, when only the XBRL 2.1 specification was available, the presentation relationships in parent-child relationships could be represented using the presentation linkbase. This made it possible to define the concepts in business reports in a proper sequence, which was then used for the representation of the report. Rendering is not a problem for simple business reports, but poses a problem for reports that are more complex. The implementation of XBRL Dimensions 1.0 has made it possible to use dimensional structures in the taxonomy. Tables can now be included in a taxonomy as well. However, rendering these tables has turned out to be a problem, since the presentation linkbase does not support rendering for dimensional structures. For some projects, the choice was made to realise the rendering of instance documents and taxonomies using customised solutions.

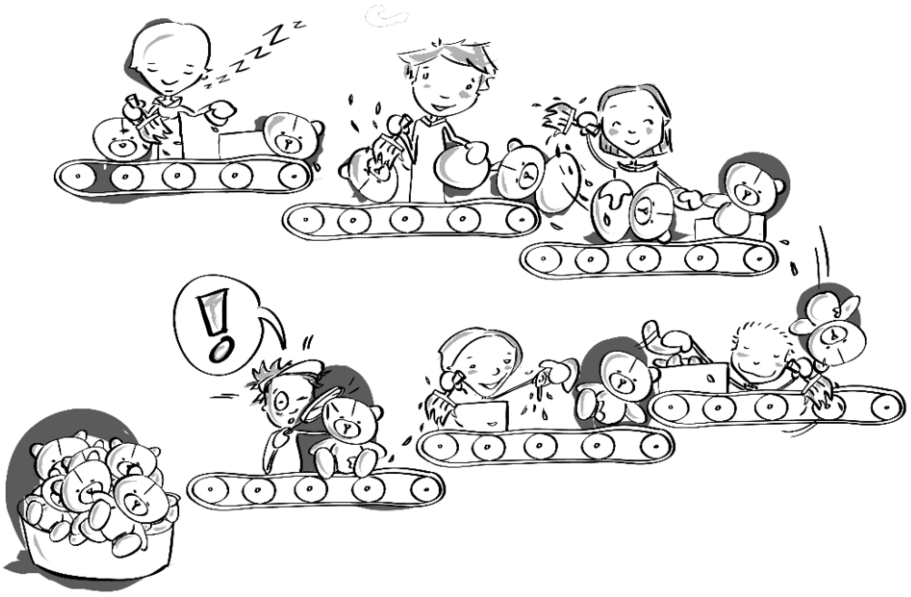
In 2011, the Inline XBRL specification was also issued for rendering instance documents. Inline XBRL combines the presentation capabilities of HTML with the communication strengths of XBRL. This specification also makes it possible to render data that is not available in XBRL format, creating the possibility that data that cannot be processed by automated systems can be made available for viewing by humans. This is why Inline XBRL is not an attractive option for many requesting parties. The table linkbase specification, published in 2014, is the most significant development in the rendering of instance documents. The table linkbase provides a standard means of rendering of the concepts included in an XBRL taxonomy. Dimensional structures are expressly addressed, ensuring that tables can actually be presented.

5.5 Chapter conclusion

In this chapter, we considered the subject of data in information chains. Communication needs, standardisation of syntax and semantics, legal requirements, the different perspectives (i.e. communication and presentation) and the development phases of a taxonomy were covered. XBRL was given much attention as a standard. An increasing amount of literature is emerging regarding XBRL, and the emphasis is usually on the possibilities created by XBRL for standardisation of syntax and semantics. This chapter's contribution to that field is the concrete description of how XBRL is actually applied in information chains. Our discussion has shed a different light on the possibilities, as well as on the efforts that are required to reap the benefits of XBRL. It is clear that XBRL plays a significant role in system-to-system exchange and processing of business reports and this significance will surely increase in the next few years.

Pinsker (2003) named XBRL a 'sleeping giant' that would trigger a far-reaching transformation of the business reporting sector and information chains over the coming years. SBR is only one example of such a transformation. From a research perspective and given the recent, relatively large-scale application of XBRL in chain information systems, it must be kept in mind that the literature still has gaps that require further research. Examples of these gaps include the conditions for effective application of specifications such as Inline XBRL, and success factors for the multi-domain application of XBRL (e.g., in the health care and education chains). SBR provides an empirical environment in which questions like these can be investigated.

6 I-processes



Chapter highlights

- Narrowing in on the umbrella term 'process'
- Learning how to classify, model, analyse and improve processes
- Getting acquainted with 'I-processes'

6.1 The umbrella term 'process'

This chapter is about processes and process specifications. First, we will deal with 'process' as an umbrella term. One specific category of process can be distinguished: information processing processes, which are also known as information processes (I-processes) in the literature. We will discuss the characteristics of working with I-processes and then take a closer look at SBR. In the context of SBR, a SSC carries out certain portions of I-processes for the exchange and processing of business reports.

In this chapter, we want provide guidance for applying the abstract concept of I-processes in a targeted way when redesigning information systems. We will start with the general characteristics of processes, after which we will use SBR as an example illustrating how these general ideas can be converted into a specific and structured process implementation and process management. Particular attention is paid to the standardised process components of SBR. The object of SBR I-processes is the XBRL instance (for a detailed explanation, see Chapter 5). Be-

cause of the generic infrastructure – which leads to S2S integration – these generic I-processes will mostly be processed by automated systems. Like the message specifications, the specifications for the I-processes define the services and underlying technology that allow the I-processes to be executed. These components are maintained and changed separately, but are closely interrelated. The chapter regarding the technical design of SBR (Chapter 7) will provide greater detail on this interrelationship. We conclude this chapter with a brief overview of outstanding issues with regards to the automation of I-processes and significant ongoing developments in this area.

In summary, this chapter will answer six questions that also comprise the sections of the chapter:

- **Section 6.2** – what is a process?
- **Section 6.3** – what is a good process?
- **Section 6.4** – what are the management philosophies concerning process improvement?
- **Section 6.5** – how can a good process be maintained?
- **Section 6.6** – what tools and methods can be used for design and maintenance?
- **Section 6.7** – what specific requirements are imposed on I-processes in SBR chains?

6.2 What is a process?

The simple definition of a process is a serial set of tasks with a predetermined objective. The notion of a process has broad applicability, which in practice, has positive and negative effects. The positive aspect is that the notion of a process is a generic formula that is applicable to many different fields of expertise, so there exists a great deal of literature about how processes can be set up and controlled. Various theories have been put forward that can be applied to virtually any process, from preparing a meal to handling an XBRL instance. A negative effect of the notion's high level of abstraction is that every practical situation requires a specific translation of what is happening at a given time and who/what is involved (from an overall setup to operation). This translation is difficult and cannot always be done. As a result, discussions get stuck in generalisations that will fit any definition of what a process is, as long as we think/model at a level 'where everything still seems OK.'

One example is the use of the standard ITIL change management process without critically examining whether the process is the most useful for the specific situation. The process model/description of the standard ITIL change management process provides no guidelines about what the management should do if there are differences in opinion. Another effect is an excessive focus on the 'happy flow', the ideal flow of how the process should work — often described in general examples and without taking exceptions into account. In practice, however, the quality of a process is determined by the way it manages to limit the exceptions and minimise their impact.

Reading this book can also be thought of as a process in which the reader goes through a number of steps with a set objective. The book must be located and opened, and the following step is actually reading it. In business studies and the organisational literature, processes are often seen as tasks that are carried out over time (Davenport, 1993). Davenport and Short (1990) define a process as *"a set of logically related tasks performed to achieve a defined business outcome for a particular customer or market."* Hammer and Champy (1993), on the other hand, define a process as "*a collection of activities that takes one or more kinds of input and creates an output that is of value to the customer. A business process has a goal and is affected by events occurring in the external world or in other processes*" (p. 53). This definition is aimed at transforming input by means of output activities. Carrying out individual tasks and looking at which tasks are associated with others yields a process description. Tasks receive input from the preceding tasks, creating output that can be used as input for subsequent tasks. When describing or modelling processes, it is not only important to focus on the individual tasks, but also on the connections between the various tasks, and the relation between the input and the output that provide the added value of the entire process.

Another definition of a process is "a lateral or horizontal organisational form, that encapsulates the interdependence of tasks, roles and people, departments and functions required to provide a customer with a product or service" (Earl, 1994, p. 13). This definition is formulated from an organisational perspective and focuses on tasks, roles and the people who perform the tasks. An organisation may have various roles, where 'actors' are people who perform a certain task based on a role. People may carry out multiple tasks and roles. At an abstract level, a role refers to what a person must do, without going into the specific functions and tasks involved. A role is therefore an abstract way of looking at the tasks to be completed.

Weske (2007) defines a process as "*a set of activities that are performed in coordination in an organisational and technical environment. These activities jointly realise a business goal*" (p. 5). His definition highlights that an environment consists of both organisational an technical components. In additional, this definition highlights that processes are meant to realise a business goal. The latter is important, as the goal provides clarity about the conditions that a process must fulfil. If the goal changes, it can have consequences for the process architecture. While the goal addresses the question of 'what,' processes address the question of 'how.' Processes describe how a chain or organisation realises its goal.

The elements of processes are summarised in Table 6.1. Actors are those who perform the tasks. They can be human (a person or a team), or automated (software) if an electronic task is involved. Performing processes uses resources — for example, the time that a person spends on a task or the time that a server needs to complete an activity. A relevant question here is whether or not the tasks are carried out by automated systems. It is typical of information chains that many tasks are carried out by automated systems.

One specific type of task in processes is the decision. A decision implies that the actor involved has some kind of mandate in making a decision. Since, actors are involved, their state/condition affects how the process is performed. Take, for instance, an example in which the information required to perform a process is incomplete/incorrect or the person responsible for performing the process is ill. Actors are part for the environment in which processes occur. Interruptions often begin in the environment. Depending on the context, it might be possible to influence the environment to some extent. Six Sigma, in particular, focuses on reducing interruptions (see §6.4.8).

Table 6.1 – Elements of processes

Process elements	**Description**
Actor	The person or system carrying out a certain process step.
Resources	The things required to carry out a manual or automated task. A manual task uses the time and effort of the actor. An automated task uses, for example, the processing capacity of the hardware.
Input	The things required to start the first task in a process or that are carried over from previous tasks in order to carry out a subsequent task. Input is often information and decisions from preceding steps.
Task (transformation)	The task that transforms input into output.
Decision	A specific task in which a decision is made.
Task performance	The way a task is carried out (electronically, manually, etc.).
Environment	The environment affects the process and may affect the course of the process and the predictability of that course
Output	The result of the task, which can be used as input for subsequent tasks.
Goal	A process is goal-oriented in the sense that the execution of various tasks is aimed at achieving a specified outcome.
Process owner	The party responsible for the course, management and improvement of the process, from start to finish.
Process control (or steering)	Process control ensures that the next task will be started after the previous one is completed. It also intervenes in the event of irregularities, such as tasks that take longer than specified.

A process, particularly in information chains, often spans multiple organisational units. Such units can be departments or even different organisations. Whereas actors are responsible for a specific task and departmental heads are responsible for tasks within their departments, process owners are expected to monitor and manage the bigger picture. Process owners are often responsible for process steering, ensuring that the process runs smoothly from start to finish. They should also implement improvements in the process if necessary. Appointing process owners for each process within an organisation is seen as a sound organisational principle. The process owner can then implement mechanisms to ensure that the processes run smoothly and that they can be evaluated and improved.

6.2.1 *Process classifications*

Processes can be classified in various ways, for instance differentiating between:

- Physical and informational processes
- Primary, controlling, supporting and strategic processes
- Chain, business and subprocesses
- Processes with high and low degrees of automation
- Frequent and occasional processes
- Structured, semi-structured and unstructured processes

We often associate the term 'processes' with physical and operational processes. This chapter, however, focuses on I-processes (those that are about information or do something with information). Still, a number of the theories we will discuss can be applied to physical processes. There is an essential difference between physical or operational processes and I-processes though, as was discussed in Chapter 2. While physical processes can often be seen with the naked eye, the same would be difficult or even impossible to do with I-processes. Besides operational processes, there are also supporting processes, including financial, human resource management (HRM), steering and change processes (Armistead, Pritchard and Machin, 1999).

From a systems perspective, a distinction is often made between primary, control/steering and supporting processes (Weske, 2007). Primary processes are the backbone of the chain and contribute directly to the performance of organisations. If these processes fail, the chain stops functioning. Control/steering processes are required to steer the primary processes, either in the short or long term. Supporting processes ensure the continuity of primary processes, for instance, by hiring personnel. They provide the environment in which the primary functions can be performed efficiently. In addition, there are strategic processes, which are focused developing and implementing strategies.

Processes can also be classified by aggregation level. A process can be decomposed into smaller parts, from top to bottom. This breakdown into finer parts is important, as various actors are only involved in some levels of the process and are therefore only interested in certain levels, and each level has its own issues. An organisational unit that performs a process can be seen as a link in a chain of processes.

Another useful way to classify processes is by their level of automation. Some processes are fully automated and are therefore able to handle larger volumes. However, other processes require human activities, for instance, in the evaluation of conflicting rules and decision-making. Structured, high-volume I-processes are best suited for automation and the achievement of scale and efficiency benefits.

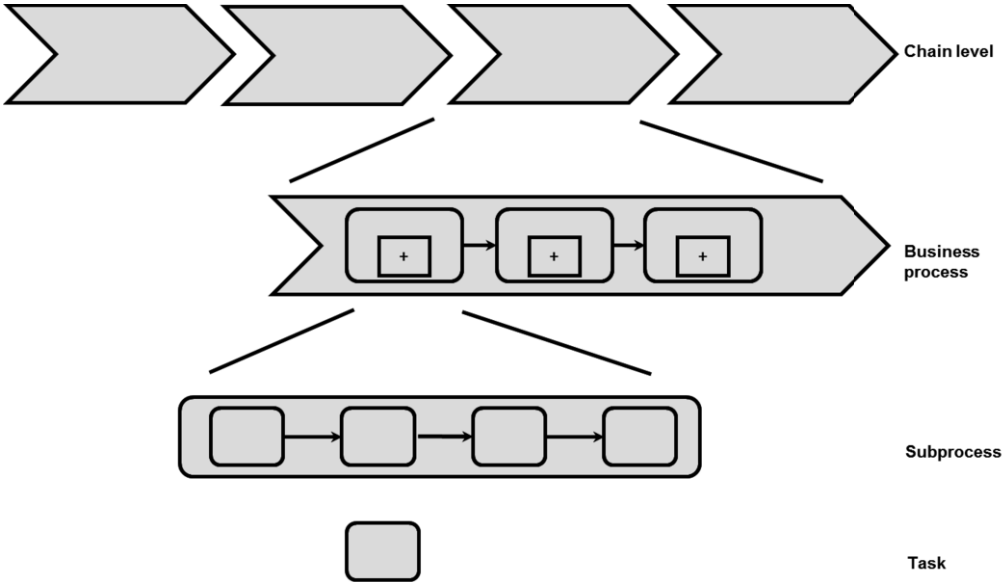


Figure 6.1 – Breakdown of chains into tasks

Further classification is possible when considering the degree of repetition in a process. Investing in processes that are frequently used provides a greater return. High efficiency is important for high volume processes, whereas it is less crucial for occasional processes.

A final important way to classify processes is by how well structured they are. Well-defined and standardised processes are usually reliable, proven and will lead to predictable outcomes. Unstructured processes, on the other hand, are difficult to follow and may have unexpected outputs. Most strategic processes fall into the latter category. Semi-structured processes often have a clear sequence at a high level of abstraction (e.g., requesting, collecting information, making decisions and communicating), but their specific tasks can be carried out in multiple ways.

SBR reporting chains involve processes with various classifications. Within a company, reporting can be characterised as a process that is carried out a few times a year and which does not necessarily need to be automated or structured (think of the well-known 'shoebox with receipts' as part of a tax declaration). However, as the SSC handles millions of messages per year, its processes are primary processes that should be fully automated in order to handle that large volumes. Figure 6.2 below illustrates the process characteristics for the various actors within one reporting chain.

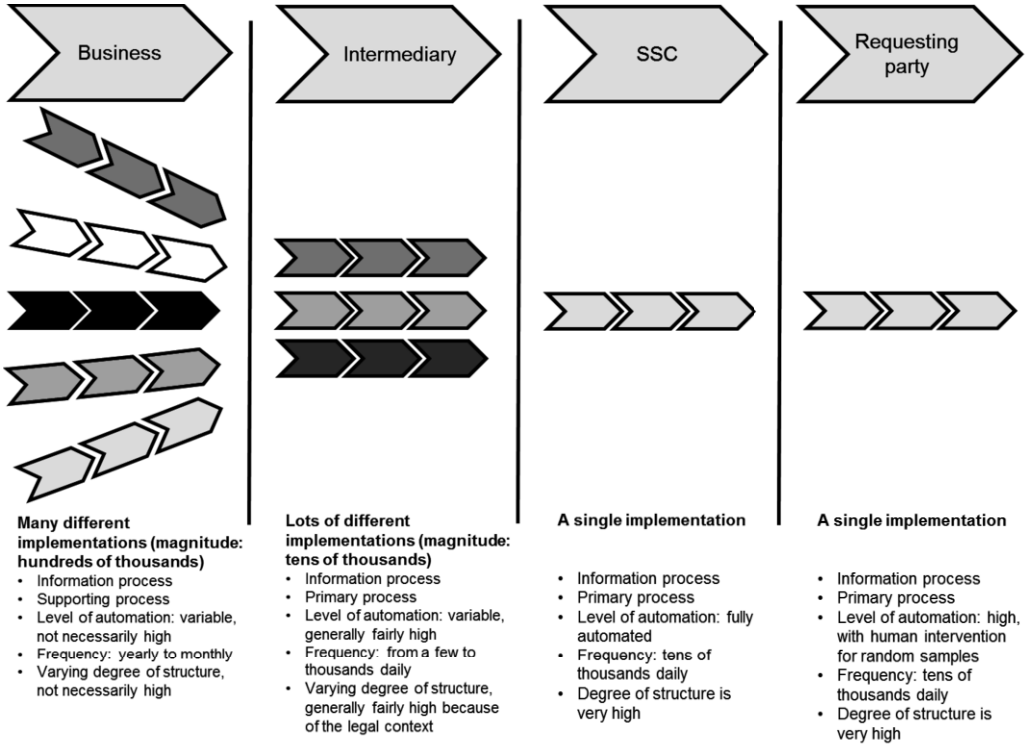


Figure 6.2 – Process characteristics for the links within one reporting chain

6.2.2 *Process harmonisation for SBR*

The presence of intermediaries in reporting chains can be explained, in part, by efforts to achieve cost-effectiveness. Specialist knowledge is required, for instance, when compiling a proper declaration or financial annual report. Some specialist organisations generally do have this type of knowledge, and – according to core competency theory – it may be beneficial to outsource none-core tasks to specialists (Drejer, 2002). The specialist (in this case, an intermediary) has multiple clients and therefore handles the specific process fare more often. Since handling certain processes is the core-activity of the specialist, competition and other cost drivers will require it to keep investing in process structuring and process automation. Process automation improves the quality of the total reporting chain and reduces the overall transaction costs. For information chains, automating information processes requires the various requesting parties to standardise the way that they want business reports declared. This allows the businesses and intermediaries to further harmonise process components for several types of reports, resulting in even larger volumes for the same process. As discussed in Chapter 1, economies of scale – the cost advantages that enterprises obtain due to size, output, or scale of operation, with cost per unit of output generally decreasing with increasing scale as fixed costs are spread out over more

units of output – make it worthwhile for intermediaries to keep investing in process structuring and process automation.

Based on the XBRL taxonomy described in Chapter 5, multiple business reports can be generated automatically from a single administrative dataset, leading to the slogan 'store once, report to many.' This means that reporting parties can use the same dataset for submitting reports to various requesting parties. Consequently, the SSC and the requesting parties can handle various I-processes using automated systems. Again, the taxonomy is key for automating on the process level. Standardization of syntax and semantics allows for reuse of generic infrastructure components. For instance, the validation service can be applied to variable message content. Considering the benefits, some large accounting firms have implemented process standardisation in the reporting processes they handle for their clients.

6.2.3 *Black box, white box*

When various processes are interconnected within a chain, the organisations involved can view each other's connections from a black box or from a white box perspective. From a black box perspective, apart from their own process, organisations are only interested in knowing about the right interfaces with the upstream and downstream organisations. The nature of the processes in adjacent organisations is unimportant, as long as they provide the expected output based on the requested input. From a white box perspective, on the other hand, the organisations analyse each other's processes down to the lowest level. Both perspectives have their pros and cons.

The advantage of the black box perspective is that less effort is expended in chain coordination. On the other hand, this perspective may lead to a non-optimal chain design, as parties, may be duplicating activities without even noticing it. Furthermore, items such as end-to-end security may get less attention than they deserve, since chain partners are only focused on the organisations they are in direct contact with and not those further up the chain. A partner with weak security measures in place can therefore undo all the security investments by the others. The opposite may also occur, with each chain partner investing in security measures for the interface that are actually unnecessary, given certain security controls elsewhere in the chain. However, it should be noted that, from the perspective of competition amongst organisations, actors may prefer to use a black-box approach.

A white-box approach provides the possibility for a lean setup of processes since all the chain processes are described. Duplication of activities will be noticed sooner. It will also be easier to identify and compare the various controls along the various organisational processes. The main disadvantages of the white-box approach are high participation costs (organisations needs to study each other's processes) and the risk of going into too much detail during harmonisation efforts and failing to keep an eye on the bigger picture.

There is some middle ground between the black-box and white-box approach. In a 'grey box' approach, parties are only transparent (white-box) on key process aspects. In some cases, a more closed, black-box approach is used to focus solely on the input and output.

Within an SBR reporting chain, the expert group processes and technology (see Chapter 9) use a grey-box approach. The various chain partners only discuss key aspects such as the way they handle incidents or end-to-end security, but they are not fully informed about all processes of the other parties.

In addition, a range of black-box and white-box relationships can be identified within SBR chains. For instance, the requesting parties are interested in the level of detail of the processes handled by the SSC. This interest is logical, as requesting parties are highly dependent on the SSC. The SSC must have a certain degree of awareness regarding the processes of the requesting parties as well, along with the developments or expected changes regarding these processes. This awareness allows the SSC to assess the impact changes may have on the chain process and what the other parties in the chain can expect from the SSC. This is an example of a white-box relationship.

An example of a black-box relationship can be found in the level of description of the processes of intermediaries and reporting parties. There are considerable differences in the way that intermediaries and reporting parties operate, causing things to be much less transparent. However, a considerable number of intermediaries (e.g., chartered accountants and accounting consultants) are required to operate in accordance with certain process guidelines depending on the professional association they are affiliated with.

The SSC provides insights into its processes by means of process specifications – one of the building blocks of SBR. A process specification is a description of the way the requesting party wants to process the data submitted, or a description of the I-process. In addition providing descriptions of the way processes are defined or designed by chain partners, the parties may also be interested in the question of whether a chain partner really operates as expected. For example, in the case of the SSC, it may be useful to have an independent qualified third party issue an audit statement. A third party audit statement with the right audit scope will allow the SSC to be transparent and openly accountable to all its partners at the same time.

In brief, such a third party statement should at least cover on the following claims:

- The SSC handles the agreed-upon processes in accordance with the process specifications. These specifications provide insights into the subprocess level (see Figure 6.1).
- The SSC has taken sufficient technical and procedural measures in order to guarantee service delivery based upon the agreed service levels.

On a side note, we see a trend in which organisations expect other chain partners to adopt a proactive attitude and to inform each other when mistakes are made in a process. This trend can be labelled as providing 'chain transparency'. In the Netherlands, initiatives such as 'horizontal monitoring' mirror this trend. The State Secretary's letter of 8 April 2005 to the House of Representatives of the States-General explained horizontal monitoring as follows:

> *"Horizontal monitoring refers to mutual trust between the taxpayer and the Netherlands Tax and Customs Administration, the more precise specification of each other's responsibilities and options available to enforce the law and the setting out and fulfilment of mutual agreements. In so doing, the mutual relationships and communications between citizens and the government shift towards a more equal position. Horizontal monitoring is also compatible with social developments in which the citizen's personal responsibility is accompanied by the feeling that the enforcement of the law is of great value. In addition, the horizontal monitoring concept also implies that enforcement is feasible in today's complex and rapidly changing society solely when use is made of society's knowledge."*

The statement expresses the essence of horizontal monitoring in relation to external parties such as tax service providers. This horizontalisation of the compliance activities will primarily be achieved, in cooperation with the relevant parties, by shifting the supervisory/regulatory process from retrospective inspections to advance consultations in combination with meta-monitoring. This cooperation will be based on mutual trust, understanding and transparency. In adopting this approach the Netherlands Tax and Customs Administration will be able to reduce the red tape imposed on entrepreneurs who file correct tax returns and devote more attention to higher-risk tax returns.

We can also look at the chain transparency trend from a contrasting perspective. In the movie *Fight Club*, one of the main characters expresses a cynical perspective of a car manufacturer, as being one that determines how to handle manufacturing defects purely from its own financial perspective:

> *"A new car built by my company leaves somewhere traveling at 60 mph. The rear differential locks up. The car crashes and burns with everyone trapped inside. Now, should we initiate a recall? Take the number of vehicles in the field, A, multiply by the probable rate of failure, B, multiply by the average out-of-court settlement, C. A times B times C equals X. If X is less than the cost of a recall, we don't do one."*

This dark-humoured scenario is very different from the chain transparency trend in which actors communicate with one other about the way to tackle problems within a chain based on the interests of the entire chain as well as 'softer' values such as the environment, consumer safety and animal wellbeing.

6.2.4 *From business process to IT process*

Generally, I-processes create a context in which business professionals and IT professionals can communicate. Figure 6.3 depicts a decomposition of processes. Business professionals will likely be more focused on describing the upper part of the figure, whereas the lower part may be more relevant for IT professionals.

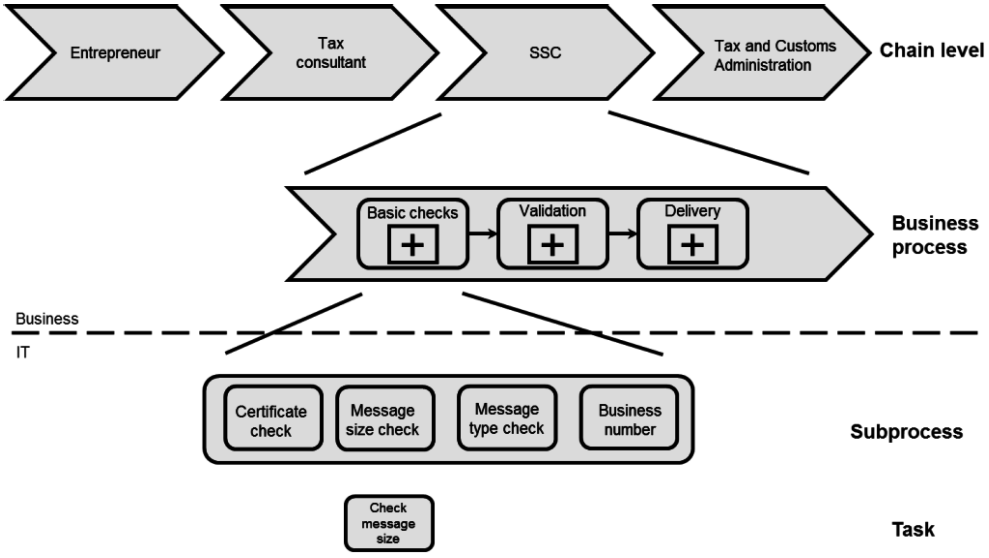


Figure 6.3 – From business process to IT process

Business professionals usually think in terms of how to create value and what is required to do this. IT professionals usually focus on how to build the required functionality for completing a task, deciding which tasks can be handled by automated systems and which technology is most suitable to do so. Therefore, when modelling processes, it is important to choose an abstraction level that is relevant for your audience (business vs. IT professionals). We return to the process modelling theme in section 6.5.

6.3 What is a good process?

A proper process ensures that the goals of the process are actually achieved, with the predefined output being realised in the shortest amount of time, for the lowest possible cost and with a minimum of resources. With these indicators, it may seem easy to evaluate a process, but the reality is much more complex:

- Time, money and resources may impose competing requirements. For example, the throughput time may go up as cost efficiency increases.
- The evaluation may depend on whether the indicators are applied to the process or the overall context. Are we aiming for an efficient chain or an efficient organisation (as part of the chain)?
- The focus on efficiency may conflict with human values. The depth or breadth of the tasks determines the motivation of the people tasked with

carrying out the process. Consider the resistance that the Dutch railways faced against plans to limit the number of routes individual train conductors could work: this would be more efficient and lead to fewer delays, but would be too boring for the conductors.

- Repetitive processes always involve averages and distribution patterns. The following considerations may play a role: a throughput time that is short on average but with a large variance may sometimes lead to long throughput times. The alternative is a throughput time that is longer on average but with little variation, resulting in fewer negative outliers.
- Information security and/or protection of the general interest of actors, may require the implementation of measures that reduce the efficiency of the process. Authentication for instance – such as the mandatory use of a complex password when logging in or using digital certificates – makes the process cumbersome, but safer.
- Sometimes carrying out a process is a goal in itself, as with playpen processes (e.g., in which the puzzle was not solved or the match was lost, but the process was fun).

Organisations assess the quality of processes against their own values. In this assessment, they are more or less attracted by competing extremes such as (based on Cameron and Quinn, 2006):

- A good process consists of a dynamic and innovative way of working.
- A good process consists of an efficient and structured way of working.
- A good process consists of a way of working that is highly aligned with the needs of the market.
- A good process consists of the most harmonious way of working (from a human perspective).

The process designs in SBR are sometimes subject to the tension between architects primarily focused on efficiency, and architects focused on first fulfilling the customer's needs in the design. One clear example of this is the tension between internally-oriented but efficient government (i.e. small government) and externally-oriented, service-minded government. The pitfall for the efficiency-oriented architect is alienation from practice. Although this perspective may ensure the efficient operation of the government, the private chain partners can only comply with the requirements imposed by the government by means of expensive constructions. In this case, the perceived administrative burden, as well as the image of uncoordinated government, remains. The pitfall for service-minded architects is that they want to serve all possible needs in the market, which makes the government's process (or the process across the entire chain) needlessly complex and expensive. If 99% of the private chain parties involved are required to deal with a 'more complex' process so that the remaining 1% of companies will not have to make changes, questions will likely be raised. Moreover, internal process handling by public parties will become more expensive when attempting to cater for all the various wishes of the market.

For SBR, the two opposite architectural pulls balance each other out, thanks to clear assumptions set beforehand and the time-boxing approach. The chain governance is set up so that it has a complete picture of the end-to-end chain process. Much attention is paid to defining the target groups and dealing with them separately, if necessary, rather than forcing them through a uniform process. Exceptional cases and request by market parties are subject to processes of their own. Such an approach is customer-friendly, but can be inefficient. Thus, reuse of services and infrastructure components is essential. A grey-box approach is used to make sure that parties behave transparently towards each other on essential points but only focus on the input and output in other aspects.

As discussed above, it is difficult to provide a clear definition of a good process, However, there are a number of variables that can be used to influence process quality. In the context of information chains, we define a good process as one that:

- is performed with a clear goal in mind.
- is as simple as possible.
- has the minimum number of defects and minimum downtime.
- restricts any effects or exceptions to 'mainstream performance' to a minimum.
- is executable.
- is scalable.
- is manageable and controllable.
- contains no activities that do not add value.
- causes a minimum amount of waste.
- complies with the values of the organisation.
- is aligned with the strategy and policy of the organisation.
- complies with legislation and regulations.
- has an owner.
- can be communicated.
- includes clear performance expectations.

The list is a non-exhaustive overview of process characteristics that can be included in a process design or evaluation. Process analysts can search for the desired optimal state as a function of the context. When a process scores poorly on one of the points, such a result should be very clearly justified.

6.4 What are the management philosophies concerning process improvement?

There are always processes that can be improved. External incentives generally trigger a process review. Such incentives can include, for example, the need for cost savings, competitors with shorter delivery times, new information security guidelines, wanting to promote the business as sustainable, or a major incident that led to the loss of business reporting information. In principle, it is a good thing for an organisation to review processes to make specific improvements. However, the risk is that the scope of the improvement may be limited and that

the improvements are not made because of competing quality requirements imposed on the process. Over time, a narrow scope may create undesirable effects. On the other hand, a wider scope may cause 'better' to become the enemy of 'good.' Organisations then move from one implementation to another, which may pose a problem since businesses do not operate cost-effectively during overhauls. Process improvement is therefore a recurrent topic and has been attracting attention of managers and scholars for decades.

Over time, several movements have promoted process orientation. Process-oriented thinking emerged in the industrial age, when production processes were being carried out by automated systems for the first time. Over time, the service sector has also adopted some of these ways of working, and they are increasingly being used in the government arena as well. Many of these movements are the result of management philosophies that are based on certain assumptions. In this section, we will take a detailed look at a number of these management philosophies and will apply them to SBR where possible.

6.4.1 *Business process re-engineering (BPR)*

Business process re-engineering (BPR) is a management philosophy that assumes that fundamental and radical restructuring of business processes is required to achieve significant improvement in organisations. In addition, automation should support the redesigned processes. Numerous process design principles have been developed since the emergence of the BPR management philosophy and a number of them can be seen as universally applicable (O'Neill and Sohal, 1999; Weerakkody and Dhillon, 2008). In 1990, Hammer presented the following guiding principles of BPR:

1. Organise around outcomes, not tasks. This may lead to various tasks being combined. According to the principle, related information required for a specified result should be centrally controlled.
2. Have those who use the output of the process, perform the process. This will ensure that the performing parties are responsible for the right output and will be affected by poor output. If they experience the consequences of errors, they are more likely to implement improvements.
3. Subsume information-processing into the work that produces the information. This will ensure that activities are clustered logically.
4. Treat geographically-dispersed resources as though they were centralized. Information technology allows firms to virtually centralize their resources, aggregating resources from multiple locations. Economies of scale are then used to decrease costs and avoid a 'here-and-there' mindset.
5. Link parallel activities instead of integrating their results. This prevents any errors when integrating the outcomes of various tasks.
6. Place decision making where the work is performed, and build control into the process. This principle can be broken down in two parts. The first part builds on the logic that those who carry out the work also have the most knowledge, enabling them to make their own decisions. The

second part suggests that the process checks and inspections be included in the primary task. Checks and inspections should require minimal overhead and should be performed as close to the tasks as possible.

7. Capture information once and at the source. Information that is gathered at the source has fewer chances for the introduction of along the way.

Later, Hammer and Champy (1993) presented two additional principles for BPR:

8. Processes have multiple versions to make them customer-oriented. To meet the demands of today's environment, organisations such as an SSC may need multiple versions of the same process, each one tuned to the requirements of different reporting domains. What's more, these multi-version processes must have the same economies of scale that result from mass production. Processes with multiple versions or paths usually begin with a "triage" step to determine which version works best in a given situation.
9. A case manager should act as a clear point of contact for customers to avoid that customers have to call various departments, each of which suggesting to contact another department. Functioning as a buffer between the complex process and the customer, the case manager behaves with the customer as if he or she were responsible for performing the entire process, although that is seldom the case. To perform this role the case manager either needs access to all the information systems that the people actually performing the process use or the ability to contact those people with questions and requests for further assistance when necessary.

The application of some BPR principles can be seen at various levels of the SBR design process.

Principle 1: Organise around outcomes, not tasks.
In SBR chains, the job of providing support for connecting up parties (connection support) is assigned to an account manager that has knowledge of the following

- The business domain (e.g., accountancy, tax legislation)
- Data – creation of an XBRL instance (see Chapter 5)
- Processes – the way that business reports are handled by the government
- Technology – the use of digital certificates and web services.

Such knowledge allows the account managers to continue supporting a party until the required result has been achieved—that is, the software provider is able to use the source data to create a valid instance and can submit it using the generic infrastructure of the Dutch government (also known as Digipoort).

Principle 3: Subsume information-processing into the work that produces the information. The providers of accounting software and reporting tools make it possible for an organisation to keep accounts that can be monitored

by an auditor. The well-known image of a shoebox full of receipts is slowly disappearing. Certain tasks can therefore be built into the chain at an early stage.

Principle 6: Place decision-making where the work is performed and build control into the process. SBR capitalises on the trend in which software providers are building more and more checks into administration and reporting software. The taxonomy used for SBR allows testing against reporting rules without interpretation. The generic infrastructure provides phased feedback regarding successive validations. Accordingly, reporting parties will immediately be informed if a message fails to comply with the acceptance requirements.

Principle 7: Capture information once and at the source.
'Data at the source' and 'store once, report to many' form the bedrock of SBR chains. Businesses can report to the various requesting parties on the basis of a single administrative dataset.

Principle 9: A case manager must provide a clear point of contact for customers. Some financial consultants have recently started working with relationship managers that are responsible for maintaining contact with customers. Auditors and tax specialists thus no longer need to do this.

6.4.2 *Theory of Constraints*

The theory of constraints (ToC) states that a process is dependent on its bottleneck (Goldratt, 1997; Goldratt and Cox, 1984). A bottleneck is any resource whose task capacity is equal to or less than the demand placed upon it. A non-bottleneck is any resource whose task capacity is greater than the demand placed on it. In information chains, several resources (i.e. interface and processing services) may become a bottleneck depending on the demand placed on it. Unsurprisingly, the common idiom 'a chain is no stronger than its weakest link' is inherent to the TOC.

The performance of the entire chain can only improve after the bottleneck has been addressed, as is shown in Figure 6.4. The illustration in A depicts the bottleneck. The throughput time in B is the same as in A, despite increased capacity prior to the bottleneck. The flow subsequent to the bottleneck will only increase if the bottleneck is addressed. The link where the bottleneck exists must be the focus of the improvement action. Once the weakest link has been improved, there will be a new weakest link that needs improvement. There will always be a bottleneck somewhere. The idea behind ToC is that in determining areas for improvement, everything else should be subordinate to the bottleneck in order to improve the process.

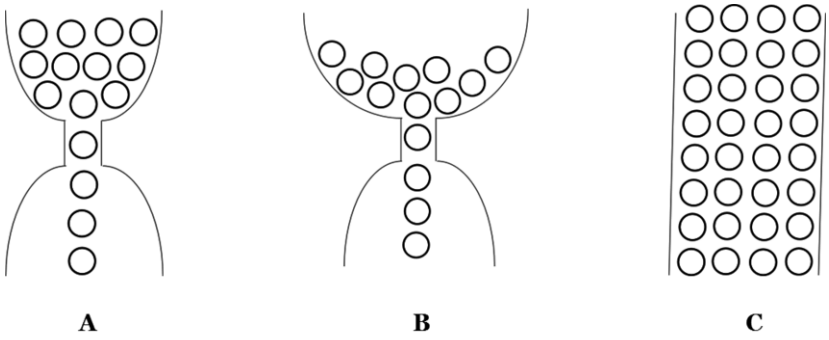


Figure 6.4 – A) visualisation of a bottleneck situation, B) process improvement, but the bottleneck has not been addressed, and C) situation without a bottleneck

The use of buffers and queues is important from a ToC perspective. If the bottleneck blocks the process, a 'gap' in the (message) delivery will immediately be created, whereas a temporary interruption in the process prior to the bottleneck can be compensated for. This effect is illustrated in Figure 6.5.

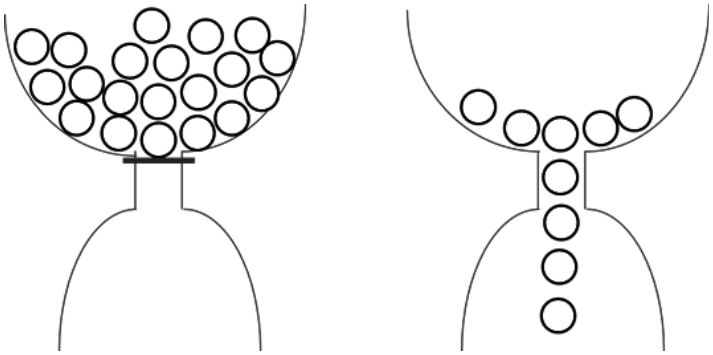


Figure 6.5 – If the bottlenecked process fails, it will immediately create a permanent gap in the production. The same will not occur if the supply before the bottleneck is temporarily interrupted, as production can continue as long as the buffer is not empty.

The buffers also reduce variation in processing time. The use of buffers in processes, however, conflicts with the principles of 'lean' (see section 5.4.3), which sees them as avoidable waste. Although temporarily storing messages in information chains is less expensive than storing production materials in physical chains, having a buffer does sometimes require the storage of confidential information. The security measures required for such a situation can be very expensive, and there exists an additional risk location from where information can be stolen.

The principle of the ToC is often used in hospitals, where specialists are scarce and expensive, and where process management is primarily focused on ensuring

that specialists are working continuously. The consequence is that many people are left sitting in waiting rooms, a totally different effect from the concept of straight through processing, which will be discussed later on in this chapter. According to the ToC, the following steps can be taken to improve processes (Goldratt, 1997):

1. Formulate the exact objective of the process.
2. Identify the bottlenecks (the task that may delay the other tasks).
3. Make sure that optimum use is being made of the bottlenecked area by identifying its constraints. Buffers may be useful and mathematical planning methods can help identify the constraints.
4. All other tasks and activities are made secondary to the bottleneck (short-term planning).
5. Address limitations and make sure that the bottleneck is resolved (long-term planning).
6. Start again at Step 1.

While the ToC provides guidelines for improving throughput time and efficiency, it can also be seen as a management philosophy. Yet, there may not only be bottlenecks in terms of time, since a bottleneck may also involve (1) the task with the greatest risk of failure, (2) the task that requires the most manpower or (3) the task that is the most expensive to complete.

The processes and technology expert group in SBR (which consists of public requesting parties and Logius/the SSC) is responsible for identifying and solving bottlenecks in SBR chains. In recent years, various bottlenecks have been identified and resolved within the SBR processes. We will discuss four of them:

1. The validation service in the generic infrastructure.
2. The link between the generic infrastructure and the requesting parties.
3. The mandatory use of an authorisation service provider (AuSP).
4. The distribution of digital certificates.

The generic infrastructure is managed by Logius – the SSC for the public agencies in SBR chains. The most archetypical bottleneck was the validation service in the generic infrastructure. This service validates an instance (XBRL message with business reports) against the Netherlands Taxonomy. To do this, the validation agent must generate the proper validation 'scheme' based on the endpoint in the instance with the taxonomy. The validation service was a classic bottleneck for processing capacity. The processing time per business report would increase quickly if the validation service needs to deal with a large number of different types of business reports (such as financial statements, VAT declarations, corporate income tax declarations, etc.). The SBR solution therefore decouples message delivery and processing within the generic infrastructure, thus having separate interface services and separate processing services. This decoupling makes it possible for the validation service to create a buffer, which may prevent process failure during peak loads.

Another bottleneck that existed in SBR was the link between the generic infrastructure and the requesting parties. When a requesting party could not be reached for a short period (longer than two minutes), the process sent a technical error message to the sending party. This meant that the reporting party had to resubmit the business report later. Decoupling between data send to the generic infrastructure, processing and delivery to the requesting party, enables further improvement of the I-processes. However, decoupling did not immediately resolve all of the identified problems. Within the generic infrastructure, the required buffer functionalities needed to be set up first. In addition, the requesting parties needed to adapt to an interface that allowed a business report to be resent.

A bottleneck of a different nature was the mandatory use of an AuSP for submitting business reports (see Chapter 1). In the original situation, intermediaries were required to use a commercial AuSP that provided assurances of their authorisation to file business reports on behalf of their clients. The intermediary (e.g., the tax consultant) needed to demonstrate that he/she had been authorised by its client to handle its tax matters. This relationship was included in a registry that was checked by the generic infrastructure during the submission process. The AuSP was seen as a bottleneck or even a roadblock for several reasons:

- The AuSP market was not mature: there were few providers to choose from and the process for the registration of approvals (authorisations) was inefficient. The throughput time for connecting to SBR was determined by the throughput time of this process.
- Previously, fiscal/financial service intermediaries did not have to deal with commercial AuSPs. Consequently, they experienced the costs associated with the registration of authorisations as an additional burden.
- There was only a limited framework of standards for fulfilling the AuSP role. Nothing had been set up for entering the market or supervision. This raised questions about the effectiveness of the mechanism.
- Intermediaries wanted to reduce their dependency on third parties to complete their services. For example, an intermediary could not submit business reports in the event of an interruption to the AuSP's service.
- The gains to be made by the unauthorised filing of tax declarations are limited. In addition, the company with formal reporting obligations will always receive the declaration on paper. Therefore, unauthorised tax reports/declarations will be noticed later. If the authorisation facility is operating properly, the unauthorised submitter of business reports can still be traced.

Chapter 8 provides a detailed discussion of the problems regarding authentication and authorisation. For our current discussion, it is sufficient to indicate that a number of measures have been taken to resolve the bottleneck. These include:

- Using a stronger authentication mechanism (i.e. public key infrastructure government certificates) is required.
- The use of an AuSP has been made optional.

- Status information regarding a declaration can only be requested by the reporting party (self-filer or intermediary).

The distribution of public key infrastructure government certificates could also have been seen as a bottleneck in 2012. Working with certificates was nearly the only option for authentication in system-to-system traffic. Furthermore, only a limited number of parties in the Netherlands were allowed to issue certificates in accordance with the public key infrastructure government. Nevertheless, all parties that wanted to submit corporate income tax declarations to the Tax and Customs Administration as of 2013 needed to have such a certificate. There were 11,000 such parties at the time. In addition, the DigiNotar affair[10] in 2011 had made painfully clear what happens when a certificate service provider can no longer be considered reliable. The SBR programme dedicated significant attention to resolving this bottleneck for connecting to SBR.

6.4.3 *Quality management concepts*

Over the past decades, different quality management concepts, including total quality management (TQM), Six Sigma and Lean, have been applied by many different organisations. TQM emerged in Japan during the 1980s and is often defined as a continuously evolving management system consisting of values, methodologies and tools, with the aim of increasing external and internal customer satisfaction while using a fewer amount of resources (Hellsten and Klefsjö (2000). This management philosophy targets continuous process improvement. Six Sigma, on the other hand, is defined as a business process that allows companies to improve their bottom line by designing and monitoring everyday business activities in ways that minimise waste and resources while increasing customer satisfaction (Andersson et al. 2003).

In Lean Thinking, Womack and Jones (1996:16) define lean thinking as "*a way to specify value, line up value-creating actions in the best sequence, conduct these activities without interruption whenever someone requests them, and perform them more and more effectively*." Lean-based process improvement originated with Toyota and Taiichi Ohno and aims to combat waste (Ohno, 1988). It became much more widely known through the book 'The machine that changed the world' (Womack, Roos and Jones, 1990). Activities that require the deployment of staff, time or money and that add no value to the process or the customer must be eliminated. Lean has a strategic perspective that focuses on understanding value, plus an operational element that focuses on combating waste (Hines, Holweg and Rich, 2004).

[10] DigiNotar was a Trusted Third Party that provided digital certificate services and hosted a number of Certificate Authorities. DigiNotar suffered a breach in June/July of 2011. This breach resulted in rogue certificates being issued that were subsequently abused in a large scale attack in August 2011.

While the definitions of TQM, Six Sigma and Lean differ, the overall aim of the concepts seems to be the same: minimising waste while improving customer satisfaction and financial results.

Lean Six Sigma (LSS) is a combination of methods that has been used in the service industry since the beginning of this century. It was also used in the production industry before that. Organisations were starting to recognise that improving quality with Six Sigma or trying to improve process efficiency with Lean wasn't enough—they needed to do both to get maximum payback. The LSS process is broken down into five interconnected stages: Define, Measure, Analyse, Improve and Control—abbreviated to DMAIC (George et al., 2003). We will return to LSS later after discussing the principles of Lean.

6.4.4 *Lean core principles*

Womack et al. (1990) identified five core principles of Lean thinking:

1. Determine value by product offering: specification of the value in terms of a specific product or service, delivered at a specific price at a specific time, which meets the needs defined by the customer.
2. Identify value stream by each product offered: identification of the value stream by identifying the tasks for each product family and eliminating tasks that have no value. Value stream analysis (VSA) investigates which tasks add value so that redundant tasks can be identified. VSA is often visually designed to communicate the processes and organisational targets, and to indicate the relationship between processes and control. All kinds of process modelling methods can be used for this analysis. However, the choice requires considering which level of detail the modelling will use. Business process model notation (BPMN) is increasingly being used for process modelling and execution. In §5.5.4, process modelling using BPMN will be discussed in further detail.
3. Make value flow: once waste has been eliminated, 'flow' can be accomplished. Flow, the opposite of batch production, requires the movement of products from one value creating step to the next with no waiting.
4. Let the customer pull value from the producer: this principle aims at letting the customer pull the product from the organisation's value stream instead of providing products in the marketplace where is possibly no demand for.
5. Pursue perfection: repetition and improvement of the cycle by ensuring transparent processes and combating waste.

When applying the principles of Lean thinking to business reporting chains, it is crucial to understand the consequences of legalisation on process design. In the Netherlands, society pays for the existence of requesting party through taxes. Reporting requirements are imposed via the country's parliamentary democracy. Legal obligations require businesses to engage in reporting processes, while the legal duties of the requesting parties are to request and process the information. These obligations cloud the push/pull distinctions of Lean. If the value for end

users needs to be specified, the question is who the end users are. From the perspective of the SSC, end users include companies, intermediaries and government agencies (requesting parties). While requesting more comprehensive business information more often may increase private sector transparency and enhance the ability of the requesting parties to execute public policy, increased reporting frequencies and amounts will impose more cost on companies. It may also require more public funding, which may require higher tax incomes. So, will reporting processes be set up in such a way that it is easy for the requesting party, but costly for the reporting party? Or the other way around? Politicians need to make the trade-offs.

The Agricultural Economics Research Institute – one of the parties that uses SBR standards – compensates a portion of the intermediaries' costs using public funds, in order to collect and publish information from businesses. In that case, part of the costs for business reporting is paid by society as a whole. Conversely, the burden can also end up with the businesses. In that case, business reporting is only paid for by a portion of society. Of course, a process optimisation that reduces the burden for all chain partners directly would be the best result. Such a chain perspective is fundamental to the SBR approach.

6.4.5 *Waste*

In addition to value creation, the other basic idea behind Lean is avoiding 'waste.' Redundant activities or activities that do not add value must be seen as wasteful. Based on the work of Ohno (1988), Womack and Jones (1996) list eight types of waste: surplus production, waiting, transporting, additional processing, inventories, poor setup, incomplete staffing and defects. Everything that requires additional actions, such as handling problems and defects, is considered wasteful. For the service sector, these eight basic types have been translated into ten types of waste (Bonaccorsi, Carmignani and Zammori, 2011).

1. Defects: typos, input errors, lost files, lost or damaged data. Womack and Jones (1996) see everything that fails to meet the customer's requirements as a defect.
2. Duplication: retyping data, use of multiple signatures, unnecessary reporting and having to answer unnecessary questions.
3. Incorrect or incomplete information: having to search for the appropriate information, storing unnecessary copies of information.
4. Lack of focus on the user (customer): customer-unfriendly, unfamiliar with the customer, impoliteness, failure to listen.
5. Surplus capacity and surplus production: drawing up reports that nobody will read, printing paper copies, delivering paper before it is required, activities to repair defects.
6. Unclear communication: incorrect information, use of non-standard formats, unclear workflow.
7. Information movement and transport: unnecessary shipments, lack of clarity about where the information needs to be sent and what type of information

is needed, having to find out the next task the information will be used for, etc.
8. Understaffing: having to wait, too much bureaucracy, limited mandate to do business.
9. Variation: not enough procedures and processes to handle exceptions, lack of standard formats, failure to define standards and expectations.
10. Waiting and delays: waiting for permission, server downtime and waiting for information.

A large amount of waste is an indication that a process is not properly controlled. Within Lean, even a helpdesk is seen as waste, since the helpdesk handles matters that are not dealt with properly within the process. Helpdesks that are very busy indicate that a process is not well organised. The list provided above can be used as a checklist for process reengineering. SBR implicitly supports many of these principles. The following are examples of each type of waste, as seen in the SBR domain:

1. Defects. SBR makes it easier and more efficient for software providers to perform checks at the front end of the process (upstream of the information chain), thus reducing the chance for errors. SBR promotes 'compliance by design,' by making it technically impossible to get defects from incorrect inputs or actions.
2. Duplication. Various validations continue to be carried out redundantly within SBR processes. If acting properly, the software provider will validate against the XBRL taxonomy. The generic infrastructure then performs this validation again and finally, the same check is included in the requesting parties' validation. It is expected that continuous process optimisation—and maturing SBR chains—will reduce such types of redundancy.
3. Incorrect or incomplete information. Logius is the SSC for government agencies within the business reporting domain. As the second example above shows, requesting parties initially set up a number of duplicate tasks (such as storing copies of messages), given their dependency on the SSC. To minimise the number of copies, the processes and technology working group incrementally developed a chain vision in 2011 that was about securing, re-injecting, re-delivering and re-submitting messages via the generic infrastructure. While storing copies remains unavoidable under the Archives Act and governmental policy, this vision means that storing copies will gradually be minimised across the chain and be done at a single location.
4. Lack of a single homogenous user community. Backed by the expertise of the Tax and Customs Administration, the SBR Programme – with its many public/private bodies – has invested a great deal of time and resources in understanding the users of the SBR services
5. Surplus capacity and surplus production. When the e-Notification process was set up, it took into account the fact that not all businesses would hire a service provider that was approved to receive tax assessment no-

tices from the Tax and Customs Administration. Before the Tax and Customs Administration generates the electronic copy, it checks a subscriptions registry to see whether parties are interested in receiving the tax assessment notices. A tax assessment notice will not be created if the party is not interested.

6. Unclear communication. One of the key thrusts of SBR is improvement of communication by standardisation at various levels, including the process level. The mandatory use of BPMN for at least the generic components is an example of this.
7. Meta-information movement. Looking at the I-processes, there is still pressure on Logius to include a relatively large variety of meta-information (at the data transport level) in its final delivery to the requesting party. The current argument for this is that the meta-information 'might come in handy' for analyses or in the event of an incident. Such a need is not illogical given the maturity of the SBR solution so far (see also points 2 and 3). It is also expected that architects in the public chain will gradually formulate stringent criteria about what (meta)information must be transferred and what information should be seen as excess baggage.
8. Understaffing. The SBR programme experienced significant bureaucracy, for instance while using AuSPs in specific chains. As explained in Chapter 1, AuSPs are not being used anymore.
9. Variation. In 2010/2011 the problem of the lack of procedures for handling incidents and exceptions was countered by enabling the project managers of Logius and the requesting parties to consult each other immediately. They kept each other informed on incidents and maintained good relationships with the line organisation of the SSC. Such solutions only work for small message volumes. From 2011 onwards, considerable efforts have been made in order to reach clear agreements about how the chain partners can handle incidents in a structured manner. These efforts were made in light of the impending increase in volumes expected in the coming years.
10. Waiting and delays. In the previous sections of this chapter, we discussed the problem of bottlenecks, and the use of decoupling and buffers to prevent downtime and unnecessary waiting. Naturally, SBR chain partners pay significant attention to these issues.

6.4.6 *Timeliness*

As a concept, Lean covers all types of items, such as Total Productive Maintenance (TPM), cellular manufacturing, Single-Minute Exchange of Die (SMED), Mixed Model Production (MMP), Just In Time (JIT) and Straight-Through Processing (STP). We will only discuss the last two types, as these are relevant for I-processes. Just In Time (JIT) is the principle in which supply and demand are matched together. Products are only available when they are really needed. The advantage of JIT is that stocks or buffers do not need to be held. For information chains, this means that information will not have to be stored locally, but will be available as soon as it is needed. This saves duplication or unnecessary transfer

of data back and forth. The downside of the JIT philosophy is that any disruption or interruption will cause the entire process to be halted.

The reporting domain is currently considering the use of JIT. If used, requesting parties will only request additional data from businesses if they need it for checks. This is an interesting thought, but does not fit in with the existing convictions of SBR and the mould from which administrative and business reporting laws were cast. On one hand, many issues will need to be solved before the JIT approach can be applied to system-to-system processing of business reports. On the other hand, the building blocks within SBR and emerging technologies, and their use in other domains, will ensure that this option becomes more and more realistic. The JIT principle fits with the new wave of redesigns in reporting chains.

Straight-through processing (STP) is an approach in which transactions are handled immediately, i.e. handling cases without human involvement. One example would be a request for a loan offer in the financial industry: all activities are carried out immediately and an answer is given within a few seconds or minutes. Another example is the situation at a helpdesk, where a problem is solved rather than merely analysed. These examples show that it is important for STP implementations to ensure automated processing of as many activities as possible. STP uses few or no buffers, and handles all tasks immediately. Processing in batches must also be avoided. Taking this principle to an extreme may actually create a situation in which the efficiency benefits of batch processing are no longer seen. It has already been noted that the processes in SBR were originally set up without buffers (i.e. in accordance with STP), but that this caused too much lost time. STP is often implemented for properly standardised processes, after which the principle is gradually extended into processes that are more complex.

STP can be realised more easily for automated I-processes if the number of business reports are spread out more gradually over time. Think of the performance of the validation service with this in mind. The chain characteristics and legal requirements determine the extent to which the delivery of business reports can be spread. VAT tax declarations are made at a relatively high frequency (most companies must declare once per quarter) and use a relatively large number of different software packages. In addition, many parties submit their own declarations and there is a strict deadline, namely the last day of the month following the period in question. The result is a large peak in declarations at the end of the month. Tax consultants can request postponements of income tax and corporate income tax for their customers. The majority of declarations for corporate income tax are drawn up by intermediaries, in which case the normal deadline of 1 April will be extended to 1 May of the following year. However, intermediaries must follow the schedule shown in Table 6.2 allowing a more continuous and evenly distributed delivery of declarations.

Table 6.2 – Arrangements for postponement of tax declarations by intermediaries (Source: Tax and Customs Administration leaflet)

Up to	Total percentage
May/June/July/August	30%
September	38.75%
October	47.50%
November	56.25%
December	65%
January	73.75%
February	82.50%
March	91.25%
April	100%

During the period of postponement, declarations must be submitted in accordance with the delivery schedule that was received. This schedule states the minimum proportion of declarations that must be delivered by the end of each period. The actual numbers are based on the percentages in the table below.

6.4.7 *Reduction in complexity*

Another important Lean strategy is complexity reduction. This strategy is needed because changes will be made over time by various people, resulting in processes that are increasingly complex. High complexity can easily lead to errors and is more difficult to control, as no parties are able to know exactly what the entire process looks like.

Lower technical and administrative complexity, on the other hand, is easier to understand and therefore less prone to errors. As a result, organisations can become more flexible, since the process can be changed more easily. Looking primarily at the information chain, we see that complexity is generated by the following:

- Number of tasks
- Number of data transfer points
- Iterations between tasks and feedback

The number of transfer points is usually the same as the number of tasks plus one. A simple probability formula can be used to show what the effect of the number of tasks, the number of transfer points and feedback loops.
Assuming the following:

T is the number of tasks
D is the number of data transfers
X is the chance that a task will produce its correct results in full
Y is the chance that data transfer will be entirely successful.
The reliability of the process (P, the chance that the process will operate properly) is then:
$P = X^T Y^D$

This is a simplified calculation based on a number of assumptions. In practice, there will be more dependencies between tasks and there may be feedback loops in order to correct for errors.

Table 6.3 – Consequences of errors in a process

	T (number of tasks)	D (number of data transfers)	X (the chance that a task will produce its correct results in full)	Y (the chance that data transfer will be entirely successful)	$P = X^T Y^D$ (reliability)
Situation 1	5	6	0.95	0.99	0.73
	5	6	0.95	0.95	0.57
	5	6	0.95	0.9	0.41
Situation 2	10	11	0.95	0.99	0.54
	10	11	0.95	0.95	0.34
	10	11	0.95	0.9	0.19

The table shows that if the data transfer points are more reliable, the entire process will be more reliable in any situation. The same applies to tasks. The difference between the two situations shows that if the numbers of tasks and data exchange points increase, the reliability will be reduced considerably. This intuitively shows that it is important to have as few tasks and data exchange moments as possible in order to reduce the process complexity as much as possible.

6.4.8 *Reducing variation*

Safeguarding the proper functioning of tasks is the basis for the perfect process (running as smoothly as possible). Six Sigma aims to reduce variation in process handling through measurements and statistical analyses. A Six Sigma process is one that is 99.99966% correct, meaning that there are less than 3.4 errors in a million. Such a figure is rather improbable for processes involving humans but is realistic for computers performing automated processes—although it should not be forgotten that things can go wrong there too. For example, consider servers that hang or get stuck in a loop or need to be reset. Mechanisms have therefore been built into the transfer of data between computers to check that data is transferred correctly and to retransmit the data if errors are detected.
An important concept is setting ambitious goals prior to the analysis. Even without knowing the details of the actual process, expectations can be set for its performance (see §6.3). Six Sigma projects follow Deming's plan-do-check-act (PDCA) cycle (Womack and Jones, 1996). There are two methods: DMAIC for projects that improve the current processes and DMADV for new products and processes. DMAIC consists of the following five stages (Feo and Bar-El, 2002):

1. Defining the problem.
2. Measuring key aspects and collecting data.

3. Analysing the data and verifying the relationships between cause and effect. What are the causes of the errors in the process? What factors affect them? Finally, all essential causes should be identified.
4. Improving the current process using techniques such as experiments, *poka yoke* (this is a combination of avoid - *yokeru* - and errors - *poka*, by making sure tasks cannot be performed incorrectly), standardisation, etc.
5. Performing checks by measuring and correcting any discrepancies and making sure they will not recur.

In DMADV, the latter two activities are replaced by the following two:

4. Design that meets the customer's expectations.
5. Verification of the design's performance and the extent to which it meets the customer's needs.

All kinds of methods, techniques and tools can be used to implement Six Sigma strategies, as is shown in Table 6.4 below. While a discussion of all of these techniques is beyond the scope of this book, it is nevertheless important to mention that they exist, as they can be useful in analysing and improving processes.

Table 6.4 – Summary of Six Sigma strategies, principles, tools and techniques (Feo and Bar-El, 2002)

Six Sigma business strategies & principles	Six Sigma tools and techniques
• Project management • Statistical process control • Knowledge discovery • Process control planning • Data collection tools and techniques • Variability reduction • Belt system (Master, Black, Green, Yellow) • DMAIC process • Change management tools	• Data-based decision making • Process capability analysis • Measurement system analysis • Design of experiments • Robust design • Quality function deployment • Failure mode and effects analysis • Regression analysis • Analysis of means and variances • Hypothesis testing • Root cause analysis • Process mapping

6.5 How can a good process be maintained?

After a process is developed, it should be maintained and improved continuously. Measurement of performance indicators or spontaneous improvement actions due to incidents may trigger maintenance activities such as updates and repairs. Maintaining processes in information chains often require substantial harmonisation between the chain partners. First, all sorts of changes to processes need to be properly communicated. It can sometimes be difficult to estimate the effects of a change on other chain partners. Therefore, it is sensible, even for anticipated

changes in message delivery volumes, to pass on the details of the change to make sure that other chain parties can prepare for it.

6.5.1 *Process development approaches*

A number of process change approaches have been developed over time. Business Process Re-engineering (BPR), for example, emerged at the start of the '90s. Its objective is radical improvement of processes (Hammer and Champy, 1993), whereas Total Quality Management (TQM), which emerged later on, embraces 'thinking in processes.'

The basic idea of BPR is to avoid look at existing processes, as this might focus too much attention on the current situation and ignore possible better solutions. BPR takes the stated goal of the process as its starting point and redesigns new processes from scratch (on a 'blank sheet of paper'). The basic idea is that substantial benefits can only be obtained through radical change (Kim, Pan and Pan, 2007; O'Donnell and Timonen, 2003; Swedberg and Douglas, 2003). Teng et al. (1994) define BPR as "*the critical analysis and radical redesign of existing business processes to achieve breakthrough improvements in performance measures*" (p. 9). BPR is typified by fundamental and radical changes that should lead to improvements, with a focus on process-oriented thinking.

Ensuing the publication of the fundamental concepts of BPR by Hammer (1990), many organisations have reported benefits gained from the successful implementation of BPR. Nevertheless, despite the significant growth of the BPR concept, not all organisations embarking on BPR projects achieve their intended result (Al-Mashari and Zairi, 1999). Hammer and Champy (1993) estimate that as many as 70% do not harvest the benefits they seek. This blend of results makes the issue of BPR implementation very important. BPR has potential for increasing productivity through reduced process time and cost, improved quality, and greater customer satisfaction, but it often requires a fundamental organisational change. Therefore, factor such as change management, competency, backing and organisational structure become a significant part of the equation. As a result, the BPR implementation practice is complex, and needs to be checked against several success/failure factors to ensure successful implementation, as well as to avoid implementation pitfalls (Earl, 1994).

BPR is now less associated with radical and revolutionary thinking than with process-oriented thinking. To avoid the negative associations, other terms such as 'business engineering' and 'process innovation' are used to indicate process-based thinking. The success of BPR depends critically on the use of BPR techniques and resources (Kettinger, Teng and Guha, 1997; O'Neill and Sohal, 1999; Wastell, White and Kawalek, 1994). Kettinger et al. (1997) provide a summary of 72 techniques that are often used in BPR. These techniques are related to tools such as Quality Function Deployment (QFD), process modelling, brainstorming, simulation, specification of rules, designing databases and process measurements. A number of these techniques are typically covered by the concept of

LEAN. As stated earlier, BPR has a high chance of failure. It can therefore be contrasted against Total Quality Management (TQM), which focuses on the incremental improvement of business processes (Carr and Johansson, 1995; Davenport, 1993; O'Neill and Sohal, 1999). Lean Six Sigma (LSS), which combines elements of LEAN and Six Sigma, originates from the TQM approach.

As with BPR, criticisms of TQM and LSS have also been put forward (Hines et al. (2004). These approaches take little to no account of the various types of organisations, and do not deal with the differences between processes and organisations. In addition, no relationship is created between the strategic level and the setup of processes. Another point of criticism is the lack of attention to the human aspects and an excessive focus on operational processes. The latter aspect ignores the strategic level. Both approaches are complementary and will follow each other over time (O'Neill and Sohal, 1999).

In major process changes, the fundamental assumptions that a system is based upon may no longer hold water, with technological options that are so different that process improvement alone is no longer viable. A radical review of the fundamental design is required in such a case: one can't make a silk purse from a sow's ear. Thus, it is better to create an entirely new blueprint in such a case. Another situation is SBR's current stage, in which no more major changes will be taking place. In recent years, much attention has been paid to continuous refinement of the I-processes to create a better match between the requirements and wish-lists of the submitting and requesting parties. Such refinement is now being done incrementally and gradually. The diagram in Figure 6.6 shows the difference in scale between major (BPR) and incremental (TQM) changes.

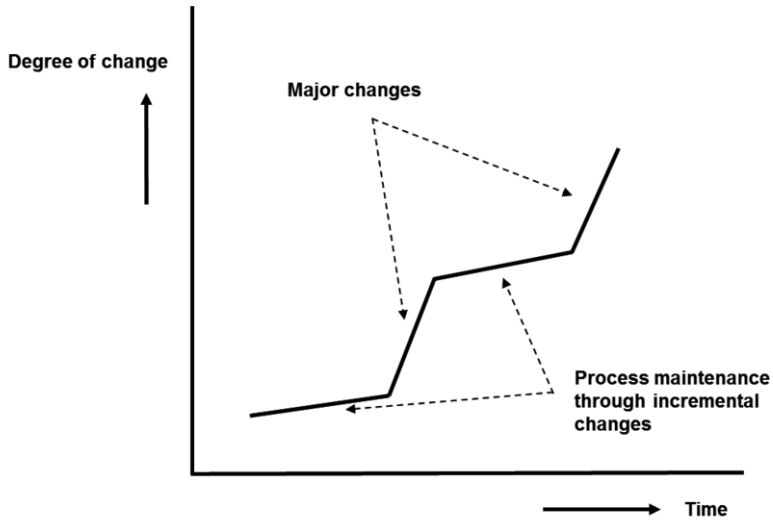


Figure 6.6 – The complementarity of BPR and TQM (based on Dervitsiotis, 1998)

Table 6.5 positions the previous and coming stages of SBR (and its predecessor, NTP) alongside BPR and TQM/LSS. The expectation is that SBR will operate increasingly in line with the TQM/LSS change approach over the next few years.

Table 6.5 – Characteristics of the process change approaches

Characteristics	**BPR**	**TQM/LSS**	**NTP/SBR 2006 to 2012**	**SBR in 2013 and after**
Change method	Radical	Incremental	Radical	Incremental
Focus	'blank sheet of paper'	Current practice	'blank sheet of paper'	New practice
Frequency	One-off	Continuous	A few iterations	Continuous
Scope	Wide, review of functions	Limited focus on certain functions	Wide	Increasing focus on certain functions
Participation	Top-down	Bottom-up	Middle-out (combination of top-down and bottom-up)	Middle-out
Risks	High	Limited	High	Reduced
Significance of IT	Key	Limited	Key	Unchanged
Tools	Methods and techniques	Employees, empowerment with tools	Employees, methods and techniques	Employees, methods and techniques and empowerment with tools
Type of change	Structure, culture	Processes	Structure, culture	Processes

6.5.2 *Maintaining the chain setup and execution*

Maintaining and controlling the processes in a chain requires harmonisation between the parties and clear agreements about their expectations. These expectations can be long-term (what to do in the event of a change) or short-term ("Houston, we have a problem"). Chains are not controlled in isolation, but often in consultation with departments or organisations that together make up the chains. This means that the planning must be done in such a context.

Figure 6.8 provides a summary of control in chains. The chain structure is a long-term structure consisting of the realisation of strategies and agreements made to ensure operation of the chain. The chain structure is relatively permanent. Changes require negotiation between the partners and implementation via a suitable form of control. Aggregate control is a periodic planning procedure to ensure sufficient available capacity for the implementation of small process improvements. Peaks might be expected during certain periods that have a relatively high number of messages sent. Implementing improvements within the chain structure is part of aggregate control, too. It can be done by removing a technical component and replacing it with an improved component, without

changing the interface. Decisions about closing or opening a portal for certain messages are made here as well.

Operational control involves actual execution and, if required, intervention. It includes monitoring the execution of the chain and intervening in the chain structure (as per the agreements made) if the chain is not functioning well, for example because of a failure in a system, a security problem or because of delays. If necessary, checks will be included in the processes to see whether the goal is achieved, to guarantee the correct, reliable, timely and continuous operation of processes, and to adjust them if required. These checks run contrary to the principle of the Lean management philosophy, which considers them to be waste and states that processes should be self-controlling. However, checks are required in chains, as problems could otherwise go unnoticed.

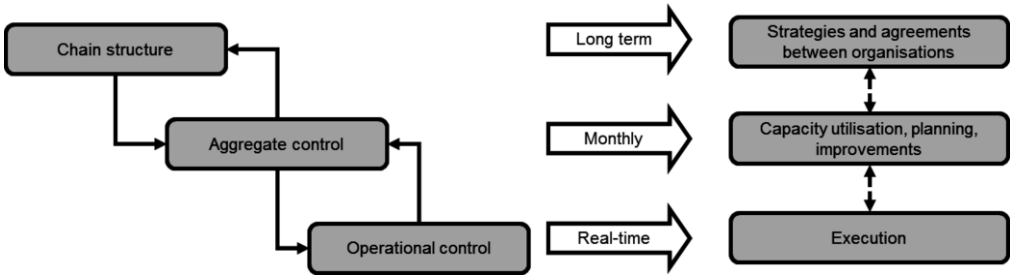


Figure 6.7 – Overview of chain control at three levels: chain structure, aggregate control and operational control

The arrows between the three levels indicate how they affect each other. A disaster at the operational control level can reach the chain level and cause changes there.

6.5.3 *Controlling and measuring the performance of processes*

Determining the appropriate process performance indicators is important for translating the organisation's strategy into measurable quantities, continuously evaluating the process performance and making adjustments to it, and initiating radical change processes. Chain partners can use performance indicators to demonstrate that the chain is under control.

Figure 6.8 illustrates the principle of a controlling process, which quantifies the operational process and can intervene via comparison against predefined standards. The figure presents two types of interventions, namely a controlling intervention and a regulating intervention. The controlling intervention (feed forward) looks ahead in the process. This is the same as what an automobile driver does while driving: looking for signals and operating accordingly. The regulating intervention, on the other hand, looks backwards in the process and is represented by dotted lines in the figure. To ensure that a regulating intervention does not take place too late (for example, after complaints have already been made), its standards need to be set higher.

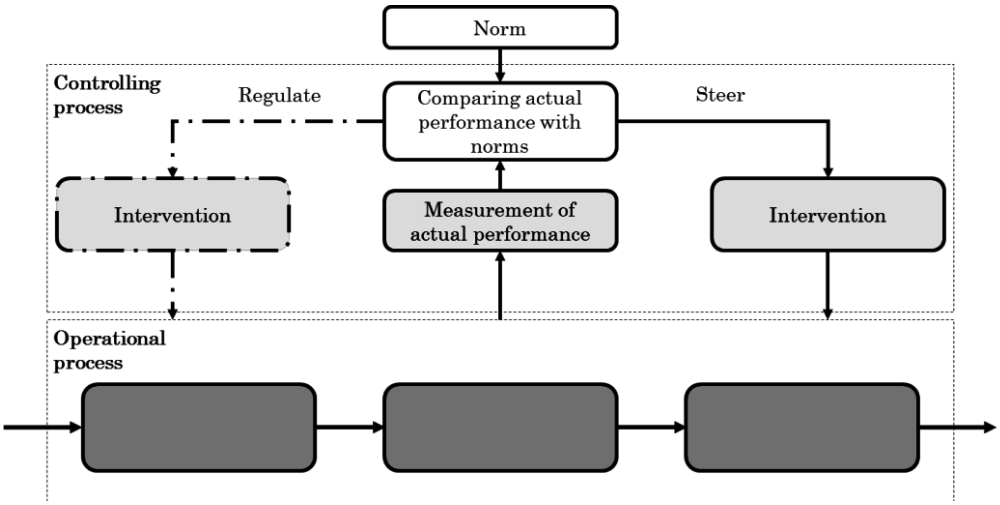


Figure 6.8 – Controlling processes that intervene and that regulate

Processes are usually controlled by means of software. From a technical perspective, such control is often supported by Web Service Orchestration software (another kind of BPM software), which continuously monitors the execution of processes, providing an overview and process status. Additionally, it is possible to set alerts that can be triggered if a process takes too long or if services become unavailable. Interventions can be automated or an alert can be sent to managers that are responsible for taking actions.

6.5.4 *BPMN as a process modelling technique for design and maintenance*

One of the requirements imposed on the SBR solution results from the need for unambiguous process descriptions (specifications), i.e. the I-processes must be defined using a process standard. The Business Process Modelling Notation (BPMN) is an open visual standard for modelling processes. It provides unambiguous symbols and constructs for mapping out processes (White and Miers, 2008), resulting in simple, communicative models (Vergidis et al., 2008). The Netherlands governmental reference architecture (NORA) sees BPMN as the standard for analysing business processes. BPMN offers public chain partners a uniform language for making processes understandable. Although there are various standards for process modelling, SBR prescribes BPMN where processes are involved. The Object Management Group (OMG) is responsible for the maintenance of BPMN. BPMN is supported by various software providers. Initially, BPMN was based on the activity diagrams of Unified Modelling Language (UML). BPMN's strength is that activities and services can be modelled, making it easy to translate BPMN into processes that can be automated. BPMN 2.0 has shifted BPMN from a primarily visual language for modelling processes to a language that can also be executed immediately (Chinosi and Trombetta, 2012). Ideally, it should be possible to model a process and implement it immediately.

BPMN uses 'swim lane' diagrams for the actors who perform tasks, as shown in Figure 6.10. The starts and ends of events are shown as circles, and rectangles with rounded corners represent tasks or subprocesses (activities). Diamonds are used to indicate the decisions (gateways). In addition, arrows are used to connect events, activities and decisions with one other. Finally, a number of objects (artefacts) are used to indicate what data is being used or which elements belong together, or to provide explanatory information. In summary, the four basic elements of BPMN are the following:

1. Flow objects (events, activities and gateways)
2. Connecting objects (sequence flow, message flow or association)
3. Swim lanes (pool and lanes)
4. Artefacts (data objects, groups and notes)

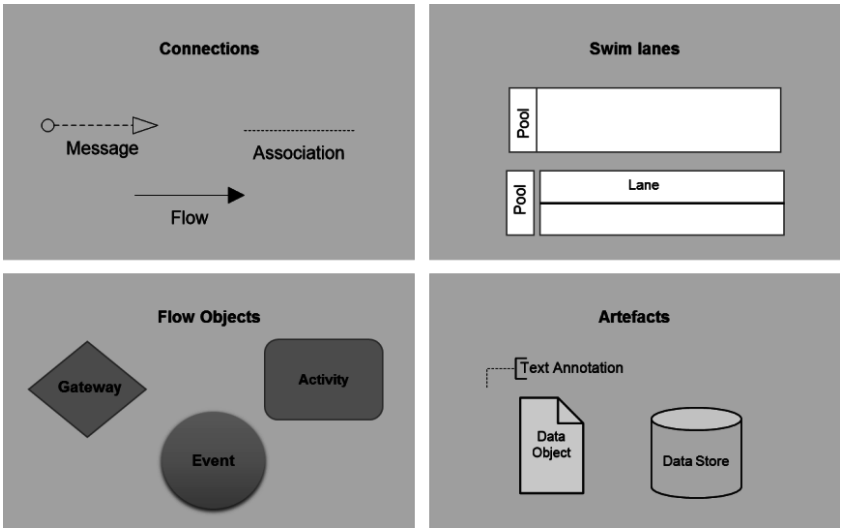


Figure 6.9 – Overview of the basic BPMN elements

BPMN is particularly suitable for mapping chain processes, since chain partners' processes can be modelled using in swimlanes, allowing the processes to be linked to responsibilities. The interactions between organisations can be handled by services (mostly web services), with the modeller choosing the aggregation level at which a service is specified. This enables a connection between the chain level processes, organisation level processes, subprocesses and tasks.

Figure 6.10 shows an SBR chain process: the lower pool is for the party submitting information, the middle pool is the process handled by the SSC, and the upper pool describes acceptance by the requesting party.

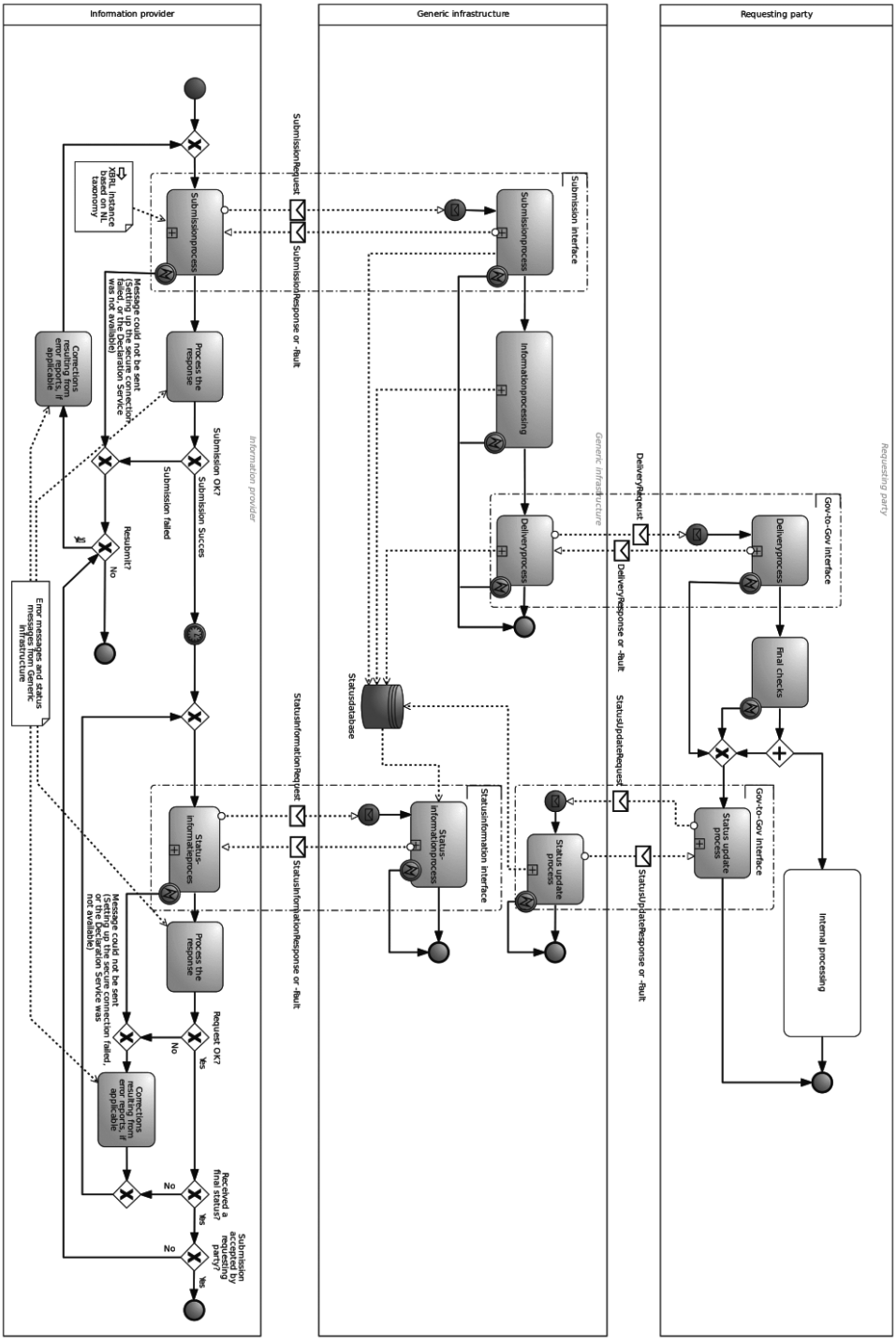


Figure 6.10 – Example of a BPMN diagram for an SBR chain

Figure 6.10 shows the various business processes that can be distinguished in a typical SBR chain. The challenge is to determine what level of abstraction and detail are needed to look at the processes and how to present this information in a model. Many modellers go no further than the most typical scenarios (the 'happy flow'), failing to go into enough detail to ensure the processes can be carried out. Staying at the higher abstraction levels can be useful when creating an overview, in order to ensure easy communication and even the use of LEAN principles. However, the person who implements the process must be aware of all details, including what the alternatives are and how the process is carried out. There is the risk for all components that are not modelled to be set up at the discretion of the programmer. When modelling, decisions need to be made based on explicit considerations, and design choices must be made visible. In SBR, the components handled by the SSC are mostly described in detail. Figure 6.15 narrows in on the information submission service and the detailed tasks involved.

6.5.5 *BPMN legibility principles*

BPMN is a visual standard, which is why it is important to make sure that models created in BPMN are also easy to read. This consideration is all the more important because different analysts looking at the same process may propose various process setups. This means that the same process can be modelled and set up in various ways, too. Principles and guidelines may assist modellers and analysts in making sure that the models show increased uniformity and standardisation. SBR has ensured the legibility of the models by implementing the following guidelines:

- Use decomposition into subprocesses if tasks are coherent (see Figure 6.1) and make sure that each process has no more than 20 tasks. If more are needed, define a new process that can cover these tasks.
- Minimise overlap between lines. This keeps processes legible, for instance when modelling feedback loops)
- BPMN models must still be legible when printed or projected so that they can be discussed with chain partners.
- Model the sequence of tasks over time from left to right as much as possible (i.e. start a task on the left and end on the right).
- If there are multiple start and end-points, use different names for them to avoid confusion.
- Always use an active verb to indicate a task and start the name with that verb.
- Always use the same type of gateway to split up a process and to join it again.
- When using an XOR gateway (one that splits into alternative flows), state which is the default and which is the conditional flow. Give these flows different names.
- Visualise the collaboration between the actors in the various pools using ingoing and outgoing messages.
- Use hierarchical decomposition (see Figure 6.1), which makes a distinction between the chain level and the organisational level.

- If the outcome of a task is a specific product or service, model this by using a data object that is linked by a connecting object. The input of an activity can be visualised in the same way. For instance, legislation can be visualised using a data object.
- A decision that requires human intervention must be modelled by a task (decision activity) followed by a diamond (gateway) to permit alternative paths.
- Do not use separate tasks for receiving and sending. Event objects can be used for this.
- Processes must always finish with an end event to prevent deadlocks.

These guidelines can be used to increase the legibility and communicability of process models. Legibility must be enforced by management measures that ensure compliance of the various process models with quality requirements, and that they are coherent and consistent.

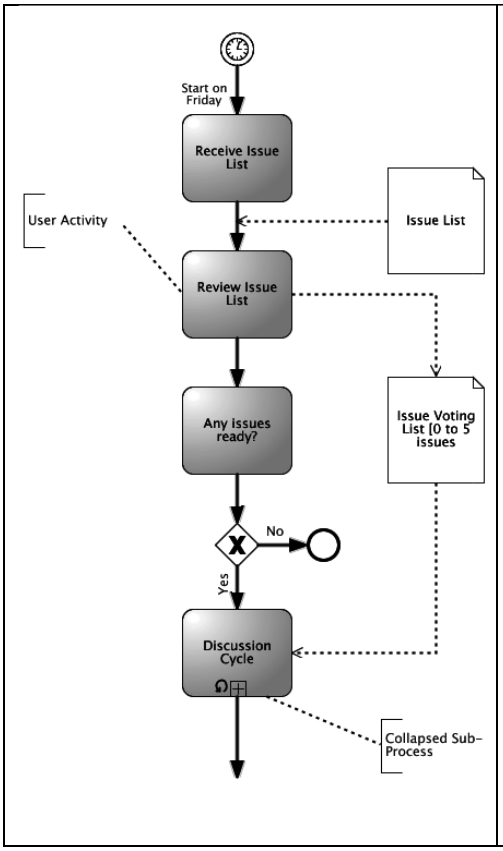
6.5.6 *From process to execution*

After a process has been modelled in the visual BPMN language, the following step is to actually perform the process. BPMN 2.0 makes it possible to carry out a process immediately, although process descriptions and their executions are often separated. The process model can be exported to an executable code for direct automated handling. XML Process Definition Language (XPDL) has been developed specifically for this. It is a standardised XML-based language that is used for exchanging process descriptions between BPM products and is maintained by the Workflow Management Coalition (WfMC).[11] XPDL stores the graphical information and information about the execution. Web service orchestration is used for the execution of the process. Web service orchestration is part of the web services stack. Process execution takes place by invoking (or calling) web services. Web service orchestration therefore focuses on specifying the logic behind the sequential invocations of various web services. It describes a process from the perspective of a certain organising logic. The *de facto* standard for orchestration is BPEL4WS, the Business Process Execution Language for Web Services, often called BPEL for short. BPEL was developed by Microsoft, IBM and BEA and combines two older languages of Microsoft and IBM: XLANG and WSFL.

The latest version of BPEL4WS contains process logic that was traditionally only found in workflow languages. For example, it provides the possibility of having tasks performed by people. Compared with workflow management, the major advantages of orchestration are the standardised deployment of processes and the invocation of applications using web services. These advantages enable the reuse of web services, as well as quick and easy implementation of new processes. When BPMN 2.0 emerged, it was often stated that BPEL was out-dated, but

[11] See: http://www.wfmc.org/

many people still see BPEL as the most effective way to execute processes (Chinosi and Trombetta, 2012). The relationship between BPMN and BPEL ensures that a process can be mapped out, as shown in Figure 6.11.




```
<process name="EMailVotingProcess">
<!-- The Process data is defined first-->
 <sequence>
 <receive partnerLink="Internal“portType="tns:processPort“ operation="receiveIssueList“ variable="processData“ createInstance="Yes"/>
 <invoke name="ReviewIssueList" partnerLink="Internal“ portType="tns:internalPort" operation="sendIssueList“ inputVariable="processData“ outputVariable="processData"/>
 <switch name="Anyissuesready">
 <!-- name="Yes" -->
 <case condition="bpws:getVariableProperty(ProcessData,NumIssues)>0">
 <invoke name=“DiscussionCycle“ partnerLink="Internal“ portType="tns:processPort" operation=“callDiscussionCycle“ inputVariable="processData"/>
 <!– Other Activities not shown -->
 <!--name="No" -->
 </case>
 <otherwise>
 <empty/>
 </otherwise>
 </switch>
 </sequence>
</process>
```

Figure 6.11 –BPMN mapped to BPEL4WS

It is often not possible to deploy BPMN based process descriptions immediately, since lower level choices still need to be made. To provide a functioning linkage between BPMN and BPEL, metadata still needs to be added to the different symbols. Nevertheless, using BPMN reduces the gap between the business and technology professionals considerably, one reason being that it leaves less opportunity for ambiguity. Various process modelling tools (software) can be used for this. Next, we discuss some requirements on such tools.

6.6 What tools and methods can be used for design and maintenance?

6.6.1 *Software for support*

Various software providers offer tools for modelling in BPMN. Support can range from basic functionality, which only allows users to graphically draw and visualise processes, to complex suites, which can help users improve and execute processes immediately[12]. Functional requirements imposed on the BPMN modelling software may include the following:

- Graphical BPMN editor for simple drawing and changing of processes
- The capability to define I-process specifications that can be reused in multiple information chains
- Allocating roles to each user for maintenance and development
- Translation from process into data structure
- Graphical UML editor to edit the data structure
- Process simulation, including data import and statistics support
- Process diagnosis (queues, bottleneck identification and so forth, as well as detection of similarities between processes)
- Export options (to XPDL) or immediate execution of processes (in BPEL). The latter option assumes the availability of advanced functionalities such as connections to web services and a graphical BPEL editor
- Integration with actual workflow execution and the Business Activity Monitor

In addition to the above these functional requirements, a large number of non-technical requirements or quality requirements can also be imposed on the software:

- Licensed (to each person/organisation) or open source
- Reliability of the provider
- Maturity/stability of the software
- Regular updates and forward compatibility (related to new updates of standards such as BPMN and BPEL)
- The possibility for training and courses
- Familiarity and user groups (availability of knowledge)
- The number of people who can work on one model at the same time
- Scalability and size of the models
- Local installation or use of SaaS (Software as a Service) solutions.

Several specialised software providers, as well as providers of workflow and application integration software offer software tools that satisfy the requirements stated above. A wide range of software tools is therefore available in the market.

[12] http://www.bpmn.org provides an overview of BPMN modeling software.

For process modelling in SBR, a SaaS solution was selected that enables authorised chain partners to remotely access process descriptions during multiple phases of an SBR chain reengineering programme (see Chapter 10).

6.6.2 *Weaknesses of BPMN*

BPMN has a number of weaknesses, perhaps as an inevitable result of its simplicity. The disadvantages experienced within SBR implementations include:

- BPMN is a visual standard. While the symbols and semantics of the notation is fixed, the output format of a BPMN model depends on the software provider. Therefore, it is not always easy to import/export BPMN models between modelling tools.
- Assessing and reviewing large, complex and multi-layered models can be a daunting task. The management of models and consistency between models remains a challenge.
- BPMN has no standard for the formulation of complex business rules.
- BPMN leaves room to define the same problem in different ways. In order to harmonise process models, we need a Netherlands Process Architecture that functions similarly to the Netherlands Taxonomy Architecture.
- In practice, the immediate conversion from BPMN into executable code is still proving difficult and demands much technical knowledge of the generic infrastructure (see Chapter 7).

6.7 What specific requirements are imposed on I-processes in SBR chains?

An I-process (information processing process) consists of a collection of tasks that, together, process information. In SBR chains, I-processes handle the automated exchange and processing of business reports. Multiple processes are performed by the generic infrastructure. We shall explore the SBR's I-processes component in this section. SBR's I-processes are made up of separate services—interface services and processing services—which will be discussed in detail in Chapter 7.

Some important requirements of the SBR solution are that the I-processes must be in line with the legal framework, they must remain compliant when the I-processes (or the frameworks) are changed, and the various procedures (and standard frameworks) must be maintainable.

6.7.1 *Compliance: conforming to predefined standards*

Based on legalisation, most requesting party in business-to-government information chains are responsible for setting up the reporting processes. The requirements regarding the set-up of such I-processes come from multiple sources. The primary source is legislation. Requirements also come from government policy, the requesting party's general policy, the setup preferences adopted by the requesting party, and the wishes and requirements of chain partners. Due to the

various sources, such requirements may conflict. Such conflict can also be the case with legal requirements. It is therefore rare for an I-process to meet all requirements in full. Setting up an integral programme of requirements for an I-process will provide insight into such considerations beforehand. When that is done, the executive level can provide architects with clear principles that they can use in the design. Figure 6.12 illustrates the relationships between norms and the operational I-processes.

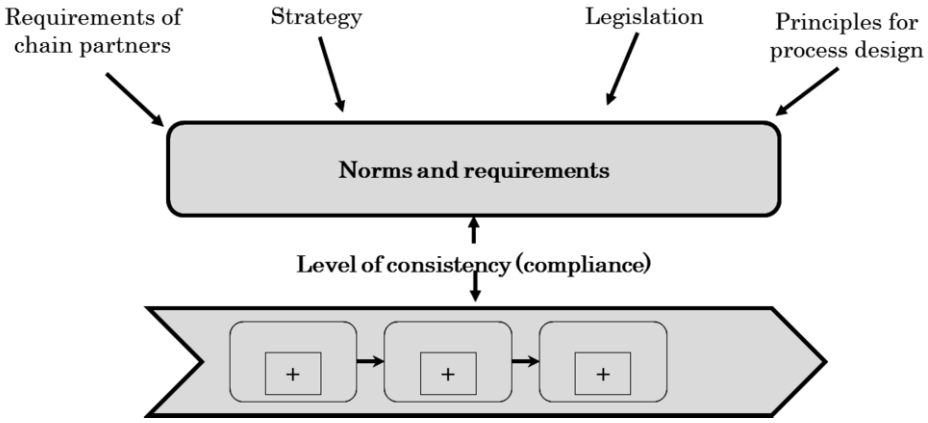


Figure 6.12 – Determining the extent of compliance: confrontation between norms and operational I-processes

6.7.2 *Translation of norms*

Compliance is about the extent to which I-processes match the predefined norms. Within SBR, there is a working group that checks the I-processes against the legal norms for the business reporting processes. The group also checks the I-processes against the applicable requirements based on semantic, syntactic and technical SBR standards. Logius carries out the I-processes using the generic infrastructure, a government owned system for S2S information exchange and processing. Requesting parties in the government commission Logius to manage the generic infrastructure and use it to carry out part of the legal tasks of the requesting parties during information exchange and processing. Logius has no executive mandate and the generic infrastructure is therefore seen as an extension of the governmental requesting parties. As a result, requirements imposed on the request process by a requesting party apply directly to the I-processes carried out by the generic infrastructure. It is therefore the requesting party that must comply with the SBR framework of agreements (the standards).

However, it is incorrect to consider either Logius or the generic infrastructure as a mere middleman. It is important to note that Logius has been responsible for the following tasks in the reporting chain from the start:

- Confirming information had been sent successfully
- Verifying the authenticity of messages received and verifying the identity, authenticity and authorisation of the reporting party

- Securing[13] and archiving the messages sent in
- Checking instances for consistency with reporting rules, which leave little to no room for interpretation
- Delivering messages

Other tasks have been added since 2011. For instance, the SSC temporarily manages the registry with claimed approvals (permissions) for obtaining tax assessment service messages (more on this in Chapter 8). In addition, Logius provides a standard e-Notification process that can provide default notifications from requesting parties such as SBAs. Looking at Logius's position in the request processes, it can be said that Logius does the following:

- Handles the largely generic tasks for the various reporting chains
- Performs the checks for criteria that can be communicated objectively and unambiguously. Logius performs checks that allow objective justification of decisions based on the Online Administrative Business Act
- Plays an additional role in providing formal feedback to the reporting parties

Figure 6.13 illustrates the position of the generic infrastructure in relation to the requesting parties.

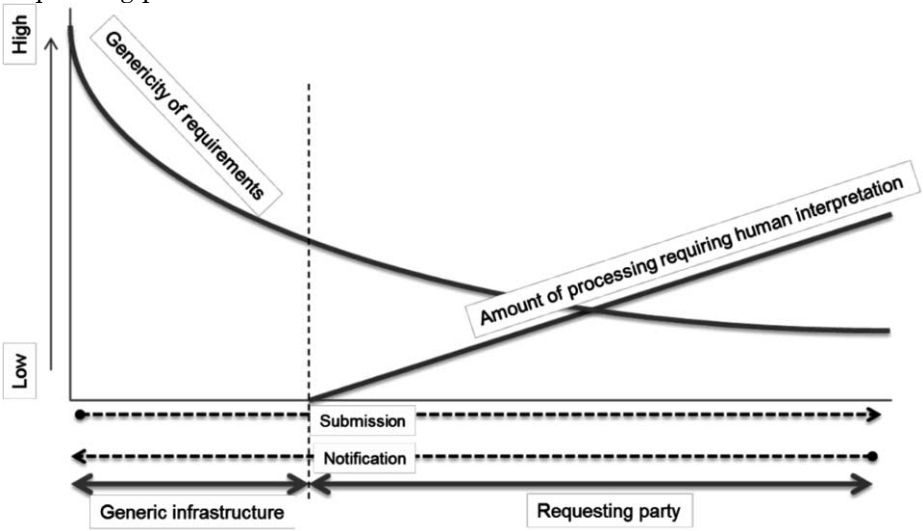


Figure 6.13 –Positioning of the generic infrastructure

Next, we discuss a number of relevant standards for the I-processes, and we will look at process designs that have resulted from these standards. The following sections are largely based on material that has been provided by the compliance working group and the processes/technology working group of SBR.

[13]Storing messages temporarily for any restore procedures.

Responsibility for the message: confirmation of receipt by the generic infrastructure

Other than the substance of a message, a reporting party first wants to know whether the requesting party has actually received the message that has been sent. This is because it does not want to be told in the event of a dispute that the administrative authorities have no record whatsoever of any declaration. Article 2:17 paragraph 2 of the Awb (Dutch General Administrative Law Act) states: *"A message is deemed to have been received by an administrative authority at the time and date the message reaches the authority's data processing system."*

In the context of SBR, the generic infrastructure is the data processing system. The recorded time of receipt is the moment the message is 'technically' received. At that moment, nothing is yet said about whether the message can be processed. The technical and functional 'processability' can be determined by checks for reliability, confidentiality and completeness, and checks on the functional content of the message. The reporting party is expected to take action if it is found that the message cannot actually be processed. For example, the feasibility of processing in a system such as the generic infrastructure can only be determined after a number of checks performed following the moment of receipt. The law (Article 4:3a of the Awb) requires a confirmation of receipt for any electronically submitted/filed message.[14] This confirmation does not need to be sent at the exact moment of receipt, but can be provided later, after the technical feasibility of processing has been established. The confirmation should be traceable back to the message. Traceability is important because a reporting party might send multiple messages (e.g., sending an additional message before confirmation of the first one was received).

In the event of an erroneous message, a correction would only be sent if the message concerned can be identified in the error report and/or confirmation. Otherwise, the reporting party may have to submit/file everything again. A administrative authority is also allowed to reject a message. Pursuant to Article 2:15 paragraphs 2 and 3 of the Awb, a message can be rejected if its acceptance would lead to a disproportionate burden on the administrative authority, and if the reliability or confidentiality of the message is not sufficiently safeguarded. An example of the latter is when the verification of whether or not an intermediary is really authorised by a client to submit a specific message comes back negative. Based on Article 2:15 paragraphs 3 and 4 of the Awb, the administrative organisation is obliged to inform the reporting party – in this case the intermediary – about this rejection.

The legislation mentioned above applies to the entire message flow of SBR I-processes, including the submission processes of the Tax and Customs Administration, the deposition of financial statements with the Chamber of Commerce,

[14] It is generally assumed that the requirement to provide a confirmation of receipt applies to all types of electronic messages, including those not related to requests.

and the submission of statistical information to the Statistics Netherlands. The set of requirements posed by legislation has led to the design for the submission service of the generic infrastructure shown in Figure 6.14.

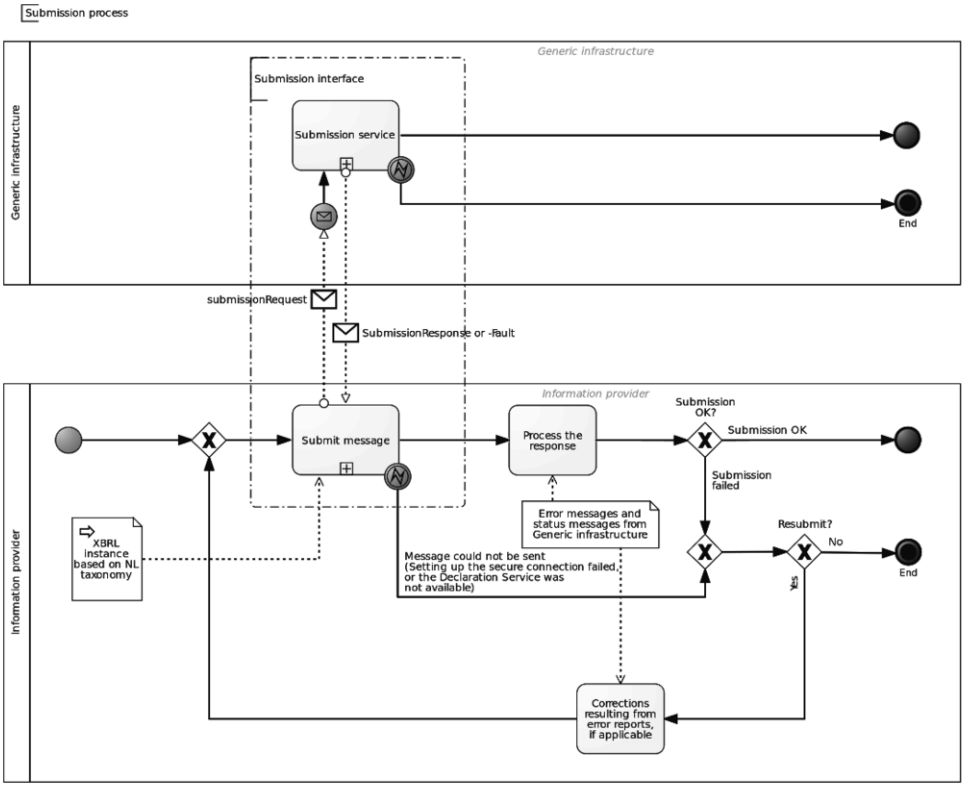


Figure 6.14 – An outline of the submission I-process

The declaration service handles a single submission in a single session of the declaration process. The information provider can include its own declaration reference in the message. The declaration will always result in either a submission error or a technical confirmation of receipt.

Two basic checks are performed in the declaration service to establish whether a message meets the following criteria:

- It has a proper web service security header, ensuring that the reliability of the message is sufficiently guaranteed;
- It does not exceed a maximum allowable message size.

Failure of either element would result in an error report. This error report can always be traced back to the message because it is created in the same session as the message. However, it does not note the submission reference number that was included, since the generic infrastructure will not handle potentially high-risk messages. This is done to prevent viruses or denial of service (DOS) attacks.

The traceability of the error report back to the message must, in such a case, be realised at the session level by the reporting application of the reporting party. However, if these checks have been performed properly, the message will be secure. Figure 6.15 shows the checks in the first part of the submission service.

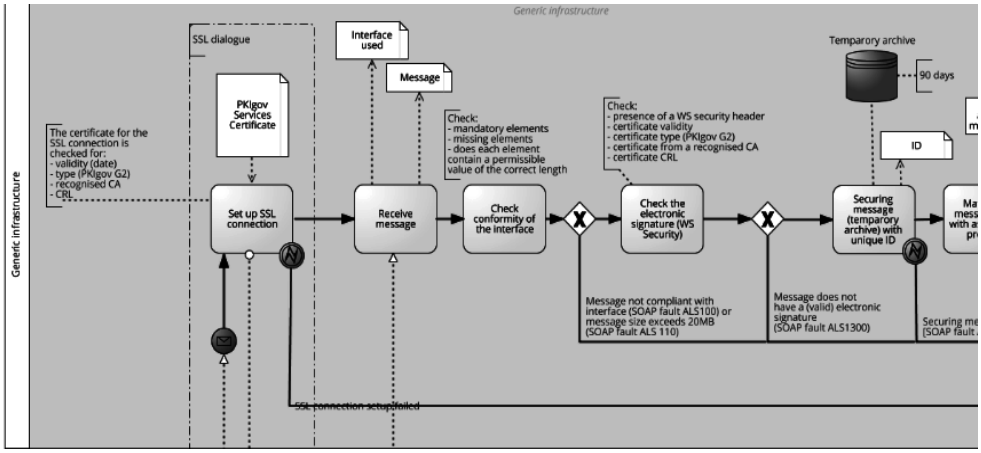


Figure 6.15 – Initial checks in the submission service

When picking up a message for further processing, the submission service performs various checks that may lead to a formal rejection of the message. However, such error reports always state the submission reference number that was included in the rejection. This makes it possible to trace the error report at the message level. The original message is also secured. Should a dispute arise about a rejection or onward delivery, the original message is retrievable for at least 90 days.

If it turns out that a message can indeed be processed by the generic infrastructure, a technical receipt response will be sent. This is a message containing the reference included by the information provider and a process ID allocated by the generic infrastructure. Further processing of the message can be tracked using this reference. After the technical receipt response, checks will also be performed in the generic infrastructure and by the requesting parties. Because of these checks, the message may be rejected and not processed further. Once an information provider knows that a message has been properly received, it must also be able to determine whether the message has been accepted for processing, i.e. whether it is functionally 'processable.' The information provider does this by initiating a new session in the generic infrastructure to request status information about the message.

Compliance with formally required submissions: acceptance for processing

Any message must comply with the functional requirements for the report in question. These requirements are imposed by or based on domain-specific legislation and regulations. Depending on its internal processes, the requesting party

can establish the level of compliance, with/after the option of corrections, and confirmation to the information provider by the latter if necessary. In an older version of the submission I-process, the Tax and Customs Administration and the Chamber of Commerce sent the confirmation as a separate notification. In the current process setup, parties are given status information about processing by the requesting party through the same status information service as used for the generic infrastructure. The information provider can follow the message status until the final status has been reached. The requesting parties provide a notification of the final status of a message that has been accepted for final processing. From that moment on, the message can be 'supplemented'. In other words, it should be possible for the information provider to supplement the message within such time limit as set by the administrative authority (Article 4:5 paragraph 1 of the Awb[15]).

Archiving

The 1995 Archives Act (Bulletin of Acts 1995, 276) prescribes how a government organisation should handle data that it has drawn up or received. The law also regulates the format, selection, retention and destruction of archived documents. The Explanatory Memorandum to the 1995 Archives Act states on page 4 that one of the key objectives of archive policy is to ensure careful and selective storage of information. This means that not all information should be archived. According to the law, archive documents include "*documents, irrespective of their type, received or drawn up by the governing bodies, that by their nature are clearly intended to be stored there*" (Article 1 sub c of the 1995 Archives Act). A number of elements of the Archives Act have been detailed in the Archives Decree (Bulletin of Acts 1995, 671), the principal implementation regulation of the Archives Act. The second regulation is the Archives Regulation (Netherlands Government Gazette 2010, 70).

The Archives Regulation also states the following in Article 17:
"The responsible party ensures that the following can be determined at all times for any archived document:

a. *the content, structure and appearance when it was received or drawn up by the government organisation, insofar as such aspects have to be known for the execution of the working process in question;*
b. *when, by whom and under what task or working process it was received or drawn up by the government organisation [...]"*

The original appearance of a message and the metadata (such as the time of receipt and the underlying task or action) need be recorded from the moment

[15] If the reporting party has not complied with any requirement made by statutory regulation for the message to be dealt with, or if the information and documents supplied are insufficient to allow the message to be assessed or the administrative decision to be prepared, the administrative authority may decide not to deal with the message, provided the reporting party has been given the opportunity to supplement the message within such time limit as set by the administrative authority.

that the archive documents have been received in order to ensure that the authenticity (conformity with the originally recorded version) can be verified.

The generic infrastructure handles electronic messages. The content of an electronic envelope—the actual instance—is Base64 encoded. To allow the message to be validated, decoding is required. In addition, the generic infrastructure replaces the original WS (web service) security header with a WS security header of its own. If an information provider thinks that the processed content does not match the content that was sent, it will want to check the message originally received by the government against the message they believe should have been processed. Article 17 of the Archives Regulation states that the requesting party should indeed be able to see this message later. Figure 6.15 shows how the message is secured immediately after checking the WS security header.

The unmodified message is temporarily stored (for at least 90 days) in case any corrections to a process should become necessary. Since the authenticity of the message cannot be determined before the check of the WS security header, storing it before this point would be a risk. If further processing of the message shows that it concerns an archived document, the generic infrastructure will place the secured original message in a temporary archive. This temporary archive can be linked to relevant decentralised archives of the requesting parties.

Securing / Reinjection
Another advantage of securing the messages is that the government will be more able to take responsibility for the message as "received." Reinjection means resubmitting a message into a process after processing has been stopped due to a technical error. At the beginning of 2013, the exact setup for reinjection was still being worked on by the processes/technology working group and the architects at Logius.

To date, the following choices regarding reinjection have been made. The process starts when certain technical errors occur. If reinjection is successful and the process goes well, the information provider will be sent the standard confirmation by the generic infrastructure for each declaration step. If reinjection fails, the information provider will be sent an error report at the end of the session, from the service where the technical error occurred.

From a legal perspective, the following are important:

- That the information provider will receive a positive or negative response to its submission/filing (confirmation of receipt or error report) right away (as required by the Awb and the principles of due care, transparency and legal certainty)
- That, in case of failed delivery, the information provider will be provided an error report as feedback via the status service, so that it can determine where the error occurred (Article 2:15 of the Awb)

- That if the process has progressed correctly, the information provider will receive a confirmation of the final status, including the time of the status report.

The submission I-process satisfies the requirements outlined above. Because reinjection takes place within the declaration process, the above elements are also guaranteed for the reinjection. The legal position of the information provider may change as a result of the error report or confirmation, but not as a result of the reinjection. All statuses of a message—including reinjections—will be sent to the information provider.

6.7.3 *Various requirements for reporting processes*

One of the requirements of the SBR solution is that the generic infrastructure should not only be able to execute I-processes, but should also be able to execute these processes according to multiple I-process configurations. The reason for this requirement is that the service levels required can vary for different information chains. While general legalisation (e.g., AwB) applies, the I-processes and the generic infrastructure are also subject to requirements based on the specific context of their domain. This is logical, as general laws often stipulate that something should be 'sufficient for a specific purpose…' The final processing therefore depends directly on the domain context. As will be discussed in Chapter 8, the setup of the overall chain process also strongly determines the requirements that will be imposed on the generic infrastructure I-processes. Differences within SBR revolve around the quality aspects of the processes in particular. For instance:

- How bad is it when an I-process becomes temporarily unavailable? It is worse for declarations with hard/fixed deadlines that are submitted in large volumes than for processes with rolling deadlines that are submitted in smaller numbers. If alternative filing channels are still available, we can expect different service level requirements regarding the availability of the submission I-process.
- How bad is it if the information is not handled confidentially? If a document is sent for publication, its confidentiality is less of an issue than a document that contains confidential information that must not be revealed. Seen that way, tax declarations are more confidential than financial statements.
- How bad is it if the information is not found to be authentic? In this case, information that is published and also used by many parties (e.g., the financial statement) can cause more problems if the copy is not authentic than if a non-authentic document causes a single party to receive an incorrect assessment. In that case, the requesting party and the information provider would have to find out together how the non-authentic information ended up in the chain.

In practice, the service level requirements used in the generic I-processes largely correspond to the requirements of the party with the largest interest in information assurance (see Chapter 8). The requesting parties look at their own context to determine what service levels are required for an information flow. Logius's latest service description makes a distinction between two different service levels: baseline and operational excellence. Both service levels comply functionally with the Online Administrative Business Act. Offering a choice between two service levels is more efficient than determining a unique service level for each process. Based on the legislation, it can be stated that the message flow must be sufficiently reliable. The baseline level is sufficient for some reporting flows (e.g., the financial statement, where a business files once a year and where declaration passed a deadline will not cause problems), while the operational excellence level is required for other flows (e.g., VAT declarations, since late submissions will result in penalties). The basic principles of the SBR solution architecture—separation of functionality and technology, and loosely coupled services that perform I-processes—help work with the two service levels.

6.7.4 *Checking against standards*

Compliance management involves designing, setting up, implementing, managing, verifying and reporting on conformity to the rules. The role of the auditor is to perform checks against the standards and to express an opinion about compliance. An auditor collects factual data from the past to determine whether a process is compliant. Performing checks within chains is not easy due to the many parties involved, the dynamics of the I-processes, and the IT systems themselves. There should be an organisation that takes responsibility for the compliance of the chain as a whole, rather than focusing solely on its own link. Checks within chains involve many organisations and cover IT as well as organisational aspects. These checks therefore require knowledge and insight from auditors (in both breadth and depth), which is not necessarily readily available. Chain partners can help auditors by doing the following:

- Setting up and maintaining an integral standard framework (in terms of legislation, performance and policy) by which the I-processes will be designed for each flow
- Building sufficient checks and monitoring into the I-process. A proper audit trail is indispensable for this.

6.8 Chapter conclusion

Several methods and techniques are available for designing I-processes. A great deal of systematic research has been performed and various principles have been published. Issues in the process are handled by continuously improving it. However, there is no perfect recipe for creating a good process. Architects from throughout the chain must be able to recognise the trade-offs in specific domains when designing or redesigning a process. Especially in the case of public/private information chains, many trade-offs and all kinds of interests need to be considered (see Chapters 2 and 3). The choice to break processes down (decomposition) or to apply the Lean philosophy or the Theory of Constraints also involves trade-offs. Translating concepts into practice is often more difficult than expected. As a reference case, SBR examples may provide some help in this regard. Next, Chapter 7 elaborates on the generic infrastructure. As operator of the generic infrastructure, Logius has as an important role designing and maintaining I-processes in business reporting chains. Logius is tasked with managing the development and maintenance of generic I-processes based on the prevailing legislation and regulations, and must make sure that the processes can be utilised by the various public parties involved in business reporting. Requesting parties that utilise the generic I-processes and the supporting generic infrastructure to handle part of the complexity of information exchange between organisations, can therefore be sure of compliance with the prevailing legislation and regulations.

7 Technical Foundations of SBR

Chapter highlights

- Specifying the interactions between chain actors
- Understanding the enabling technologies
- Demystifying the generic infrastructure

7.1 Introduction

The two preceding chapters have given a detailed explanation of information processes (I-processes) and data specifications as key components of the SBR approach to inter-organisational information exchange and processing. This chapter looks at another key component – the technology behind the generic process infrastructure (from here on: generic infrastructure).

The goal of this chapter is to provide a detailed description of the technology aspects of the generic infrastructure. Here, technology refers to 'information and communication technology' (ICT). Much has been written on the various aspects of ICT. Even if we were to limit our scope to ICT for business reporting alone, we would need far more than one chapter to cover the relevant aspects of the ICT used for inter-organisational information exchange and processing. For example, numerous books have been published solely about the implementation

Brief definitions of key concepts

- I-processes: non-core business processes of the requesting parties (e.g., authentication, authorisation and validation). The use of I-processes is also known as information pre-processing.
- Generic (process) infrastructure: shared interface services and I-processing services (including software and hardware) used for S2S information exchange and processing.
- Shared service centre (SSC): the third-party operator of the multi-sided platform that provides operational and chain coordination services.

of TLS (the protocol for secure communication over the Internet). Such is also the case for technical concepts such as service oriented architectures, web services, and orchestration. We will find that these same concepts are, in fact, key ingredients of the generic infrastructure used for SBR.

Given our broad conceptualisation of technology, we first need to establish a clear objective and structure for this chapter. Taking the perspective of the various chain partners in business reporting (see Chapter 1), this chapter is structured so as to provide chain partners with detailed answers to the following questions:

1. What are the basic interaction patterns between businesses and government agencies that need to be supported by the technology?
2. What design configurations can support these interactions? Which configuration is currently being implemented in the Netherlands and why?
3. What are the requirements for the generic infrastructure?
4. What technologies have enabled the realisation of a generic infrastructure?
5. What are the building blocks that form the currently operational generic infrastructure?

In order to answer these questions, this chapter is structured as follows:

- **Section 7.2** focuses on the first question, describing the basic interactions between businesses and government agencies. These actors interact in a predictable way, allowing the identification of some generic interaction processes or patterns. Standardisation of these interaction patterns allows the 'move to the middle,' (Clemons & Row, 1993) in which a shared service centre (SSC) takes care of the information exchange and pre-processing (I-processes). The cost efficiency of handling transactions using generic building blocks is the trademark of an SSC (see Chapter 1). Nevertheless, a more careful look at the interaction patterns reveals that some information chains have specific characteristics that pose additional challenges to information exchange and processing. For instance, some chains require that authorisation claims be checked while others do not. This is why requirements for information exchange processes need to leave adequate room for a certain amount of flexibility. Requirements such as the use of open standards, system-to-system exchange and end-to-end security will also be discussed.
- **Section 7.3** considers the second question and presents four different design configurations. The key question addressed is what can be standardised and what should be moved to the middle.
- **Section 7.4** discusses the main requirements for the generic infrastructure.
- **Section 7.5** addresses the fourth question, elaborating upon the main technologies (concepts and standards) that facilitate the realization of a generic infrastructure.
- **Section 7.6** answers the fifth question by describing the building blocks that form the generic infrastructure. This section provides an overview

of the currently available interface specifications, the supported I-processes and the current service portfolio. Note that the term 'generic infrastructure' refers to standardised components that are dynamically deployed to handle specific I-processes for a specific type of business report (or return message). Associated terms include 'shared service centre' and 'multi-sided platform.' The exact relationships between these terms will be specified in this section.

- **Section 7.7** concludes this chapter with a brief reflection on the current generic infrastructure.

7.2 Interaction patterns

When it comes to information exchange in the context of business reporting, businesses and government interact in multiple ways. From a birds-eye view, three basic interaction patterns can be distinguished: (1) requests for information, (2) submitting of information/business reports and (3) the submitting of a final response. Figure 7.1 illustrates this simplified overview of the processes (with no intermediaries shown).

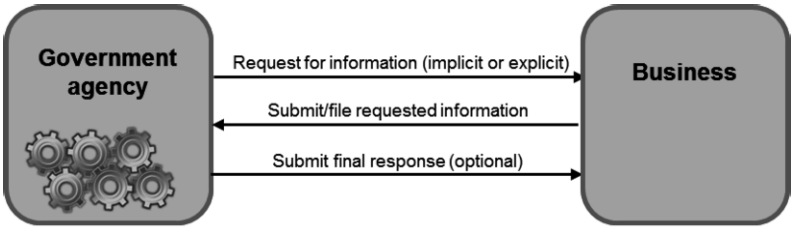


Figure 7.1 – Three high-level interaction patterns

In many countries, the request for information by an independent regulatory agency is dictated by law. The request can be implicit, meaning that the public agency assumes that the business knows the law and will provide information accordingly. The request can also be explicit, meaning that a formal obligation to share information is communicated in some form (e.g., a letter, phone call, fax or email). Take, for instance, a letter from the Tax Office that reminds a shop owner that he or she must submit a tax declaration for the business by a specific date. Depending on the nature of the requested information, the government agency might provide specific guidelines, templates or even delivery channels (such as portals) that the business should employ when submitting business information. The agency might even prescribe a set of business terms and definitions that the business needs to incorporate into its reports. When submitting the requested information, the business might receive an acknowledgement of that submission. After the submission, the assumption is that the receiving government agency will process the report and prepare a final response (the closing interaction). The duration of this final phase of the reporting is different for each information chain. Depending on the type of information chain, there might be a need for an intermediate interaction. Take, for instance, a business's desire to

obtain information regarding the status of a submitted business report (e.g., Has it been received? Is it waiting to be processed? etc.). In the end, the business will need to wait for the report to be processed by the government and to receive a final response. In Figure 7.1, the cogs in the government agency box represent the basic I-processes that are executed upon receiving a business report. Examples of such processes include identifying the sender, validating the report structure and acknowledging its acceptance for further processing. After such I-processes (see Chapter 6 for more details on I-processes), the government agency begins its agency-specific and content-oriented processing.

While this process is fairly straightforward, the situation becomes more complex when we consider the fact that businesses a required to report to (and thus interact with) multiple government agencies. Such a situation is depicted in Figure 7.2.

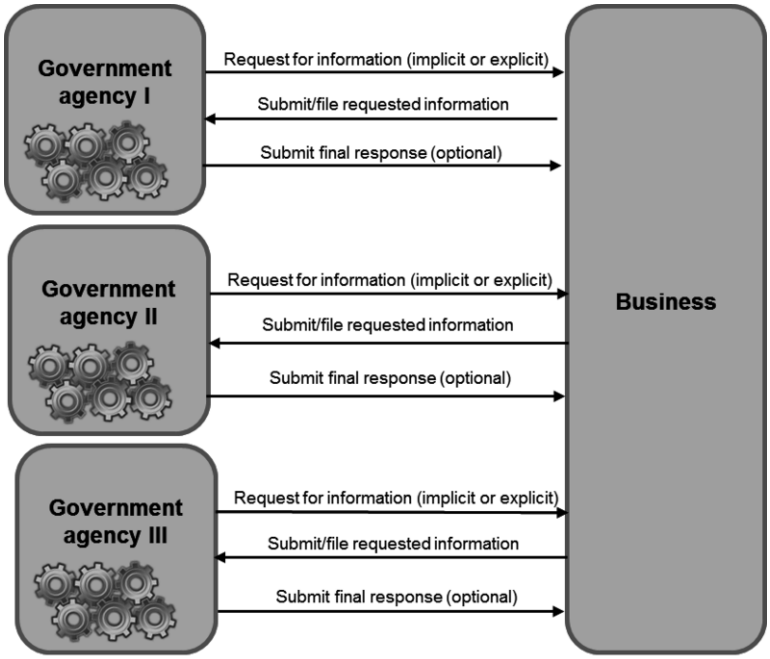


Figure 7.2 – Different government agencies interact with businesses in a similar way

Figure 7.2 depicts a situation that is common in many democratic societies: a business must interact with multiple government agencies in a similar way. This means that the same interaction patterns can be found in several information chains. However, even if the interaction patterns appear to be similar from a distance, for individual businesses, the unique features of the interactions often fuel the perception of an inefficient government and high administrative burdens. These features include the following:

- Many moments of contact between the business and various government agencies
- Many different channels (letters, portals, e-mail, phone, fax) used for communication
- Random requests for information, differing in form and content (lack of uniformity in the definitions of terms)
- Feedback from government agencies (for instance, in the form of tax returns) received at different times and in different formats
- Particularly for businesses that wish to report without the help of intermediaries (self-filers), choosing the appropriate form (document template) amongst several options for a specific declaration can be time consuming.
- Heterogeneous interactions take up much time. Time is a scarce resource that businesses would rather spend on core business processes.

In the Netherlands, some projects (NTP and GEIN – see Appendix A) were initiated to help reduce the administrative burden on businesses and improve their reporting experience. One of the fundamental insights from these projects was the importance of starting with 'chain reversal.' Conceptually, this means that instead of initiating interactions from the perspective of what kind of information the individual government agency wants, the interactions should re-modelled based on the features of the administrative processes and information systems of the businesses. This concept of chain reversal is illustrated in Figure 7.3. The cogs on the business side need to be understood. What data does a business have? How does it collect, store and submit this data? What kind of software does it use for which processes? How advanced is this software and what are the possibilities for more efficient data collection, storage and exchange? Are intermediaries involved? These are all questions that influence the interactions and determine their perceived efficiency and effectiveness. The concept of chain reversal was an important first step in SBR.

Using chain reversal, careful analysis from a supra-governmental perspective yielded two conclusions:

1. On the outside, the interaction patterns between businesses and government agencies appear to be similar. Note that this does not mean that the same processes were done in the same way. For instance, there were several ways information could be submitted (e.g., paper, portal, phone, fax, alternate forms, etc.) In other words, the same interaction can involve different components for completing a specific activity.
2. Looking at the government agencies, each started with the same I-processes (authentication, validation, etc.) as a form of pre-processing, prior to initiating more agency-specific processes (content-specific evaluation, decision-making, etc.). Following these specific processes, the return flow activities—the interactions between the government and the business regarding the intermediate/final response—also show signs of similarity across government agencies.

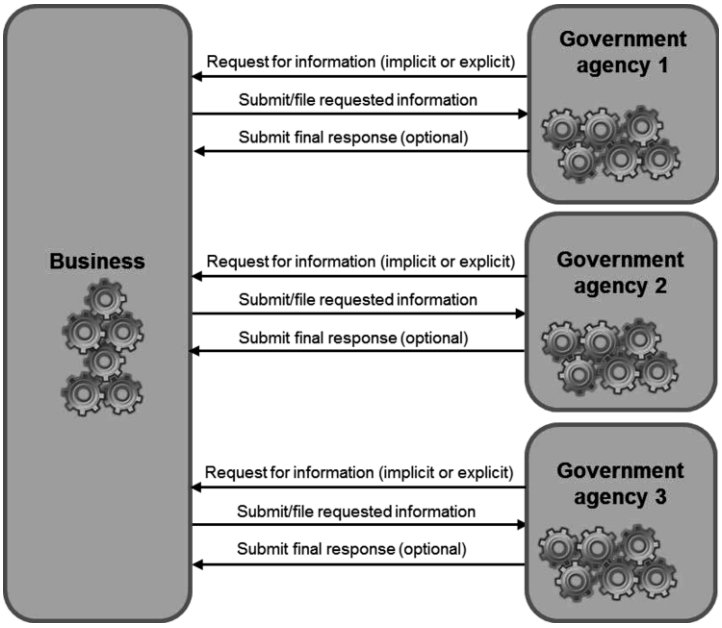


Figure 7.3 – Conceptually reversing the chain: putting the business at the centre of business reporting

Both conclusions prompted further investigation into the possibilities for standardisation, specialisation and the move away from vertically integrated information processing at government agencies. Here, standardization includes the way interactions take place (their sequence) and the components used for information processing activities. When the various interaction processes are implemented in a standard way, a business only needs to learn one way of interacting with the government. The same holds for the components used for interaction processes. To ensure that the interaction processes are implemented correctly and in the same manner, it is important that they be described in a standardized way. In this way, all the actors and systems involved will know what do, when to do it and how to do it. Alignment of processes is required for efficient and effective information exchange and processing. Chapter 6 explains how processes were standardised for SBR and why the Business Process Modelling Notation (BPMN) was used to describe the processes.

Arguments for standardisation can be found throughout this book. Chapter 5 encourages the standardisation of syntax and semantics. Chapter 6 promotes the standardisation of information processes. We have yet to address the question of what to standardize on the technical infrastructure level. In order to understand the standardisation options there, the following section elaborates upon four different technical configurations for information exchange and processing.

7.3 Configurations for standardisation of information exchange and processing

7.3.1 *Four archetypical configurations*

As the previous section concluded, standardisation is the key to improving the interactions between businesses and government agencies. In order to address the question of what should be standardised in terms of the technology that facilitates information exchange and processing, we first need to understand the existing opportunities for standardisation when it comes to information exchange and pre-processing. Looking at four archetypical design configurations allows us to pinpoint these opportunities.

There are four possible configurations for information exchange and processing:

1. Configuration A: multiple proprietary I-process infrastructures with heterogeneous interfaces
2. Configuration B: multiple proprietary I-process infrastructures with standardised interfaces
3. Configuration C: multiple standardised I-process infrastructures with standardised interfaces
4. Configuration D: a single generic I-process infrastructure with standardised interfaces (operated by a shared service centre)

Two design variables shape the above configurations: interface standardisation and I-process infrastructure standardisation. Note that system-to-system (S2S) information exchange is assumed in these configurations, meaning that information is exchanged in an electronic format via an interface between two applications/software systems. An interface refers to the implementation of a set of agreements and industry standards permitting the exchange of electronic data between information systems.

The four configurations are discussed below. In Figures 7.4 through 7.7, the standardised processes are depicted with white boxes. A table highlighting the similarities and differences between configurations will be presented at the end of the chapter.

Configuration A: multiple proprietary I-process infrastructures with heterogeneous interfaces

The first configuration symbolises what is now considered—at least in the Netherlands—as the 'traditional approach.' In this configuration, each government agency has its own proprietary 'modality,' meaning that it defines how a business can create a linkage (also known as an interface) and submit business reports. In addition, each agency has its own dedicated I-process infrastructures to handle interactions and I-processes (e.g., checking sender identity and determining whether reports have been structured according to specification). Figure 7.4 presents a simplified representation of this configuration.

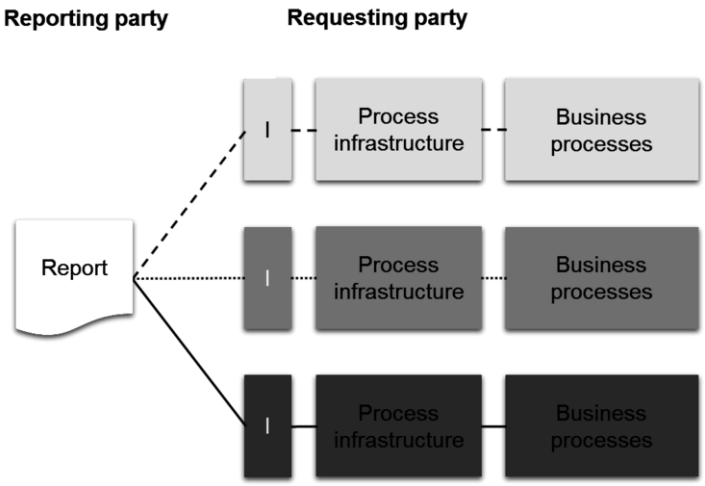


Figure 7.4 – Configuration A: multiple proprietary I-process infrastructures with heterogeneous interfaces

Configuration A is characterised by heterogeneity across interfaces, I-process infrastructures and business processes. Several technical exchange standards and components are used for I-processes such as authentication and authorisation. Reports are exchanged in different formats (e.g., pdf, word, xml) and businesses (with or without intermediaries) must use multiple interfaces for interaction. Requesting parties are fully autonomous in defining how they want to interact with businesses.

Configuration B: multiple proprietary I-process infrastructures with standardised interfaces

Configuration B differs from A in that the interfaces are standardised, as shown in Figure 7.5.

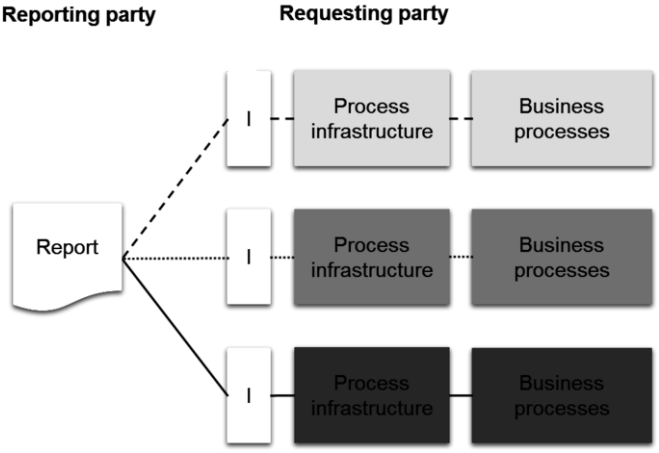


Figure 7.5 – Configuration B: multiple proprietary I-process infrastructures with standardised interfaces

Configuration B addresses the problem of businesses having to understand and utilize multiple interface specifications for information exchange (as in Configuration A). In this configuration, a business can exchange messages with multiple government agencies using the same interface specifications. It is assumed here that the government agencies have agreed on a single type of interface for information exchange. For this to happen, the government agencies involved would need to give up some degree of autonomy in decision-making regarding the interface, for instance, when deciding how to deal with updates. It should be noted that in this configuration, the government agencies still have their own proprietary I-process infrastructures.

Configuration C: multiple standardised I-process infrastructures with standardised interfaces

In the third configuration (C) for S2S information exchange, both the interfaces and the I-process infrastructures are standardised, as shown in Figure 7.6. From a government perspective, this configuration represents the so-called 'enterprise architecture' approach, in which the same architecture and design principles are utilised by all government agencies. This means that all government agencies—as part of the same enterprise—utilise exactly the same interface specifications, middleware, software and hardware ('the same boxes everywhere') for S2S information exchange and I-process execution. Configuration C thus requires some form of centralised decision making regarding IT and public-private interactions.

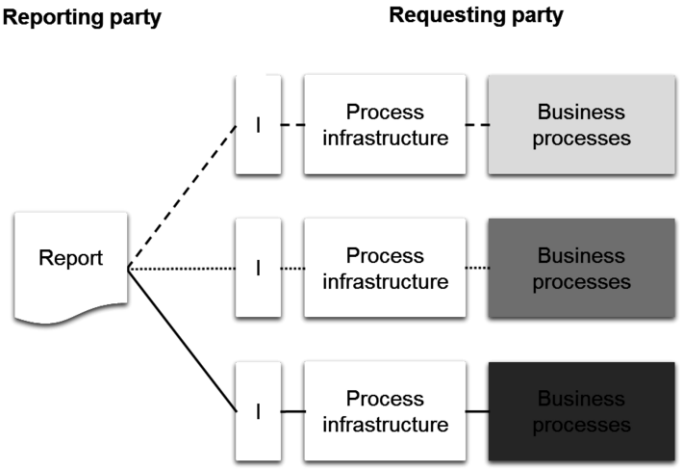


Figure 7.6 – Configuration C: multiple standardised I-process infrastructures with standardised interfaces

Configuration D: a single generic I-process infrastructure with standardised interfaces (operated by a shared service centre)

Configuration D involves a highly standardised form of S2S information exchange via one set of interface specifications and a single I-process infrastructure that executes standardised I-processes for multiple government agencies. The

separate but uniform I-process infrastructures see in Configuration C are abandoned for a standardised and consolidated ('move to the middle') I-process infrastructure that is shared by various agencies. This allows for the introduction of a shared service centre that acts as the commissioned operator of the generic I-process infrastructure.

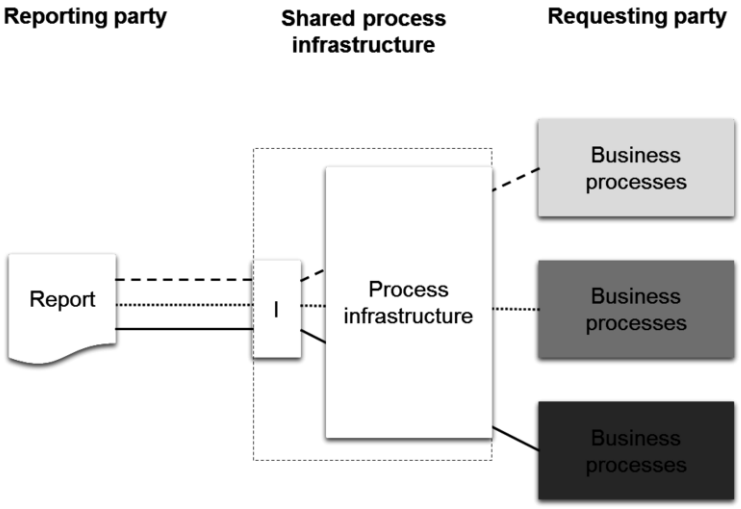


Figure 7.7 – Configuration D: a single generic I-process infrastructure with standardised interfaces (operated by a shared service centre)

The generic I-process infrastructure (generic infrastructure for short) is the entirety of resources such as hardware, software and network equipment, including security policies that are required for S2S exchange and execution of I-processes for multiple information chains. The generic infrastructure is operated by a shared service centre (SSC).

7.3.2 *Comparing the four configurations*

Each configuration has its own pros and cons. Configuration A—which represents the world of information exchange prior to SBR in the Netherlands—was often considered to be burdensome for all chain actors. Moving to Configuration B, with its slightly higher level of standardisation at the interface level (and non-standardised proprietary I-process infrastructures), might seem attractive, especially because doing so requires few major changes from Configuration A. In addition, the impact on the parties' autonomy is minimal and the strategy does not require discussions about who owns the infrastructure components. However, the danger with Configuration B is that the lack of a single development platform may lead to several different types of configurations and distinct implementations within separate infrastructures, making it all but impossible to manage the cohesiveness between these different infrastructures. Furthermore, if old systems have to be linked to new systems often causes technical problems that can only be resolved with a high degree of technical knowledge. Such knowledge

is scarce and expensive. However, the same I-processes are developed and managed multiple times by each party in Configuration B, the result is duplicate development efforts/costs and wasted resources in terms of technical expertise.

Configuration C is often found in large enterprises/multinational corporations that have a centralised IT department and multiple geographically dispersed settlements with small IT support departments. In theory, this configuration can solve most interoperability problems and makes economies of scale possible on a number of fronts (e.g., decreased coordination costs, software licence costs, learning and training costs, etc.). On the other hand, this configuration has some drawbacks, including the following:

- Rigid management is required to ensure success and to prevent relapse back to Configuration B.
- For some collaborating parties, disinvestments in proprietary I-process infrastructure must be made.
- For the government, homogeneity is often associated with huge investment. Once designed, the same I-process infrastructure must be deployed several times in different government agencies. Such action does not match well with society's overarching desire for a compact government (see Chapter 1).
- The throughput time to move from configuration A to C is relatively long. These are complex transformations that may easily be underestimated (Berkelaar, 2007).
- The parties must be willing to give up their autonomy to determine the design of their I-process infrastructure. This means that a consensus must be reached, or that a supra-governmental department must have sufficient power to enforce the decision.
- The parties must be willing to accept a one-size-fits-all position, leaving no room to cater to exceptional demands.

The final two drawbacks are also the case for Configuration D. Table 7.1 provides a summary of the key features of the various configurations.

For the SBR case in the Netherlands, Configuration D was chosen and realised. The features of this configuration have proven very attractive, especially for government agencies. The installation of an SSC, for instance, reduces the transaction costs, at the same time increasing the total number of customers reached by the requesting parties. In the literature, this is known as the "*electronic brokerage effect"* (Malone, Yates and Benjamin, 1987). In addition, Configuration D avoids most of the downsides to Configurations A, B and C that were listed above.

Table 7.1 – Summary of configurations

Configuration	A. Traditional/ heterogeneous I-process infrastructures	B. Proprietary I-process infrastructures	C. Homogenous I-process infrastructures	D. Generic infrastructure
Interfaces	Proprietary	Standard	Standard	Standard
Functionality development and management	Individual	Individual	Shared	Delegated to an authorized specialised organisation
Design of I-processes (flow, use of components)	Proprietary, divergent	Proprietary, divergent	Imposed, homogenous	Agreed-upon, centralised, reused
Knowledge required in each chain organisation	High	High	Medium	Low, knowledge pooling, centralised expertise, learning and training
Chain governance	None	Limited to agreements on interfaces (decentralised)	Medium, including agreements on interfaces and I-process infrastructures	Public-private collaboration using a framework of agreements
Transaction costs for businesses	High (need to understand and implement various specifications)	Medium	Medium	Low
Transaction costs for the government	High	High	Medium	Low (economies of scale)

From a conceptual perspective, the generic infrastructure is the bedrock for a multi-sided platform (MSP). An MSP is a concept that comes from institutional economics and is defined as "*products, services or technologies that connect different types of customer groups to each other*" (Hagiu and Yoffie, 2009, p. 75). The concept of a 'platform' refers to a number of coherent building blocks. 'Multi-sided' refers to the fact that multiple types of consumer groups use the platform's building blocks for their own interactions and processes. In the case of SBR, the customer groups include reporting parties (businesses and intermediaries, but also public agencies), software providers (e.g., accounting and reporting software) and receiving parties (government agencies, but also private actors). The range of MSPs in practice is wide (Boudreau & Hagiu, 2010). Frequently studied examples of MSPs, however, come from the digital entertainment industry, with platforms such as iTunes, Google Play, Sony PlayStation Network and the Apple

App Store. Markus and Bui (2012) also cover MSPs such as Visa Inc., a payments network that coordinates billions of transactions each year, and networks for public safety information sharing (e.g., Capital Wireless Information Net), which function as inter-organizational coordination hubs.

MSPs deal with the various types of customers without being the owners of the data exchanged. This allows MSPs to support mutually dependent actors. In the SBR case, the MSP not only facilitates but also regulates S2S information exchange and I-process execution through strict specifications that apply to all user groups. What these specifications are and the way they are managed is laid down in the SBR framework of agreements (see Chapter 1).

Moreover, as various scholarly works on the economics of standardization have noted, the formation of an MSP results in so-called 'network effects' (Cusumano, 2005). Katz and Shapiro (1985) distinguished between direct and indirect network effects. A telephone becoming more valuable to an individual as the total number of telephone users increases is a direct network effect. In the context of business reporting, direct network effects means that reporting parties benefit from an increasing number of requesting parties (both public and private) that use the MSP. Network effects can also be indirect, and these are sometimes very powerful as well. Indirect network effects exist when an increasing number of users stimulates the platform operator to develop complementary services that then increase the value of the initial platform. For instance, A Blu-ray player becomes more valuable as the variety of available Blu-rays increases, and this variety increases as the total number of Blu-ray users increases. In the context of business reporting, the operator of the SSC will be motivated to develop more complementary services as more information chains join, since more users mean greater investment potential. Additional services should enhance the quality of the MSP, making it more attractive to other information chains.

Nevertheless, when it comes to such large-scale transformations, particularly in the public domain, it is well known that many factors determine the outcome. To maintain the focus of this chapter, we will not address all these factors. However, interested readers refer to Appendix A for an overview of the various projects and programmes that were implemented in the Netherlands, leading up to the implementation and large-scale use of the generic infrastructure.

7.4 Requirements for the generic infrastructure

The Requirements Elicitation Programme for the generic infrastructure (GEIN) – one of the predecessors to the SBR programme – was fundamental to the development of the generic infrastructure used in SBR chains. At the time, the technical and legal architects collaborating in the GEIN programme considered the different configurations described in Section 7.3 and advised the Dutch government to develop a generic process infrastructure (Configuration D). The final programme report includes a long-list of requirements and a first sketch of the architecture for the generic infrastructure. The sketch, which was discussed in

Chapter 1, includes a uniform data specification (the Netherlands Taxonomy) and I-process specifications. The current generic infrastructure comprises web services that are used to establish interfaces between systems and to carry out specific I-process flows. The components of the generic infrastructure are discussed in Section 7.6.

Before discussing the enabling technologies and resulting components, let us first consider the most important functional and non-functional requirements for the generic infrastructure. Such a consideration will be brief, as the GEIN programme report includes extensive coverage of all the requirements from multiple different perspectives (business, technical, functional, legal, economic and service management).

The requirements were formed, in part, based the characteristics of the information flow that needed to be supported by the generic infrastructure. These characteristics include the following:

- Information is exchanged with a relatively high frequency.
- The size of the total information set is large.
- Some information is highly confidential. There is a need for accurate identification, authentication and authorization of parties exchanging information with one other.
- There is a need to validate the information submitted before accepting it for further processing. Validation helps in establishing the processability of the information.

Functional requirements for the generic infrastructure include:

- Flexible I-process orchestration: different type of messages (e.g., business reports, status updates, final notifications) may demand different I-process flows that use various components and services (e.g., the need to check authorisations).
- The generic infrastructure must be able to deploy multiple versions of the Netherlands Taxonomy.
- The generic infrastructure facilitates both the server-push and the client-pull models of interaction.
- All errors including those regarding date and time of occurrence, must be included in the audit trail.
- It should be possible to include in multiple electronic signatures in business reports.
- Reporting parties should be able to retrieve optional notification messages via the generic infrastructure.
- Return information can be directed to multiple parties (e.g., the business and its intermediary).
- End-to-end information security should be guaranteed. This means that the message exchange, from the moment of delivery by a reporting party to its final delivery to an information-requesting party, is secured. Note

that Chapter 8 is dedicated to describing how end-to-end security is achieved.

Non-functional requirements include:

- The generic infrastructure must be available 24 hours per day, 365 days per year.
- The generic infrastructure must automatically divide its workload (load balancing).
- Use of open standards: components must be reusable.
- Platform independence: information exchange must be possible regardless of the specific characteristics of the technical environment.
- Loose coupling: the generic infrastructure must be designed to withstand dynamic situations (e.g., policy changes, legislation and regulations, advancements in technology, etc.) by having components that are independent of one other.

The GEIN programme report details a far more comprehensive set of requirements. It should also be mentioned that the requirements listed by the GEIN programme were shaped by the technological developments occurring at that time (2006), including system-to-system integration, loosely coupled interfaces, web services and service-oriented architectures. We will provide a brief explanation of these enabling technologies in the following section.

7.5 Enabling technologies for the realisation of the generic infrastructure

7.5.1 *System-to-system integration*

SBR relies on system-to-system (S2S) integration, which generally refers to the extent to which the various technologies used within a chain can communicate with one other or can be used together for a given purpose. An important precondition for S2S integration is thus a high level of interoperability. We described the forms of integration in Chapter 1. The following is a summary of the main concepts regarding integration presented in Chapter 1, which will be useful for our current discussion:

- Interoperability is a precondition for S2S integration. Standards play an important role in ensuring interoperability in each building block of the SBR solution (including I-process specifications, interface services and processing services).
- The I-process specifications and message specifications mostly deal with defining activities. The 'actual' work is done by invoking and orchestrating several web services.
- The essence of the taxonomy is that businesses only need to do one setup process by mapping the concepts in the taxonomy onto their own data administration. They can then easily generate the various business reports: the 'store once, report many' concept. This should not be confused with one-off delivery of data.

- The interfaces are essential for the actual data exchange.
- The physical layer has become a commodity. There is little to no discussion about standards for physical components in the IT world nowadays. If a network is needed immediately, a TCP/IP network can be requested. Discussions about whether the network should be an X.25, token ring or TCP/IP network are a thing of the past. This means that now there is considerable agreement about the types of basic standards for the types of networks that should be used.
- SBR's choice for web services is based on a preference for individual interface standards.
- An enterprise service bus (ESB) makes it possible for different web services to communicate, which in turn allows them to execute a fixed, defined I-process.
- A process engine is required for automatic invoking web services according to a predetermined process diagram (BPMN).

This summary includes concepts such as interfaces, web services, the enterprise service bus and the process engine. Given how interwoven these concepts are, however, it is a challenge to find the proper sequence in which to discuss them. Using a message flow as a guideline, we get the following sequence of topics:

1. Interfaces (§7.5.2)
2. Web services (§7.5.3)
3. SOA for supporting flexible I-processes (§7.5.4)

7.5.2 *Interfaces*

An interface will be provisionally defined as a system-to-system connection between information systems that facilitates the exchange of information. Later in the chapter, it will become clear that this definition does not entirely cover the situation in practice. However, for now, we will focus on the functions of interfaces and the available standards.

A simple metaphor for an interface using a practical example is an electricity network. Let us assume that an interface is a socket that provides a service (electricity) in a standard manner (by means of a plug) using a standardised network. One only needs to 'plug in' in order to use such a service. It is not necessary to own a power station or to have any knowledge of how a power station works.

Interfaces are therefore important. So how is one chosen? Multiple variables play a role in the selection of interfaces for information exchange. First, the interface must be an open standard that is sufficiently well supported to ensure the continuous presence of solutions and expertise in the market. In addition, the interface needs to comply with the requirements imposed by the I-processes. The purpose of the information transfer determines the interface's required characteristics, such as the degree of reliability, security or capacity. Given the different features of the available protocols, multiple protocols can be used together in

order to comply with the requirements of multiple I-processes. From a practical and economic perspective, not *all* possible interfaces can be offered.

In theory, there are several standards for setting up interfaces. These are sometimes complementary and sometimes competitive. The exchange between service providers and users can be divided into three layers:

1. Content: this layer comprises the agreements made by organisations regarding the content of the message to be exchanged, including the structure, semantics, scope of values, etc.
2. Session (logistics): this intermediate layer can be split into two sub-layers:
    - Communication: refers to transport protocols (HTTP, SMTP etc.)
    - Application: refers to messaging standards (such as ebMS and WUS, which are based on SOAP), security (authentication and encryption) and reliability
3. Transport: this layer is responsible for the final transfer of messages.

Figure 7.8 summarises interface standards in a layered model. The relationships between the layers and the standards shown are explained below. The 'application-specific' blocks represent the possibility of many specific communication solutions for a certain application that have not been recorded in formal standards.

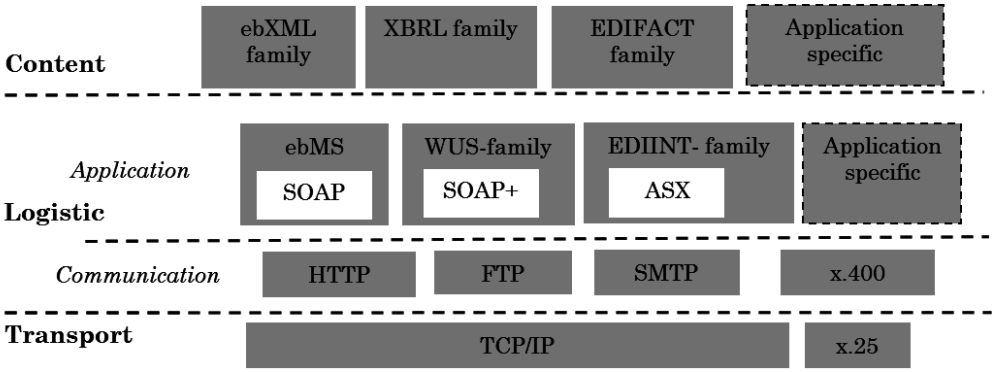


Figure 7.8 – Typical standards for the design and implementation of interfaces

The striking aspect of the figure above is that the content is kept strictly separate from the logistics and transport. This is because the content involves the information that needs to be transferred, irrespective of the means of transport chosen. The technique generally used is to pack the content into a standardised envelope. The transport layer and session layer will be explained in detail below. Then, we will take a close look at SOAP, as this is the most important protocol for the realisation of interface standards for SBR chains. The content layer was discussed in Chapter 5 (Data).

TCP/IP is used in the transport layer. The advent of the Internet has made TCP/IP a generally accepted standard for network communications and message exchange (Stallings, 2009). TCP/IP can also be used in closed data communication networks. The protocol can therefore be used for developing standard interfaces. In this chapter, TCP/IP is seen as a *fait accompli* and we shall not discuss its operation in more detail.

Strictly speaking, the upper layers can all be referred to as 'the application layer.' Practice shows that multiple layers can be applied here. A clear distinction exists between the layer used for the logistics of messages (irrespective of their content) and the layer used for the content (irrespective of its logistics). We can therefore split up the 'logistics layer' into two sub-layers: the communication sub-layer and the application sub-layer. These layers are discussed in detail as follows.

- The communication sub-layer is the layer where communication protocols such as HTTP, FTP and SMTP can be found. FTP deals with retrieving and placing *files* on a server. SMTP deals with providing and receiving messages such as e-mail from a server. HTTP was originally focused on retrieving and providing textual documents to a server. X.400, an older protocol whose use is currently decreasing, can also be found in the communication layer. Despite the different origins of these protocols, they can all be used to transfer content-based 'messages.' However, there are considerable differences between protocols in the way that this action is done. In particular, the amount of information available regarding the sender and receiver and the routing options are different for each protocol. The protocols do not provide security by default (other than through the connection itself) and they have a limited level of reliability. A large number of extensions have been created for SMTP and HTTP in particular. These extensions are defined in additional standards. Not all extensions have been tweaked to fit together properly, and various software providers make different choices regarding the extensions they want to support.
- The application sub-layer arose due to the fact that not all communication sub-layer protocols work in the same way. Such differences are undesirable for applications that operate in a heterogeneous environment, since extra functionality must be implemented for the different protocols. The widespread use of EDI (electronic data interchange) before the emergence of web services led to the use of 'EDI over the Internet' (a.k.a. EDIINT), also known as the ASx family. These protocols standardise the way that EDI applications handle security and reliability for various communication protocols—SMTP (AS1), HTTP (AS2), FTP (AS3)—and web services (AS4, based on ebMS).

From a functional perspective, all application-oriented protocols fulfil the need for reliable and safe transport of content-based messages. The way this is done also differs between protocols. As technological preferences can be very different depending on the organisation and sector, choosing a single standard is not feasible. Part of the *raison d'être* for a generic process infrastructure is therefore its

ability to translate between protocols, thus bridging the gaps between organisations and sectors in how different protocols and standards are used.

SOAP

Let us move ahead on the protocol applied in the generic infrastructure for a moment: all three interfaces being used for S2S integration via the generic infrastructure use the SOAP protocol (see http://www.w3.org/TR/soap/). These interfaces—SOAP2008, WUS and ebMS Digilink—will be described below.

In its original version issued in April 2000, SOAP was an acronym for Simple Object Access Protocol. However, because of the broadened application of SOAP as part of the XML and Web Services stacks, that meaning no longer applies. Since the completion of the SOAP 1.2 specification, the World Wide Web Consortium (W3C) has used the acronym without writing it out in full.

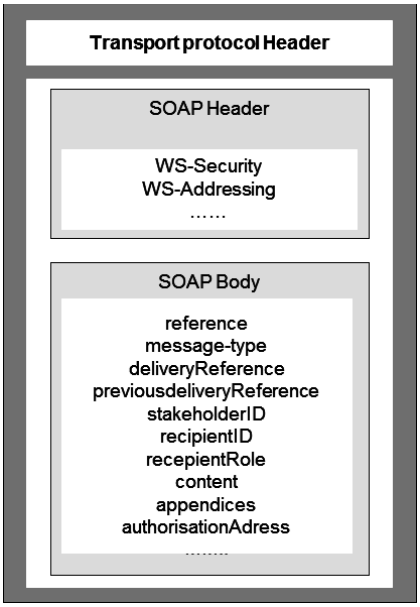


Figure 7.9 – The structure of a SOAP message

As illustrated in Figure 7.9, a SOAP message consists of the following:

- The transport protocol header
- The SOAP envelope, which contains:
  - The SOAP header
  - The SOAP body

The need for SOAP arose from the limitations of other protocols. The data transfer capability of HTTP and the Internet mail protocol (SMTP) was limited to a single block of 7-bit ASCII text. After a while, there was a need to transfer more and other types of data through Internet mail (Stallings, 2009). SOAP fulfils this

need by using the different approach of functioning as an envelope (Weerawarana et al., 2005). SOAP supplies the envelope to allow electronic messages exchanged by web services to be sent over the Internet. Figure 7.9 above provides a simplified representation of the elements of a SOAP message, including the SOAP envelope.

For the actual transport of messages, SOAP generally uses HTTP. However, other protocols such as the Simple Mail Transfer Protocol (SMTP) can also be used. The SOAP envelope contains the header and the body. As will be seen in the chapter on security (Chapter 8), this distinction is important in several ways. In view of security, businesses[16] must add a digital signature to the body and header elements of a delivery request to the generic infrastructure. This message must include an electronic signature and a PKIgov certificate issued by a certificate service provider (CSP). A certificate is a digital document containing data that guarantees the integrity and authenticity of files, and/or which can be used to set up a secure connection. These security measures will be discussed further in Chapter 8.

SOAP headers provide information about data encryption, authentication or how the receiver must process the SOAP message. A SOAP header can also be used to pass on information about control and checks between the service user and the service provider; this includes information relating to items such as asynchronous communication, transactions, routing and security, and for implementation of other quality-of-service attributes. Ensuring reliable, complete and safe transport of the actual message content requires additional agreements, including WS addressing and WS security – concepts that will be explained later in the chapter.

The SOAP body contains in a number of elements, as shown in Figure 7.9. The reference element, for example, is a unique reference to an instance in the I-process that can be used when requesting a status. The 'message type' element describes the type of I-process that is initiated with the message delivery process. All of the elements can be defined using the WSDL specification.

Two important protocol families have been created based on SOAP: web services (as in SOAP via HTTP) and ebMS (e-business XML Message Service). As these are also used for the generic infrastructure, they will be briefly explained below.

7.5.3 *Web services*

In the context of information exchange, it is important to distinguish between web services (plural) and a web service (singular). The term 'web services' refers to a set of standards (a protocol stack) for information exchange (see Figure 7.10).

[16] The signature does not have to be that of the message owner (the business). The party responsible for the technical implementation (which can be an intermediary) usually signs the message.

The term 'web service,' on the other hand, refers to a specific functionality for the transformation of input information into output information, which can be invoked by using the standards. From this point forward, the term 'services' will be used when referring to more than one web service, to avoid confusion.

Through the use of standards a Service Oriented Architecture can be realized for supporting message exchange between several different systems. For an example, refer to the definition of web service given by the World Wide Web Consortium (W3C):

> *"A web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other web-related standards" (W3C, 2004).*

A web service not only ensures system-to-system transfer of information, but can also immediately activate an application and receive its result as a return message. This chapter therefore distinguishes between the transfer of information and the immediate activation of an application. A web service consists of the following elements (Erl, 2008): the application logic, the message processing logic and the service contract. These elements are illustrated in Figure 7.10 below.

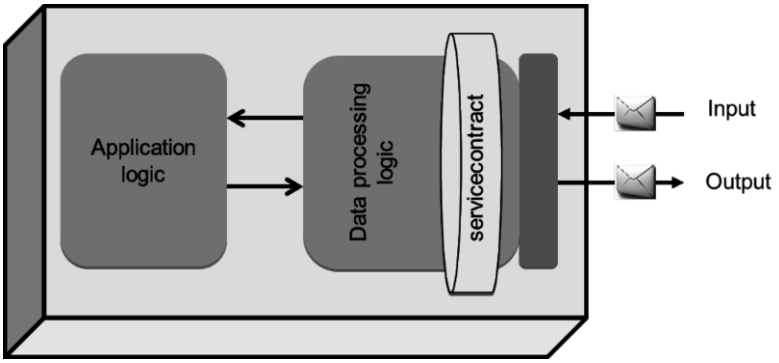


Figure 7.10 – Elements of a web service (based on Erl, 2008)

To briefly describe the three elements of a web service, we start with the application logic, a functionality block that processes input (data) into output. To carry out this process, the input must be provided to the application logic in a suitable way. This is where the message processing logic comes in. The final element is the service contract, which describes what the service does (its operations). The service contract is independent of the other elements and consists of a WDSL definition and an XML schema definition. It can therefore be compared

to a traditional application-programming interface (API). From a technical perspective, the service contract is the interface's basis, which may or may not be supplemented by other specifications. Based on the above information, it can be concluded that a web service is more than just a piece of functionality. The use of services for information exchange therefore requires more standards than SOAP and XML alone. The protocol stack depicted in Figure 7.11 shows the standards used for exchanging information with services.

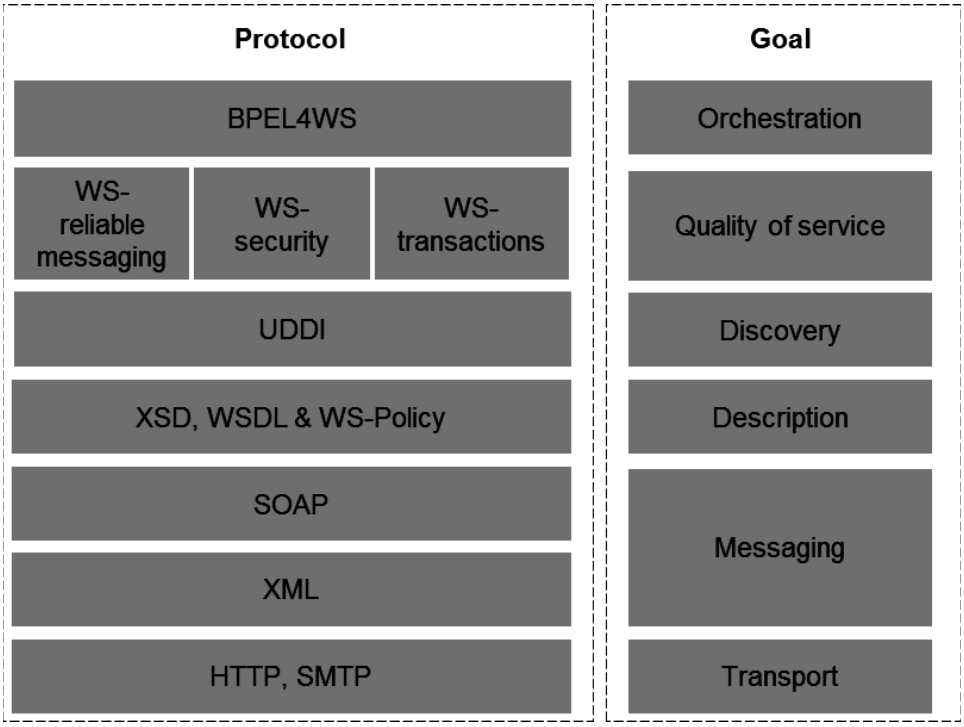


Figure 7.11 – Web services protocol stack (Juric, Mathew and Sarang, 2006)

Figure 7.11 makes clear our assertion that using services requires more than just SOAP and XML. We do not aim to provide an extensive description of the entire stack – plenty of articles and books can be found on the subject (e.g., Curbera et al., 2002; Erl, 2008; Newcomer and Lomow, 2005; Weerawarana et al., 2005). We will, however, give a brief explanation of the functions of the main open standards used for the generic process infrastructure:

- HTTP is used for addressing and communication between a web client (usually a web browser) and a web server.
- XML is used for encrypting/drawing up the content of a message.
- SOAP is used for writing messages.
- WSDL is used for defining service interfaces.
- UDDI is a library (telephone book) for finding services.

- WS stands for several different standards, which will require some more explanation. These include standards for addressing (WS addressing), security (WS security), reliability (WS reliable messaging), etc. The users of the standards must decide for themselves which aspects are important for their services. Having several WS standards has benefits, such as greater flexibility and faster implementation, but also disadvantages, such as a complex message structure and less interoperability. One example of this disadvantage is the choice of a security architecture. In point-to-point situations, the confidentiality and integrity of the data are usually enforced using the Secure Socket Layer (SSL), or its successor, Transport Layer Security (TLS). This is done, for example, by sending messages using HTTPS. TLS operates at the transport level while WS security operates at the message level. WS security solves the broader problem of enforcing the integrity and confidentiality of the messages independent of the transport protocol. It therefore also functions when the message is transported using different transport protocols and intermediate stations (end-to-end security). Services of this type can be implemented easily, but have a relatively large overhead. The use of TLS, however, reduces the overhead of SOAP messages because encryption keys and signatures are not required in XML when sending messages. TLS is not a signing protocol, while XML Signature is. Encryption at the transport level also requires measures other than encryption at the message level. In Chapter 8, focus will be placed on the choices made for the security issue.
- BPEL4WS is a language that describes sequences and conditions for invoking individual or combined services. The situation in which a bundled set of services is called by a web service is also known as a composite service. BPEL4WS makes it possible to combine generic infrastructure applications and I-processes using services from heterogeneous environments, without taking into account the details of, or differences between, those environments. We will return later to the significance of this standard for flexible calling and orchestration of services.

As illustrated (figure 7.13), the XML document is the lynchpin of the web service because it contains all the application-specific data that a service user is sending to the service provider for processing. The documents that a web service can process are described in an XML schema. The two I-processes taking part in a web service conversation must have access to the same description to ensure that the documents they are exchanging can be validated and interpreted by both. This information is usually described using WDSL. Using the standards listed above ensures that the services function independently of suppliers, programming languages or operating systems.

ebMS

As mentioned earlier, two important protocol families have been created based on SOAP, namely web services and ebMS (e-business XML Message Service). We

shall briefly consider ebMS here, as this family is relevant for the Digilink interface that will be described later in this chapter. As with web services, ebMS is based on open standards, with the same clear combinations of XML and Internet-related standards, including SOAP (Turner, 2003). This protocol family has a more limited field of application than web services, however, and is aimed at situations in which security and reliability have traditionally played a major role. The ebMS standard already regulates those aspects by means of a Collaboration Protocol Agreement (CPA), a contract that describes the configuration of the connection.

There are two endpoints in ebMS and each system 'knows' the location of the other. Aspects such as security, reliability and addressing are already set out in the CPA. This creates a situation that makes implementation of ebMS more complicated, but in which communication is much easier and requires less overhead once implemented. For ebMS, the simpler and smaller messages, in particular, increase the efficiency of sending large quantities of data and conducting very frequent information exchange. Figure 7.12 below provides a simplified representation of the elements of an ebMS message, including the SOAP envelope.

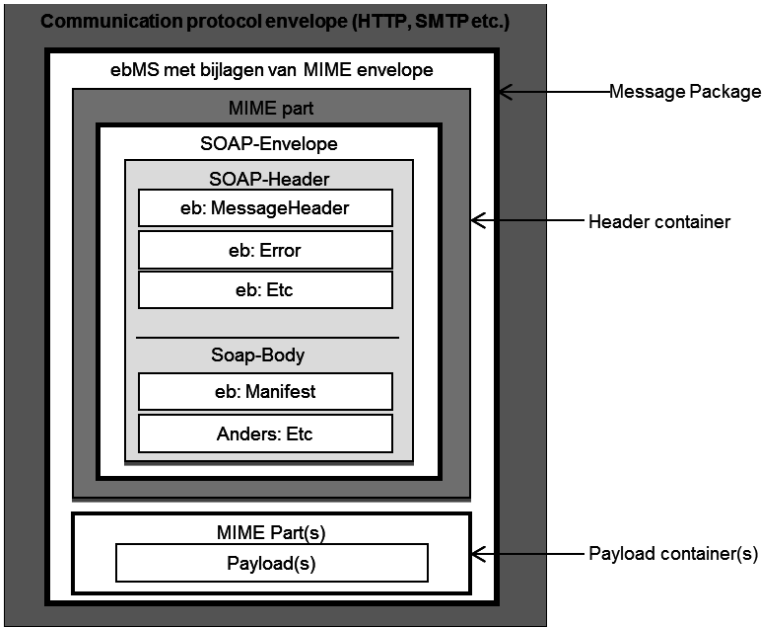


Figure 7.12 – Structure of an ebMS message

SOAP version 1.1 cannot be used as an envelope when multiple types of message content are involved. However, multiple types of payload sometimes need to be placed into a single SOAP envelope, for instance, if they belong together. An example of this could be a message and its associated digital signature. To realise this, various MIME elements are included hierarchically in the body of the (ebMS) SOAP message.

MIME (multipurpose internet mail extension) provides the possibility to indicate in the message itself what type of data it contains (the 'MIME type') and to subdivide the message into multiple parts ('multiparts'). Each part may have a MIME type of its own, this again can be the multipart type. The special thing about MIME is that it can be used to define hierarchical structures, in principle making it possible to include all kinds of mixed content within a single message (although this does have technical limits). For example, MIME allows the actual message in textual format to be combined with control information, a binary attachment and a digital signature each in its own MIME part, separated by boundaries.

7.5.4 *SOA for supporting flexible I-processes*

Service-oriented architecture (SOA) goes beyond SOAP, web services, BPEL and the other technical possibilities described previously. Interfaces and web services in themselves are not sufficient to realise unambiguous information exchange. An overall 'umbrella' vision for the interfaces, links and the processing is also needed: when is which service required, and where can that service be found? SOA is a strategic direction within the evolution of IT in general.

SOA is not in itself a revolutionary idea—the basic concept existed in the mid-'80s. However, the increase in electronic messaging within chains and the need for flexibility and reuse have generate renewed and more prominent attention on this concept in the business and IT sectors. This is because SOA emphasises the collaboration of services, independent of the implementations of certain configurations and platforms. In addition, SOA plays a role in addressing the need for applications to work together (enterprise application integration) and the need for automation of the interactions between organisations (Linthicum, 2003). The most distinctive feature of SOA is that it forces organisations to think about reuse of functionality, the service interfaces, the granularity of services and the contractually determined quality of services. The assumption in designing the architecture is that services will be used in more than one I-process, thus placing a heavy emphasis on the design of electronic messaging and, at the same time, the design and implementation of the generic infrastructure the services are run on. SOA also forces parties to use standards within a chain.

The basis of the architectural style of SOA is a three-way split between service users, providers and a service directory, as illustrated in Figure 7.13. The idea presented in this SOA template is that every time users want something, they first browse the 'Yellow Pages' (the service directory, UDDI). After that, they select the most suitable provider or combination of providers. A process is then initiated in which the providers are actually contacted (via web services technology: SOAP/XML).

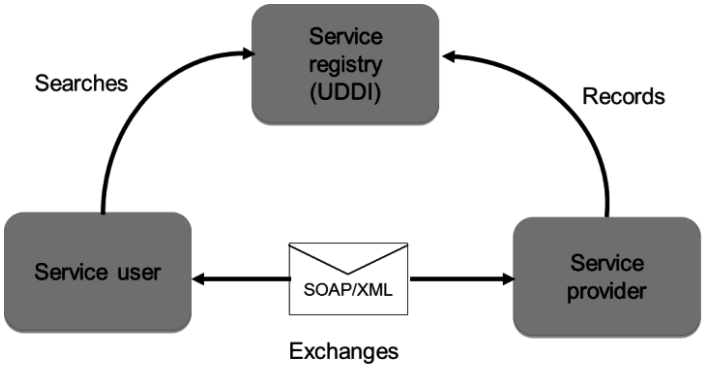


Figure 7.13 - The original idea behind service-oriented architecture (Curbera et al., 2002)

The caption of Figure 7.13 deliberately refers to the 'original idea behind' SOA. There are three reasons why we refer to this as the original idea and not the practice as it has been implemented:

1. In practice, outgoing calls are rarely made to contact UDDI services, for information security reasons.
2. SOA has many alternative templates, including one with a service bus for linking services. We will describe this alternative layout later in this chapter.
3. SOA includes a party that 'hosts' the services and a party that calls the services. However, this does not say anything about the directionality of the information. Nowadays, it is normal for hosting to be done by a basic registry. The requesting party can consult a basic registry (service) in an *ad hoc* manner, but it can also receive event-driven information (on its own service) from the basic registry.

Despite these differences between practice and the model, it is important to explain the foundations of SOA according to its original idea. The model distinguishes between three roles, namely those of the service user, the service provider and the service registry. These roles are described as follows.

The service provider provides a service that handles part of the automated process. The service makes it possible for the service provider to respond to external requests in the form of messages. The party that sends these messages, the service user, requires something to be done by the receiving party. The service itself performs that task. The provider of a service lists the service in a service registry. This registry (also known as UDDI – Universal Description, Discovery and Integration) can be compared to a phone book (Curbera et al., 2002), where users can find and call the services remotely (via 'outgoing calls'). The way that services can be used is described in a service contract (see Figure 7.10) and this description is also presented in the service registry. A service therefore describes the data that is delivered or processed and the conditions under which this data is

delivered or processed. The data is actually exchanged via the technical implementation the service. The web service technology discussed above is often used for this: the web service uses an underlying web service protocol (Figure 7.11) for electronic messaging and service users can find the services in a service directory. Software systems are seen as service providers for other software systems, which are the service requesting parties.

Finally, it is important to consider the types of services. McGovern et al. (2006) state that services can be classified in various ways. One well-known classification based on functionality divides services into presentation services, process services, business services, application services and data services. Each type of service requires a different identification method. In this chapter, we will discuss the business and application services in particular. These two types of services can be categorised further into the following actions performed: query, select, record, modify, remove, terminate, transform, generate, validate and calculate values.

Granularity

We will now look at a complex issue in SOA, namely what level of granularity of services is needed in order to realise the objectives of information exchange. The granularity of a service refers to the scope of the functionality provided.

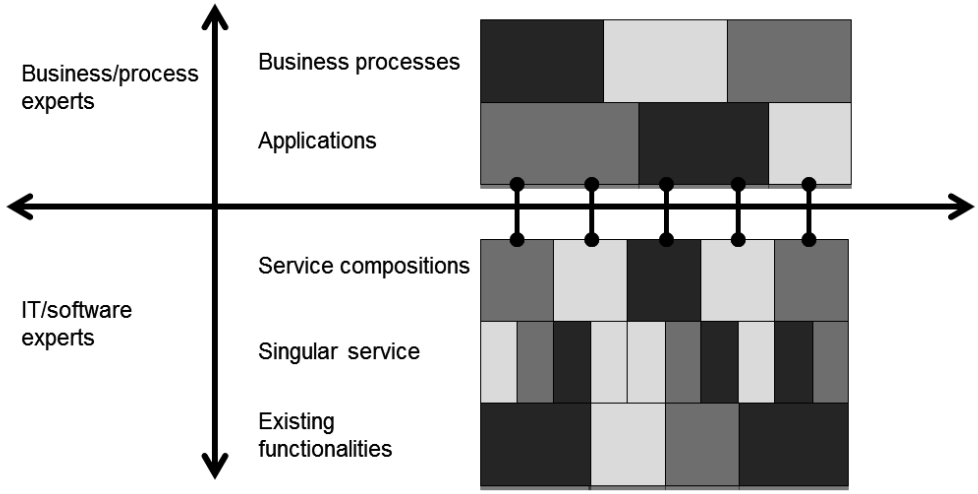


Figure 7.14 – The granularity issue

Ever since SOA and web services have become popular, there have been discussions about the best way to identify services. For example, when is a service 'too large' or 'too small'? When is it 'too specific' or 'just right'? We will examine a few of the insights from the relevant literature (Feenstra, 2011). In this context, a distinction is often made between 'fine-grained' and 'coarse-grained' services, i.e. those with single or combined functionality (Arsanjani, 2002). Fine-grained

services offer a limited amount of useful business process functionality, such as basic data access. Coarse-grained services, on the other hand, are made up of fine-grained services that are combined intelligently to meet specific business needs. Such is the purpose of combined services (also known as composites). Figure 7.14 should help clarify the distinction.

Carter (2007) states that many SOA projects fail because their granularity has been determined incorrectly. This occurs because business/process experts often think in terms of combined functionalities, whereas IT experts think in terms of singular functionalities. In order to bridge the gap between these two worlds, Carter recommends adopting the coarsest granularity possible for services, preferably at the application or application module level. The coarser the granularity, the less dependent and more self-supporting the service can be (Papazoglou and Georgakopoulos, 2003), meaning that the service can handle a complete internal transaction (such as a new order) without depending on other services. Of course, the situation is more complicated in practice: if the level of granularity is too coarse, it could be an obstacle to reuse, since only some elements could be reused and not entire applications (Feenstra, 2011). Determining the appropriate level of granularity in specific situations is very much a task for the architects. Finally, the definition of a properly specified service is depends on the angle you approach it from. For example, a manager may impose different requirements than a process designer or a tester.

7.5.4.1 Enterprise Service Bus

One important SOA template is the Service Bus—also known in ICT jargon as an Enterprise Service Bus (ESB)—which is a specific substantiation of an SOA, as illustrated in Figure 7.15. As an integration technique, ESB ensures that services can be called from anywhere, irrespective of platform or programming language. It is important to realise that an ESB is not a software product in the generic sense, but is more of an architectural style or template. This means that there are many types of ESB, each differing in the possible features provided (Chappell, 2004). However, all ESBs have an 'abstraction layer' that is responsible for the message management, ensuring that the software components fit together consistently and efficiently and can send messages to one other. The ESB ensures the communication between services so that they can carry out a fixed, defined I-process.

Carter (2007) describes the following key functions of an ESB:

- Routing messages between services
- Converting transport protocols between the calls and the services (an interface function)
- Transforming message formats between the call and the service
- Monitoring the agreed-upon service quality (security, reliability and transacted interactions).

In addition to the functions mentioned above, use of an ESB also reduces complexity, as large numbers of bilateral actions are replaced by a fewer number of

multilateral actions, which are easier to maintain. From a generic process infrastructure perspective, this encourages the option of using or reusing the desired services, both inside and outside the organisation. The desired services can be selected from a larger pool, for instance, if no specific programming language is required. New services can be more quickly included in the generic process infrastructure due to reuse or because of fewer requirements being imposed on compatibility. Therefore, users' requirements can be met more easily.

The ESB also adds value by linking various loosely coupled services. An ESB can be used in multiple applications of multiple types, from specific to highly generic. A specific situation arises when the services jointly provide a single functionality to an application (when made up of one composite). Here, the advantages of decoupled services—in terms of maintenance and reduction in complexity—are combined with rigid process execution. The situation outlined here, however, only offers benefits for sizeable and complex systems that have one specific task. An ESB can also be used in combination with a process engine that determines the sequence of services to be invoked (when made up of multiple composites). This allows the process engine to execute different I-processes, whether they use the same services or not. The following section will discuss this situation in detail.

7.5.4.2 Orchestration by the process engine (BPEL4WS)

Although the ESB has an essential function as an interface between services, more must be done to automate the calling of various different functionalities to process a message. For this purpose, the concept of a process engine was developed, which calls web service functionalities in a certain sequence. This task is called process orchestration, and is not the same as the chain orchestration concept, which we will return to in the later chapters. Here, the term 'orchestration' is used to indicate that the process engine has the same role for the individual web services as a conductor does for the orchestra musicians (Janssen and Gortmaker, 2005). During the concert, the conductor (the process engine) indicates what the various orchestra members (the web services) need to do. The process engine thus has a controlling role because it determines the process flow. The ESB makes sure that one generic process can activate a variety of services that may have been drawn up in different programming languages, and which may be inside or outside the organisation. An ESB thus makes orchestration much simpler. Figure 7.15 below summarises the role of ESB in orchestration.

The striking aspect of the setup in Figure 7.15 is the process-specification representing the control of the process flow. The automated information processes in the process engine are derived directly from the business processes defined in BPMN (see Chapter 6) and implemented as an executable I-process. When information is supplied to the ESB along with the associated information-processing request (which must be handled using an interface, portal or an independent application), the process engine determines which I-process should be executed. After that, all services that are part of the I-process will be performed automatically, step by step.

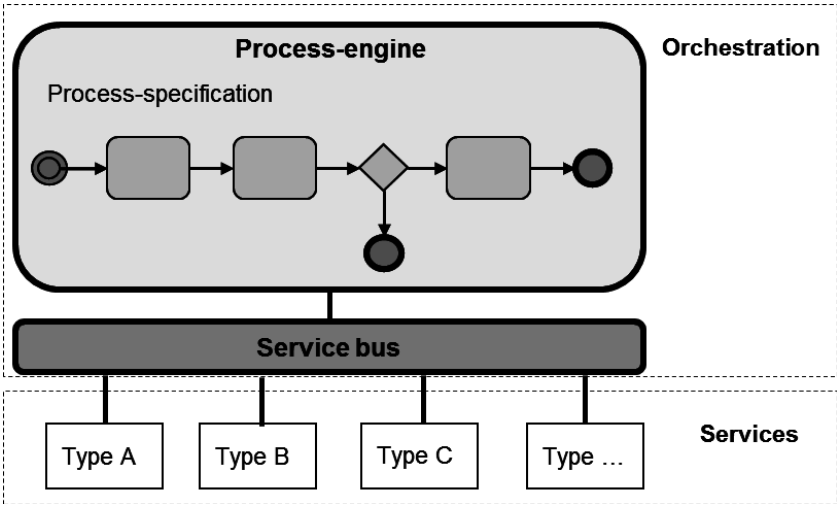


Figure 7.15 – Relationship between ESB and orchestration

Figure 7.15 also says something about the role of an ESB. An ESB can support multiple types of services and their associated protocols. This is illustrated in the figure by the various boxes representing the services. If web services are supported, for example, this means that SOAP and WSDL will be instantiated. Most ESBs provide broad support for communication styles, including publish-subscribe and guaranteed delivery. As described in §7.5, such functionality is an important condition when exchanging various types of messages.

BPEL4WS

Now that the relationship between the ESB and the process engine has been described, we can turn our attention to the standards for orchestration. The *de facto* standard for orchestration is BPEL4WS, which stands for Business Process Execution Language (BPEL) for Web Services (https://www.oasis-open.org/committees/wsbpel/). This language assumes the presence of a central component known as a process engine, which controls and calls all web services (Khalaf, Keller and Leymann, 2006). This creates a hub-and-spoke model, with the process engine at the centre. This function is different from choreography, which is more peer-to-peer in nature (Kloppmann, Koenig, Leymann, Pfau and Roller, 2004).

BPEL was developed for orchestration that involved invoking web services in a certain sequence. BPEL is used here for defining executables, or processes that can be run. An executable is a white-box model of a process that can be executed by a BPEL server. Executables are designed to call web services: it is also possible to offer the executable process as a web service.

In addition to the above functionality, Version 2.0 of BPEL4WS will also contain process logic, which has traditionally only been found in workflow languages. This version will also provide the option of having tasks performed by people.

Orchestration of individual services in the required sequence ensures optimum support of I-processes, using functionality and data from all internal systems as well as from partner systems (Janssen, Gortmaker and Wagenaar, 2006). The available services can be called in the required sequence with the required parameters for each message exchanged. The idea behind SOA—that the services can be reused—can be realised in this way. This means that orchestration contributes to the generic character of a generic infrastructure.

The orchestration requires a number of choices that must first be made to determine the characteristics of the generic infrastructure. The process steps (the sequence of services to be called) can be defined in full beforehand. Another possibility is to define the subsequent service based on the latest known process characteristics. In both cases, individual services that are called can be present on site—within the organisation's system—or outside it, managed by third parties. When third-party services are involved, there is a choice between using only known, screened services or calling a public catalogue of services that the third parties themselves offer.

The use of BPEL provides two main advantages (Gortmaker, Janssen and Wagenaar, 2004). Firstly, orchestration is required to obtain a full process description and to run the I-processes with due care. A process engine is used for automated handling of I-processes that are part of a workflow and that require other applications and services. To realise this automated handling, the process engine uses the ESB integration and mediation functionalities. Secondly, the execution of I-processes can be decoupled from the machine that finally executes the subprocesses. This improves the manageability of these processes, in addition to making them easier to reuse. Web services are, after all, replaceable. An example of this replaceability was included in Chapter 6 (I-processes). Finally, orchestration should be seen as more than just a technical layer. Just as web services should be designed for reuse, processes must be reusable too, and it should be made clear who is responsible for their execution. Chapter 9 discusses the division of responsibility in detail.

7.6 Architecture and components of the generic infrastructure

This third part of the chapter discusses how the technology described above has been used to create the generic infrastructure in SBR. The generic infrastructure has resulted from the interaction between the need for a generic process infrastructure and the technological options for creating it. Chapter 1 provided a brief description of the SBR building blocks. The generic infrastructure comprises the two components called 'Interface Services' and 'Processing Services,' which oper-

ate in accordance with the technical standards. However, a more in-depth description is required to truly take the lid off this black box and reveal its inner workings. For one, the name of the generic infrastructure—'Digipoort'—requires additional explanation. On one hand, there is Digipoort PI, which is the process infrastructure, and on the other is Digipoort OTP, also known as the Government Transaction Gateway. As this division may cause some confusion, it is important to state clearly what the name 'generic infrastructure' refers to in this chapter.

The two process infrastructures are technically separate electronic infrastructures that are maintained by Logius, but there are few similarities between them in terms of setup, other than the naming. Digipoort OTP originated from the OTP programme and its predecessors. It is used for communication with the Customs service via the outdated X.400 protocol, but also uses SMTP (MSA/MTA), POP3 and FTP. Digipoort PI originated from the GEIN programme of requirements, as stated in section 7.4. The I-processes in the SBR Programme are only run via Digipoort PI and information flows other than reporting processes can also be connected to the PI. When the term generic infrastructure is used in this section, it is only referring to the part of the Digipoort PI that the business reporting processes are run on. Consequently, Digipoort OTP will not be part of the further discussion.

Yet, despite this limited scope, it would be impossible to provide an in-depth discussion of all the relevant aspects of the generic infrastructure in a single chapter. The documentation that has been produced on the topic over recent years could fill a bookcase, as with other public-sector projects that have been implemented on a similar scale. Choices have therefore been made about what will be discussed here. The guiding principle is, again, the goal of providing relevant technical insights to users. Our advantage now is that both the requirements for the generic infrastructure and its underlying technology (web services, SOAP, BPEL4WS) have been described in previous sections. For non-technical matters such as management and organisational issues, please refer to Chapters 2, 3, 4 and 9.

Our focus here will be the following aspects of the generic infrastructure:

- What agreements have been made regarding interfaces?
- What does the generic infrastructure do?
- How was the requisite flexibility in the I-processes created?
- Which I-processes are orchestrated?
- What services are ultimately provided to the requesting parties?
- What are the implications for the users?

These questions guide the organization of this section.

7.6.1 *What agreements have been made about interfaces?*

The loose coupling required in the chain, the accessibility of the generic infrastructure and the decoupling of interfaces from the data layer are all realised

using generic interfaces. These interfaces are either for the reporting parties or for the requesting parties. This distinction results in three types of interfaces:

1. SOAP2008
2. WUS (acronym for WSDL, UDDI and SOAP) for Businesses
3. ebMS Digilink

Earlier, we gave a simple definition of an interface—a system-to-system connection between information systems that facilitates information exchange. This is a technology-oriented definition but requires more than just standards. This is suggested by the fact that interoperability can mostly be found at the organisational level. The interface specifications are a set of agreements for data exchange with the generic infrastructure that have the following components:

- The technical standards, or the specification of the various open standards used for connections, data exchange and security. The technical standards comprise the physical layer, communication sub-layer and the application layer. These layers have were discussed in §7.5. Connections are created in the physical layer. Common Internet standards such as TCP/IP and HTTP can be found here. The data exchange comprises the messages actually exchanged in the communication sub-layer. The SOAP message standard was discussed earlier. Security plays a role in various layers, from the physical layer (TLS) and the communication sub-layer (encryption of exchanged messages) to the message content (digital signatures). We will return to the security aspects in Chapter 8.
- The application / configuration. An interface specification is more than just a specification of the technical standard(s) used. The specifications also comprise agreements about how strict the technical standards are applied. There are agreements regarding mandatory and prohibited fields in the SOAP message. Requirements are also imposed on the certificates used and on the maximum size of the message. These agreements ensure that use of the chosen technical standards is consistent with the specific requirements of the I-processes for security, authentication, non-repudiation and processing capacity.
- The end-points. A simple but essential element of an interface is the address that the generic infrastructure can be reached at via the interface in question. This is called an end-point. The end-point is a URL, as we know them from websites. The only difference is that the address does not reach a server that displays a website in a browser. Instead, the end-point interacts with the message submission service of the generic infrastructure.
- The payload (message content). Using generic interfaces allows the information to be exchanged independent of the modality. A SOAP message is seen as an envelope for business reports, status reports or information that is exchanged via the interfaces. The payload of a SOAP standard may be a MIME object. MIME is a recognizable term from e-mail attachments. Various files, such as PDFs, holiday photos, XML messages, program code, an XBRL instance, etc., can be attached.

Please note that currently, the generic infrastructure only accepts XBRL instances as the payload.

Choosing open standards

The three types of interfaces—SOAP2008, WUS, and ebMS Digilink—are kept as generic as possible through the use of open standards. Within the SBR Programme, the choice to use open standards was based on the following considerations:

- Open standards are often embraced by a large number of parties, and the more they are used, the greater the interoperability becomes.
- The market already knows a great deal about a large number of open standards. Acceptance of open standards is thus gained more easily reduced costs for market parties and authorities. In addition, there is no dependence on the limited expertise at Logius or on some niche in the market. Many of the open standards chosen have already been set up—either entirely or in part—for other purposes.
- Generally, implementation of the more common open standards is relatively simple. Modules exist for a number of new and legacy systems, software packages and programming languages. Connecting up with a heterogeneous outside world is therefore simpler.
- The authorities cannot really force businesses to purchase products from a single private party. This is undesirable from society's point of view. An artificial monopoly position could be created if a closed (proprietary) standard was chosen. Potential consequences include vendor lock-in, unfair competition and price increases. This is more likely happen if there are no alternative channels because the existing one has been made mandatory.
- Open standards are changed in consultation with many parties. The consequences of changes are generally carefully considered so that parties will not be at the mercy of a specific supplier.

The three interface types are well documented and information is freely available. We will provide a brief description of the interfaces as follows.

The three types of interfaces in use

As described earlier, the generic infrastructure has three types of interfaces: SOAP2008, WUS for Businesses and ebMS Digilink. These interfaces were designed by Logius based on open standards. They are also used outside the SBR domain. A number of additional requirements are imposed on these interfaces for use within the SBR domain, due to the specific context of business reporting. The additional requirements are part of the configuration of the interface specifications. The similarities and differences between the three types are examined below. Each of the three interface specifications is based on the SOAP protocol. The additional requirements and specifications defining how the SOAP protocol is used then result in interface characteristics that differ greatly between interfaces. While newer versions of the three types of interfaces have been issued, the broad outlines of the interface specifications do not change. At the same time,

some details can be modified to ensure that the latest requirements regarding the I-processes of a specific SBR chain are met, for instance, by providing additional functionality or supporting a slightly different authentication model. In this case, different versions may remain available for some months so that all users have plenty of time to switch to the new version.

The SOAP2008 and WUS for Businesses interfaces were derived from the standard web service specifications. Both are based on the SOAP protocol and require a number of additional WS specifications, including WS security. SOAP2008 provides immediate feedback about the entire process after items are sent in, whereas WUS for Businesses only provides immediate feedback about the initial step (sending items into the generic infrastructure). On the other hand, WUS is more reliable during peak loads in particular.

SOAP2008 and WUS for Businesses focus on the 'front end' of the generic infrastructure: the reporting parties. The overhead for these interfaces is greater than for ebMS Digilink because of the numerous WS extension protocols, but they are much easier to implement and use. These protocols also have a single end-point, at the generic infrastructure. All these characteristics make SOAP2008 and WUS for Businesses particularly suitable for integrating a large group of heterogeneous users. They can be seen as analogous to a network of small roads that provide access to a residential area: many connections without much traffic.

The ebMS Digilink interface is derived from the ebMS standard and is a much more complex interface than SOAP2008 or WUS for Businesses. Implementation and day-to-day use require more expertise and effort. On the other hand, it has a number of advantages that come particularly to the fore when message numbers are higher. The overhead for each message is lower and 'reliable messaging'—referring to a number of security features for two-way messaging—is already included. Sticking with the road network analogy, ebMS Digilink can be seen as a motorway: more awkward to construct than a small road, but with a much higher capacity and higher efficiency. That is why ebMS Digilink is particularly useful at the 'back end' of the generic infrastructure.

The ebMS protocol uses two end-points, one at each side of the connection. In this case, the generic infrastructure and the other party must both be known by both endpoints beforehand. This, however, would be impractical at the 'front end,' where authentication using PKI government certificates is more appropriate. Having two end-points makes it possible for either party to initiate messaging and the generic infrastructure can deliver validated messages and status information whenever it wants. Status updates and notifications can be sent to and from the generic infrastructure.

Although we have described the interfaces used to access the process infrastructure, we have not yet explained exactly what the generic infrastructure— the process infrastructure—does. The following section discusses how the process infrastructure works.

7.6.2 *What does the generic infrastructure do?*

Up until this point, the generic infrastructure has been presented as a black box. We are now going to take the lid off the black box to explain what functionalities it needs to fulfil, or in other words, the services that the generic infrastructure must provide. The answer to that question depends on the chain that is being connected. The nature of the message to be exchanged and the business processes to be supported determines the requirements for the generic process infrastructure, which can include a considerable number of factors, such as security level and the need for archiving. We will start with a simple example, followed by a thorough analysis.

To put it simply, the function of the generic infrastructure comprises three steps:

1. A reporting party submits an envelope with address details (in the form of an electronic message) to the generic infrastructure, with the option of attaching documents.
2. The generic infrastructure takes the documents from the message, performs any validation required and checks to see which requesting party they are intended for.
3. The generic infrastructure forwards the message with the appropriate documents to the appropriate requesting party.

Table 7.2 summarises the functionalities provided by the generic infrastructure.

Table 7.2 – Required functionalities for information exchange and processing

Requirements for information exchange	**Communication sub-layer**	**Application layer and data layer**	**Process layer and user layer**
Non-repudiation	Transport confirmation, reliable messaging	Acknowledgement of receipt, logging	Audit trail
Confidentiality	Channel encryption	Message encryption	Authorisations
Integrity	Boundary protection	Message signature	Electronic signature
Reliability	Buffering	Backup/reinjection	Archiving
Correctness	Interface conformity check	Schema validation, semantic validation	Business rule validation
Identification	Resource identification	Message identification	Partner identification
Logistics	Network addressing and routing	Logical addressing and routing	Orchestration
Information processing	Stacking, unstacking	Merging, splitting	Extraction, enrichment
Translation	Channel conversion	Message conversion	Transformation

The table above lists a wide range of functionalities for information exchange. Not all functionalities are required for every I-process. For example, certain messages may not require enrichment or splitting up. Each envelope sent is checked to establish whether the sender is known and authorised to send data to the recipient. Authentication and authorisation are therefore key aspects of the generic infrastructure. Chapter 8 will explain these subjects in more detail.

7.6.3 *How was the requisite flexibility in the I-processes created?*

The required flexibility in the I-processes carried out by the generic infrastructure was created using an SOA. In §7.5.4, we argued that three aspects of SOA are crucial in achieving such flexibility: the services, the service bus and the process engine. The main elements of the SOA architecture style can be found in the design of the generic infrastructure. The application landscape consists of web services, the service bus is the connecting element between the services, and a process engine orchestrates the various I-processes. BPMN I-processes and the Netherlands Taxonomy are the bases for orchestrating the services. Orchestration involves making decisions, based on information received, about which I-process is to be followed, along with centralised execution of the generic parts of this I-process. The central component of the generic infrastructure – the process engine – is supplemented by services for validation, checking authorisation and storing status updates. These are called processing services, and they monitor the technical processing of the information supplied.

As stated earlier, the generic infrastructure uses various interfaces to communicate with the reporting and requesting parties. Interface services are responsible for sending in and passing on messages. The processes used on the business end (for instance, drawing up a business report) or by the requesting party (for example, analysing business reports) are not part of the generic infrastructure's I-processes. These I-processes will be explained below, followed by a description of the interface services and processing services that are used to execute the process.

7.6.4 *Which I-processes are carried out?*

Process orchestration was discussed earlier in the chapter. Process orchestration is jargon for automated calling of services in a specific sequence in order to carry out I-processes. The I-processes, which have been defined using a process standard, must be checked by a process engine. The process engine and the interface services ensure that the I-processes are always carried out appropriately and that the relevant parties are kept informed of the status of the ongoing I-processes. Executing I-processes involves a controlled series of specified process steps carried out in a defined sequence. The sequence and conditions are directly derived from the BPMN process diagrams and implemented as executable I-processes. When information, along with an associated information processing request, is sent to the process engine by an interface service (via a portal or an independent application), the process engine uses the process diagram to determine which processing services need to be invoked. Then, all services associated

with the processing of that information are invoked automatically, in sequence. Services may focus on various forms of information processing, which could include, for example, an analysis that generates a report, or information security checks resulting in an output of 'authorised' or 'unauthorised.' An I-process often has multiple possible results, depending on the information fed in. A summary of typical I-process types is provided below. The list, however, is not exhaustive. Depending on the information chain, fewer or alternate processes may be involved.

- Setting up a secure connection
- Submitting messages
- Forwarding messages
- Re-delivery
- Recording the audit trail
- Requesting status
- Authentication
- Checking authorisation
- Backup
- Archiving
- Report generation
- Validation
- Conversion
- Extraction and filtering

Next, each of these I-processes is briefly described.

Setting up a secure connection
The purpose of a secure connection is to protect the client/server applications against eavesdropping. Setting up the security must be possible from either the client or the server roles. The protocol currently used for doing so is TLS (duplex). The reporting party (the self-filer or intermediary) must have a valid certificate from a certificate authority (CA) that is recognised and trusted by the government and that meets the requirements imposed by PKI-government or similar. This certificate and the certificate of the information submission service are used to encrypt the connection. If a secured connection cannot be set up, the process will end.

Submitting/filing messages
A service for sending in messages to the generic infrastructure ensures that they are accepted, checked, backed up and registered, and that the reporting party receives feedback about the result of the message submission. Message submission is realised by means of a submission request. When the message is submitted, checks are performed to establish whether the message meets the specifications defined in the respective interface specification. These controls may also check for the following:

- The required elements are present.
- There are no unknown elements.

- The values contained in the elements have appropriate values and lengths.
- The maximum message size for the interface has not been exceeded.
- The digital signature is present.

If the submission request fails to meet any of these conditions, it will be flagged as having an error.

Forwarding messages
In the delivery, a message is transferred to its intended recipient, in a confidential and reliable manner. For this to occur, the recipient must have implemented a service that can receive messages per the applicable interface specifications. The message must be in line with those specifications.

Re-delivery (re-injection)
If the recipient's service is not available, a message will be re-delivered. The timeout period and the maximum number of attempts are configurable.

Recording the audit trail
Creating an audit trail record makes sure that all relevant information about the processing of a message is recorded in a traceable, irrefutable and unalterable manner. The audit trail is primarily for internal use, such as for trouble-shooting. Reports can be generated from the audit trail to inform the requesting parties about how the generic infrastructure is functioning. Availability of the process infrastructure, failures caused by incorrect message content and throughput times of messages are interesting statistical information regarding the performance of the I-processes.

Requesting status
Status request functionality makes it possible for reporting party to inquire about the processing status of their sent messages. The status information is a selection of information from the audit trail that is relevant to and comprehensible for the reporting party. The status information indicates the steps that have been completed. The final listed step provides the status of the total processing. Status information is requested via the status service.

Authentication
Authentication refers to determining the identity of the sending party up to a certain degree of reliability. The identity of the reporting party is recorded in a trusted registry such as the following:

- A basic registration: Trade Registry or Chamber of Commerce number, company number, municipal personal records database, social security number
- The administration of a service provider (fiscal number, VAT number)
- An equivalent registry outside the Netherlands

There are various methods for authentication:

- Variant 1: based on a certificate that includes an identity with an OIN (governmental identification number) or HRN (trade registry number)

- Variant 2: based on a certificate without an identifying number for the reporting party
- Variant 3: based on an external authentication service

Checking authorisation
This service checks whether the reporting party is authorised to use a certain service (either for requesting or submitting messages) offered via the generic infrastructure. This type of authorisation control is complementary to the authorisation performed when creating a secured connection with the generic infrastructure. Authentication of the reporting party is always performed prior to the authorisation check. The identity established in the authentication is then used for checking the claimed authorisation. In practice, there exist various methods for checking authorisation:

- Blacklist: the identity of the reporting party does NOT appear on a list of reporting parties that are NOT trusted.
- Whitelist: the identity of the reporting party DOES appear on a list of parties that ARE trusted.
- Not trustworthy enough: the identity of the reporting party has not been established at the reliability required for the service.
- Checking if there is a valid approval (permission) in a trusted registry: the reporting party claims that it is authorised to act on behalf of a represented party named in the message. Checks are performed against a registry in which approvals are recorded – an approvals registry. Such approvals can be recorded based on an opt-in or opt-out procedure. More on how this works in Chapter 8.

Backup
Saving an identical copy of a message. This protects the message against processing errors that could result in the message being lost. In a backup's basic form, a message is backed up until processing and archiving have been completed, after which it will be deleted. A message can be secured (backed up) for a longer period, if so requested by the party responsible for the chain.

Archiving
Ensures that archive documents are stored together with the audit trail, until they have been transferred to the next archive creator or until the archiving term has elapsed.

Report generation
Relevant information from the audit trail database is collected and presented in a clear format.

Validation
The message (payload) is validated using a schema/model. If the message is deemed invalid, a validation report will follow, which can be used as the basis for the rest of the I-process. Possible variants of validation include:

- Schema validation: validation based on an XML schema definition (XSD)
- XBRL validation: validation based on business rules defined in XBRL.

- Taxonomic validation: content-based validation using a domain taxonomy

Conversion
A message supplied in a given message schema is converted into an equivalent message in a different message schema, using a set of conversion rules.

Extraction and filtering
Only the message data that are allowed or required for a subsequent step in the I-process will be passed on.

In summary, the following can be concluded from the process descriptions provided above:

- The I-processes of the various reporting flows are virtually the same, broadly speaking. The precise configuration can be different, however, for each type of message.
- The message type determines the I-process that is run.
- Internal applications are modelled, called and configured as services. These are almost exclusively internal services. External services are only called for checking authorisations.
- Reuse of services is possible. They remain reusable (configurable) when the taxonomy changes.

In the following section, we will discuss a number of the services that are orchestrated in further detail.

7.6.5 *Which services are invoked?*

This section describes a number of services that are used in the generic infrastructure as part of the I-processes for business reporting. This summary is non-exhaustive, as other services can be called or developed for information chains. Here, we distinguish between interface services and processing services. Interface services comprise the submission service, the delivery service and the status information service. The other services are processing services, performed by the process engine.

Table 7.3 – List of interface services and processing services (non-exhaustive)

Service	Type of services
Submission service	Interface services
Status information service (for the reporting party)	Interface services
Backup and archiving service	Processing services
Validation service	Processing services
Check authorisation service	Processing services
Status update service (for the requesting party)	Processing services
Final delivery service	Interface services

It is worth noting that the services listed in Table 7.3 are described at the business level, which makes the reuse of services easier. We chose a coarse level of

granularity (combining multiple single functions) to describe them, because otherwise, we would need to summarise many separate services and it would remain unclear how they fit together. Next, some brief explanations of the listed services are provided.

1. Message submission service

The generic infrastructure includes a message submission service. The message submission service is initiated by the reporting party via an interface specification. The message submission service runs through a number of actions for each type of message sent in. These actions can be classified into message checks, process initiation and feedback. The first step carried out by the message submission service is the message check. The interface has a number of specifications, or requirements, that the supplied message must comply with. The basic check consists of the following elements:

- Checking for the presence of a known message type. Without a message type, the submission service would not know which I-process should be run when the process is initiated, so no I-process can be executed.
- Checking the maximum message size. The size of the supplied message is limited in order to guarantee the performance levels of the generic infrastructure.
- Checking for the presence of mandatory elements and absence of prohibited elements.
- Authentication. This includes checking the validity of the PKIgov certificate used and checking to establish whether the certificate is included in a blacklist (list of certificates to be rejected) or whitelist ('guest list' of certificates to be accepted).

If the message meets the specifications of the basic checks, process initiation will follow. The purpose of the process initiation is to ensure further processing of the message by the generic infrastructure and delivery to the requesting party. A message reference will be created to make sure that the message processing is traceable. The original message is also secured (backed up temporarily) at this stage. The backup service will be described in the following section. The proper I-process is activated in the process engine, depending on the message type. The message is transferred to the process engine for further processing. The last step in the submission service is feedback. The submission service provides immediate feedback to the reporting party regarding the message specification checks. Such immediate feedback is required from the process-handling point of view, as it indicates whether the message will be processed further or whether an error has occurred. In the event of an error, an explanation is provided so that the reporting party can take action to submit an acceptable message. If the SOAP2008 protocol is used, the result of the entire submission process will also be attached. In WUS, the session ends with either acceptance for further processing, or an error. The status of further processing must be queried separately. In both SOAP2008 and WUS, if the message was received successfully by the generic infrastructure, a message reference is generated and attached to the message.

2. Status service (for the reporting party)
Through the status service, the reporting party can obtain the current status of each message supplied. The interfaces used for sending in data are the same as the ones used for requesting the status. A different end-point is used to address the WSDL of the status service. The reporting party should have received a message reference upon submission, stating that it met the message submission specifications. The status information and audit trail are stored in the generic infrastructure under this same reference. The response from the status service includes the status history, i.e. a list of relevant actions (services) that the message has run through and their results. The user of the generic infrastructure could receive any of the following information from the status report:

- The message has been accepted by the requesting party.
- The message is currently being handled somewhere in the I-process.
- An error has occurred somewhere in the I-process, with an explanation of the content of the error.

3. Backup and archiving service
Securing (backing up) means that any message that has successfully completed the message specification checks is then stored as a backup in its original state, with a WS security header. If an error occurs in the processing, the original message can be retrieved and processed once again. The original message can also be referred to in the event of a dispute, as it remains in the state it was prior to processing by the generic infrastructure or the requesting party. Chapter 6 (I-processes) provides more insight into the role of security in process compliance. The backup service is a permanent element within the submission service. The archive service is complementary to the backup service. It stores messages provided by the backup service for a predefined period of time. Using an archive service is optional and depends on the agreements between the generic infrastructure and the requesting party.

4. Validation service
The validation service checks whether the content of the message is consistent with the Netherlands Taxonomy and its associated agreements, including the correct use of the XML schema and the XBRL standard. In particular, the following is validated:

- XBRL 2.1
- Dimensions 1.0
- Generic Links 1.0

Validation is only performed against the Netherlands Taxonomy. The generic infrastructure is set up in such a way that it cannot retrieve or consult external extension taxonomies. Please refer to Chapter 5 (Data) for a detailed explanation of the XBRL standard and the Netherlands Taxonomy. Messages that comply with the Netherlands Taxonomy are then transferred to the delivery service. If a message fails to comply, it will not be delivered, as messages that contain errors will always result in an error further in the process. A clear (though often

technical) explanation is provided for any errors encountered. If the user requests the status of their message, this explanation will make clear why the validation failed. The user can then try to resolve the error and re-submit the message.

5. Check authorisation service
The authorisation checking service used for some SBR chains consults a trusted approvals registry to establish whether the reporting party is actually authorised to use a service, for instance allowing it to submit a message or request a message on behalf of a represented party. The authorisation service receives and processes the response from the trusted registry. If the registry's response declares the authorisation to be valid because there is a valid approval in the registry, the authorisation service will give 'permission' for the message to be further processed. If the response from the trusted registry does not declare the authorisation valid, the message will not be processed further and the reporting party will receive an error report.

6. Status update service (for the requesting party)
The status update service keeps the reporting party informed after the message has been delivered to the requesting party. This is particularly important for when the requesting party decides to perform semantic checks itself before it accepts the business report for processing. Once the supplied message has been delivered to the requesting party, the generic infrastructure is no longer aware of how the process is progressing. In fact, the status update informing the reporting party that the message has been accepted by the requesting party is the final result in many processes. However, the generic infrastructure is still the place where the reporting party can request status details, including whether or not a business report message has been successfully delivered. The status update service allows the requesting parties to add the status of their internal message checks to each process reference in the generic infrastructure. The use of this service is optional, as not every requesting party will perform message checks of its own. In that case, successful delivery to the requesting party would be the submitted message's final status.

7. Final delivery service
The process engine transfers the message to the delivery service so that it can be supplied to the requesting party. The delivery service forwards the message to the appropriate requesting party. Only validated messages will be sent, preventing contamination of the requesting party's systems in the form of unprocessable or malicious messages. The delivery service uses the interface between the generic infrastructure and the requesting party to deliver the message. The interfaces listed earlier can also be used for the delivery service. Of those, the preferred choice is ebMS Digilink, since a large number of messages are sent very frequently in both directions. The orchestrating role of the process engine allows services to run through all the required process configurations to fulfil the process infrastructure role of the generic infrastructure.

The list of services provided above is not sufficient for processes that are very different in nature from the processing of business reports. A conversion service must also be developed in such a case to support other types of processes, for instance, processes that require message conversion.

7.6.6 *What are the implications for the users of the generic infrastructure?*

The choices described for the architecture of the generic infrastructure have implications for the user groups, i.e. the businesses and requesting parties. Here, we will discuss the implications that must be taken into account by the users. For businesses (and any intermediaries), the generic infrastructure is a single digital service desk for business reports. Because this process infrastructure operates as a black box, businesses and intermediaries do not need to know much about how the generic infrastructure operates. A company's software only needs to establish a connection with the submission service of the generic infrastructure to be sure that messages will be automatically submitted, processed and received by the requesting party. This allows the generic infrastructure to facilitate exchanges of information between businesses and government entities in a simple and uniform way. Conforming to the interface standards is the only thing that requires effort on the part of businesses and intermediaries. Interface standards must create maximum interoperability with minimum development effort required. The need for quick and easy utilisation of the generic infrastructure by market parties led to the choice of using open standards and existing building blocks as much as possible. It is expected that the open standards used will be further developed in the next few years and that the communication needs will also be subject to change. Consultation with the market, which will be required to accommodate these developments, is a governance theme that we will return to in the final chapters.

For the requesting parties, the generic infrastructure is the link to a large and varied group of businesses. The generic infrastructure enables requesting parties to resolve some of the legal, technical and support issues faced when electronically interacting with reporting parties. The generic infrastructure functions as an automated processing system that carries out well-specified tasks for the requesting parties. The tasks – I-processes – include activities such as message reception, authentication, authorisation, verification and provision of sufficient feedback to chain parties. This enables the requesting parties to focus on tasks that require content-based and domain-oriented expertise. In addition, because the generic infrastructure is based on a SOA, it offers flexible procedures, ensuring that any changes (in the law or otherwise) can be implemented in a simple and unambiguous way. Finally, using the generic infrastructure means that the requesting parties do not have to develop proprietary process infrastructures that need to comply with the stringent reliability, availability and security requirements. Thus, costs are reduced. Conformity to the interface specifications is the main precondition for requesting parties.

7.7 Chapter conclusion

This chapter has provided a detailed understanding of the concept of a generic infrastructures as a building block for SBR chains. The generic infrastructure is build using open standards. It uses a service oriented architecture that safeguards the modular design and loose coupling of web services. The process engine allows for a message-based execution of I-processes. This means that each type of business report follows a specific type of process flow. For example, a VAT return is processed in a slightly different way compared to a statistics report. Moreover, the generic infrastructure handles return messages from requesting parties to reporting parties. In close collaboration with the requesting parties, the SSC determines how a specific type of message is handled. This type of flexibility ensures that the generic infrastructure can be employed in various SBR chains. Satisfying the requirements for a generic infrastructure that can automatically handle multiple types of messages, carry out various process configurations, invoke different web services depending on the type of message and is secure, scalable and flexible, was a challenge, despite the availability of proven and well-documented technological standards (e.g., SOAP, XML, BPEL, X.509). While the more general challenges (such as interdependency and uncertainty) are covered in Part A of this book, Chapter 9 will reveal how more specific governance challenges regarding the generic infrastructure are dealt with. But first, Chapter 8 will describe how the end-to-end information exchange and processing via the generic infrastructure is secured.

8 Information Chain Security

Chapter highlights

- Specifying the risks and requirements for information exchange and processing
- Understanding the enabling technologies
- Realising information security in SBR chains

8.1 Introduction

SBR involves the automated, system-to-system exchange and processing of business information. The following points are important to note:

- The information exchanged is often confidential and only intended for the specified requesting party.
- Confidentiality may apply to all data states (in transit, data at rest/stored and data in use).
- Return messages from requesting parties to businesses can also be confidential (e.g., the tax assessment).
- Actors that employ SBR to complete their own reporting processes must comply with all the applicable laws and regulations.
- Information can be disclosed to authorised intermediaries (e.g., accountants) on behalf of businesses. Intermediaries can also be authorised to access return messages.
- While information is exchanged in a system-to-system manner, it is still transferred via the Internet. Thus, multiple risks from transferring information over the Internet need to be addressed.

Given the above characteristics of information exchange via SBR, information assurance is a shared responsibility of the actors in SBR chains. According to the U.S. DoD directive 3600-1, the essential functions of information assurance include the operations that protect and defend information and information systems. *The objectives of* information assurance *are to provide availability, integrity, authentication, confidentiality, and non-repudiation of information. The process includes protection, detection, and reaction, as well as the capability for information restoration. Physical protection of hardware, timely responses to incidents and fall-back provisions in the event of a disaster are also part of information assurance.* Figure 8.1 provides an overview of the various aspects of information assurance.

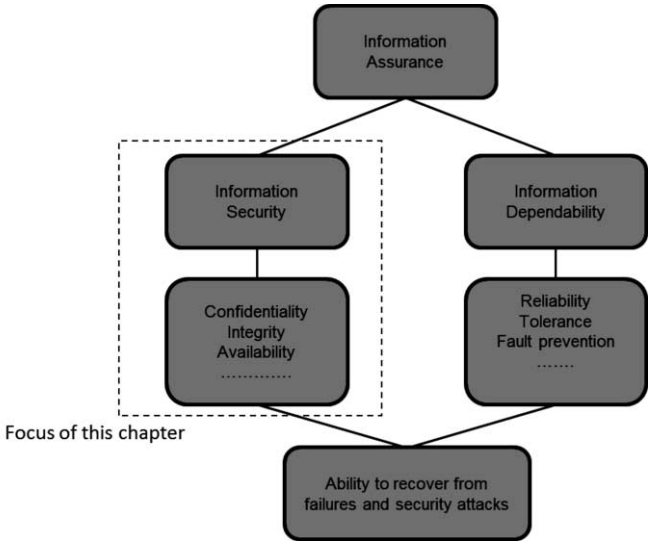


Figure 8.1 – Scope of information assurance (based on Qian et al. 2007)

Led by the shared service centre (SSC), actors in SBR chains are currently undertaking several steps towards strengthening information assurance. Information assurance includes management control over the multi-sided platform, which serves multiple SBR chains.

While this chapter does not cover all the aspects of information assurance in SBR chains, it does address the left part of Figure 8.1, with the assumption that SBR chains actors have already implemented the basic IT security measures (e.g., virus scanners and firewalls) and actively use an ISMS (information security management system) tailored to their environment and interactions. The objective of this chapter is to describe the inter-organisational measures that are the norm for SBR chains. These include setting up a secure (encrypted) connection, identification (the assertion of who someone is), authentication (the act of verifying a claim of identity) and authorisation (determining what actions actors are allowed to perform). In order to provide a comprehensive account of these measures, their descriptions (the 'how') will be preceded by discussing the 'why'

and the 'what' regarding information security in SBR chains. Accordingly, this chapter is divided in four sections.

- **Section 8.2** discusses the risks of information exchange and processing in chains.
- **Section 8.3** elaborates on the applicable requirements for information assurance, which are rooted in laws and regulations. Combined, section 8.2 and section 8.3 address the 'why' question: why information security is necessary in information chains.
- **Section 8.4** covers the technologies that fulfil the requirements presented in section 8.3. This section therefore focuses on the 'what' question.
- **Section 8.5** presents the inter-organisational/overarching information security measures taken in the current SBR chains. Combined, section 8.4 and section 8.5 address the 'how' question: how information security is realised in SBR chains.

8.2 The risks of information exchange

In the first three chapters of this book, we discussed how information chains consist of multiple actors that exchange and process information. Actors employ a chain information system that includes linkages to systems and processes outside their direct control (horizontal S2S integration – see Chapter 1). In the simplest case, at least two parties are involved: the sender (reporting party) and the receiver (requesting party). Figure 8.2 depicts a generic model for information exchange between two parties: the sender (A) and the receiver (B).

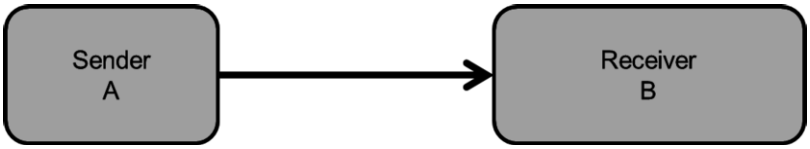


Figure 8.2 – Generic model for exchange between parties A and B

The sender naturally desires assurance that the message cannot be intercepted or manipulated in transit and that it will only be read by the specified receiver. The receiver wants to be sure that the message was indeed sent by A and that it has not been manipulated in transit, since decisions with legal consequences for the sender are made based on the contents of A's message.

While the guarantees that A and B want may seem straightforward, implementing them is not. Similar to exchanging information on paper via mail, exchanging information in an electronic format is not without risks. We define risk using two familiar and adjacent concepts: vulnerability and threat.

A *vulnerability* is a weakness in a system, procedure, design, entity, implementation, or internal control that could be exercised (accidentally triggered or intentionally exploited) by a threat, resulting in a security breach or violation of the system's security. As will be discussed in §8.4, there are multiple vulnerabilities that can be exploited in any S2S information exchange.

A *threat* is a potential cause of an incident that may result in harm to a system or organisation. Threats normally require an active subject to bring about the damage—the threat agent. A threat implies that a certain action could originate from a party external to the system in question, who could initiate action against it.

A *risk* appears when a certain threat materialises, exploits a vulnerability and produces an undesired effect. Risks to information emerge from threats targeting one or more information properties such as the confidentially, integrity and availability. §8.3 provides a more extensive description of these properties. When it comes to the risks to information, we can classify them using the three states of digital data: 1) data-in-motion (in transit), 2) data-in-use (processing/active) and 3) data-at-rest (in storage/inactive). The remainder of this chapter focuses primarily on the risks to data-in-motion, with the assumption that actors will address the risks regarding data-in-use and data-at-rest using their own preferred means.

From the data-in-motion perspective, SBR chains pay significant attention to specific risks related to so-called 'man-in-the-middle' attacks. In this form of attack, a malicious threat agent—let's call him Actor C—may compromise the communication between A and B in various ways. Such attacks form a significant threat and are designed to exploit information, deny or affect service to authorised users, or to acquire, modify or corrupt data. Furthermore, they are often executed by capable, resourced and motivated perpetrators. Figure 8.3 provides an overview of four types of man-in-the-middle attacks, which have been described extensively in the literature (Callegati, Cerroni and Ramilli, 2009; Stallings, 2011).

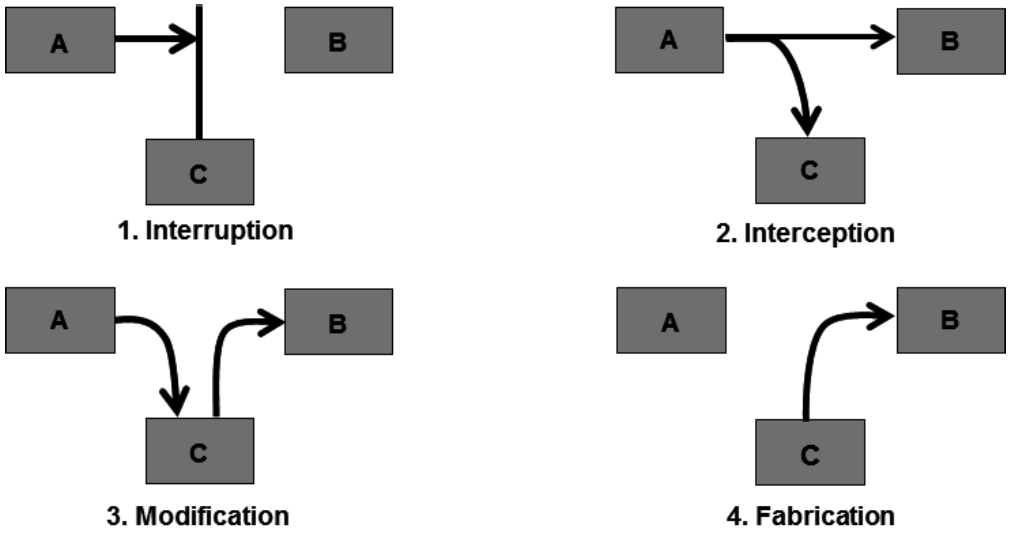


Figure 8.3 – Typology of man-in-the-middle attacks (by malicious party C) that may occur during electronic data interchange between A and B

The first type of man-in-the-middle attack—an interruption—is an attack in which a message sent by A never reaches B. The second type—an interception—is an attack in which a message is copied and viewed by C. The third type —a modification—is an attack in which A's original message is intercepted and modified before it reaches B. Finally, a fabrication attack involves a message composed by C and sent to B under the name of A, but without A's authorisation. Hybrid variants of these attacks are also possible, increasing the number of potential security breaches. These hybrid variants will not be discussed further in this chapter (for examples, see Stallings, 2011).

Please note that the attacks here are described from an 'information push' perspective. Aside from the obvious notifications received when submitting information (e.g., the transaction was successful, the message was rejected etc.), SBR chains can also include an information pull. This means that reporting parties (e.g., businesses and intermediaries) can retrieve notifications (e.g., status updates and final decisions) using their reporting software. Such return messages and others (e.g., tax assessments) are temporarily stored in a 'records repository' (that is part of the generic infrastructure – see Chapter 7) and can be retrieved for viewing by authorised actors. Since the content of return messages is also very confidential, it is important that unauthorised actors not be able to retrieve these messages. Because SBR chains allow both the business and, when applicable, its authorised intermediary to pull information, securing return messages is not as straightforward as one might expect. Moreover, many businesses continually change intermediaries, so it is important that the generic infrastructure is able to automatically determine who is authorised at a given time and who is not. We will come back to the risks associated with the information pull model and how to address these later in this chapter. First, we will describe the broader set of information assurance requirements that are rooted in laws and regulations. An extensive review of the applicable laws and regulations in the Netherlands reveals that legislators have acknowledged the man-in-the-middle attacks described earlier and have prescribed some generic principles that should be adhered to when it comes to information exchange with public agencies.

8.3 The information assurance requirements rooted in laws and regulations

Each country has its own sets of laws and regulations that put forward certain principles, norms or guidelines for information exchange and processing, especially when government agencies are participants in the information chain. The term 'requirement' is often avoided in laws and regulations since it invokes the idea of very specific conditions that must be satisfied in a predefined manner. Anyone who is somewhat familiar with the subject of law and regulations will probably know that they often contain open norms that can be met in various ways. Clearly defined measures are rare, especially when it comes to those based on information technology. Since the field of information technology is dynamic in nature, measures enacted today can be rendered outdated tomorrow. Furthermore, legislators usually understand that measures impose costs and that the

question of whether these costs should be incurred mandatorily depends on the nature of the transaction and its consequences (e.g., financial or legal). Based on open norms, precise requirements are created, tailored to the specific context for which laws and regulations are needed. Nonetheless, we continue with the term 'requirements,' as its use simplifies our discourse explaining why SBR chains are designed in a specific way.

This section proceeds with an elaboration of the information assurance requirements rooted in the laws and regulations that constitute the legal framework for SBR in the Netherlands. Since these laws and regulations are defined in accordance with the laws and regulations of the European Union (EU), they may be relevant for other EU countries as well. Moreover, to our understanding, many countries have implemented similar laws and regulations. Thus, readers from non-EU countries might recognize some of the requirements discussed next.

8.3.1 *Reliability and confidentiality: two abstract norms*

In the Dutch context, the law entitled '*Wet elektronisch bestuurlijk verkeer'* (which, from this point, will be referred to as *Webv*) includes an elaborate set of principles for information assurance, which are based on the more abstract norms of 'reliability' and 'confidentiality' in information exchange. Let us consider the abstract norms first, followed by the more specific set of principles that can be interpreted as requirements.

Reliability and confidentiality: two abstract norms
The Webv states:
Art. 2:14 paragraph 3 AWB
"If a public agency transmits a message electronically, it must be done in a sufficiently reliable and confidential manner, with respect to the nature and content of the message and the purpose for which it is used."
Art. 2:15 paragraph 3 AWB
"A public agency may refuse an electronically submitted message to the extent that the reliability and the confidentiality of this message are insufficiently guaranteed, given the nature and content of the message and the purpose for which it is used."

8.3.2 *Requirements*

Based on the more abstract norms of 'reliability' and 'confidentiality' in information exchange, the Webv stipulates specific requirements for the following:

1. Authenticity
2. Integrity
3. Non-repudiation
4. Transparency
5. Availability
6. Flexibility
7. Exclusivity

The following subsections provide a detailed description of these requirements.

8.3.3 *Authenticity*

According to the Webv, authenticity refers to the degree to which the origin of the document can be ascertained. Is the information what it claims to be? Is it where it claims to be from? Did the message indeed come from the person indicated as the sender? Authenticity can also mean that the source of the information is known and has been verified (Klingenberg, 2011). If a certain public agency electronically sends a decision (e.g., a response to a subsidy request) to a company, it is important to be able to establish (both at the time of receipt and later on) that this decision did indeed originate from that specific public agency and not from someone or somewhere else. The principle of authenticity is closely related to integrity and non-repudiation, as well as to transparency: it must be possible to permanently establish the authenticity of the message. Furthermore, the literature states that authenticity also refers to the amount of certainty to which the identity of the sender can be determined (Schellekens, 2004). When aiming for a high degree of authenticity, one wants to know whether the sender's identity is indeed 'correct.'

8.3.4 *Integrity*

Integrity refers to the assurance that the information received is exactly the same as it was filed (i.e. it contains no modifications, insertions or deletions).[17] Integrity also implies that the information system components utilised are running properly, assuming the structural correctness and completeness of the registration, processing and storage of information. Integrity, like authenticity and the other stated principles, helps achieve legal certainty (Klingenberg, 2011).

8.3.5 *Non-repudiation*

Non-repudiation provides protection against any of the involved entities' denial of having participated in all or part of the communication. Non-repudiation is a two-way concept. Looking at the party that provides information, non-repudiation refers to the proof that the message was sent by the specified reporting party. With regard to the party receiving the information, non-repudiation refers to the proof that the message was received by the specified requesting party.

8.3.6 *Transparency*

Transparency can be interpreted in two ways: 1) transparency regarding the executed process of information processing and 2) transparency about how the information system works and what kind of resources are used. The interpretations are not mutually exclusive. The Explanatory Memorandum to the *Webv* adopts the first interpretation, stating that transparency represents the possibility of detecting data modifications in case they have occurred. The law thus imposes requirements regarding data storage and suggests the possibility of conducting audits. Archiving and the use of audit trails in a system are therefore

[17]Explanatory Memorandum, p. 15.

relevant. With respect to the second interpretation, the Memorandum states that the communication system's operation should be visible and comprehensible (Klingenberg, 2011, p. 11). The publication of official documentation by government agencies contributes to this interpretation of transparency.

Archiving
The requirements for archiving by administrative authorities are regulated by the Dutch *Archiefwet 1995*. This act requires that authorities store the 'specified documents' that they receive and create.[18] Therefore, the government authority needs to prepare a list that specifies what does and does not need to be archived, for how long and where, etc. Two underlying Dutch regulations regarding archiving, the *Archiefbesluit* and the *Archiefregeling,* include requirements for archiving and electronic archive documents. The reconstruction of an original message has high importance, since the content, structure, and format of electronic files can be modified quite easily. This creates a dual challenge: messages must be archived in their original form (as originally received or created) and, at the same time, the information—which may possibly be confidential—must be secured. The archive must thus be protected against unauthorised access or processing (for instance by means of encryption). In turn, the archive must also remain available for authorised consultation.

8.3.7 *Availability*

Availability refers to how reachable and usable the information processing service provided by a public agency is, in accordance with the service level requirements imposed (for instance 24/7 availability). An attack aimed at achieving denial-of-service may be successful when targeting a specific server or application. If the attack is successful, the service will be rendered unavailable. Furthermore, there is a relationship availability and accessibility of the service provided by administrative authorities to businesses, in the sense that it should be possible to use the service with readily available and/or standard (commercial) software.

8.3.8 *Flexibility*

Flexibility refers to the extent to which various, changing and new requirements can be met. When technical capabilities improve, information assurance processes must include these improvements. Therefore, they must be adaptable to changes. It is also important to be one step ahead of hackers regarding intrusion into systems, or at least to be aware of hackers' current capabilities and have the flexibility to implement modifications accordingly.

Each government agency needs to reconsider whether it can protect its information chain against new threats and whether it can easily cater to higher security norms (e.g., following regulations at the national or European level regarding the format of identification numbers, issuing digital certificates) in the existing chain information system.

[18]Article 3 in conjunction with Article 1(c) of the Public Records Act of 1995.

8.3.9 *Exclusivity*

Exclusivity concerns data at rest, data in transit and data in use. Is the data disclosed exclusively to an authorised party, the party that the message was intended for? This principle is closely related to the administrative principle of due diligence. We need to be confident that public institutions will handle data carefully (Klingenberg, 2011) and if necessary, treat it confidentially, such as with personal data or data that could be misused. Special exclusivity requirements are imposed when processing personal data. These requirements are laid down in the Dutch *Wet bescherming persoonsgegevens (Wbp).*

Data protection
The party responsible for the data (e.g., the public institution receiving or processing it), also called the principal, has an obligation to secure the data, which leads to requirements regarding the processing. The principal must ensure that the security requirements are also applied when a secondary processor (another party on behalf of the controller) carries out the processing (articles 13 and 14 of the *Wbp).* The Dutch Data Protection Authority, the CBP, provides guidelines for the application of the legal security standards (Guidelines for personal data protection (CBP 2013), which replaced the CBP AV23 background and exploratory guidelines from 2001). These guidelines inform organisations about how to achieve an 'appropriate' security level. They emphasise privacy by design (i.e. building protection of personal data into the information system from the start) and the importance of risk analysis.

The processing of personal data does not only occur in processes that focus primarily on citizens and their data. The *Wbp* thus also applies when personal data is supplied as secondary information within a message. Examples are the names of board members stated in the financial statements or the address details of a company when processing its business reports. Furthermore, confidential handling can apply to more than just personal data (depending on the category and quantity of the data). Other types of data in the messages exchanged between parties can be confidential and may require measures for exclusivity, for instance information that companies exchange with regulators.

The requirements mentioned above are important for safeguarding legal compliance. This certainty is particularly needed within electronic communication to and from public institutions, as such communication may have significant legal consequences. In addition to the listed set of requirements, a government organisation must always take into account the principles of due diligence and proportionality. Due diligence requires that a government organisation prepare a decision with care by collecting the relevant facts and interests to be balanced. Proportionality means that the goal to be reached must outweigh any interests that are infringed upon and that the government organisation, when possible, must use the fewest/least burdensome measures or resources possible to achieve the goal (Ten Berge and Michiels, 2001).

8.3.10 *Realising reliability and confidentiality*

The open nature of the legal standards can be derived from the required degree of confidentiality and reliability, namely 'sufficient' confidentiality and reliability (i.e. not the maximum possible). The Webv indicates how to determine what is sufficient: it is done *"having regard to the nature and content of the communication and the purpose for which it is used*[19]*."* In the case of information made public by the municipality, the need for information assurance may be different when compared to filing taxes. Depending on the state of the technology, different measures will be taken in such cases.

Nevertheless, the Webv provides a few suggestions for the technical implementation of information assurance measures in information chains. For instance, the explanatory memorandum of the Webv states that electronic signatures, time stamps and encryption are useful techniques for achieving reliability and confidentiality. A practical explanation is given for message encryption and a public key infrastructure (PKI).[20] For an electronic signature aimed at providing evidence of intention, the law refers to the Dutch Civil Code and the Telecommunicatiewet, in which requirements for qualified certificates are laid down.[21] In the end, however, each public agency must decide for itself which practical measures or combinations thereof it will use.

To help shape guarantees/measures for reliability and confidentiality, the Webv states that a public institution can impose further conditions on the use of electronic communication.[22] These requirements and accessory measures may have a technical or organisational character. For example, they could obligate the use of a digital signature for which the party issuing the certificate must fulfil certain requirements. The public agency is also required to formally announce any requirements and measures imposed.[23] If these requirements are not met, the agency may refuse to handle the message received, as the integrity, authenticity and/or exclusivity cannot be guaranteed. This refusal can also occur if the sender fails to meet the technical regulations imposed by the government organisation for receiving certain types of messages—if the sender, for instance, uses software that the government organisation cannot handle.[24]

---

[19]Article 2:15 paragraph 3 of the Awb (Dutch General Administrative Law Act).
[20]Explanatory Memorandum, pp. 16, 19, 21, 35.
[21]Article 2:16 of the Awb states that the regulations in Article 15a and Article 15b of Book 3 of the Dutch Civil Code apply to electronic signatures.
[22] Article 2:15 paragraph 1, Awb. Explanatory Memorandum, p. 16.
[23]P.J.J. van Buuren in Tekst en Commentaar Algemene wet bestuursrecht (Text and Comments on the General Administrative Law Act), 2009, p. 69.
[24]Explanatory Memorandum, p. 31.

8.3.11 *Intermediate conclusion*

The requirements discussed above demonstrate legislators' awareness of man-in-the-middle threats such as interruption, interception, modification and fabrication, and of the volatility of electronic communication, which may prevent the required legal outcome of information exchange and processing. Because of these threats, public agencies are faced with the question of how to satisfy the imposed requirements. According to the Webv, the nature, content and purpose of messages should be taken into account when determining measures. The law provides little actual detail about how to satisfy the requirements.

In short, a public agency will need to determine for itself which technical and organisational implementations it will apply in practice. The Webv explanatory memorandum, however, does refer to resources used in practice, such as message encryption, digital signatures and a public key infrastructure. These and other enabling technologies are used to secure SBR chains, helping to shape the inter-organisational measures that are the norm for SBR chains. Before we explain how certain specific technologies are applied for the purpose of information assurance, we will first elaborate upon these enabling technologies in more detail.

8.4 Enabling technologies

Many books are available on technologies that enable the development of confidentiality and reliability measures. In order to provide a comprehensive description of the inter-organisational measures developed to secure SBR chains (§8.5), it is important that we elaborate on the essentials of the following technologies:

- Cryptography: encryption, decryption and digital certificates.
- The application of cryptography to the communication layer and the application layer: TLS protocol, hash functions and digital signatures.
- Public key infrastructures (PKIs).

The following sections describe these technologies in more detail.

8.4.1 *Cryptography*

8.4.1.1 Encryption

The infrastructure that SBR chains employ for system-to-system information exchange and processing—the Internet—is, in its original design, open and not secure (see textbox).

Cryptographic techniques such as encryption and decryption play a crucial role in addressing the weaknesses of the Internet. Encryption is a process in which a readable text (plain text) is converted into encoded or enciphered text through the use of cryptographic algorithms, which make the text incomprehensible in its encrypted form (Laudon and Laudon, 2010). Examples of cryptographic algorithms include AES, Triple DES and RSA (Stallings, 2011). Such algorithms render the text unreadable by performing various mathematical operations on the bits and bytes. In order to be able to read the encoded text, the process must be

performed in reverse order—from encoded text to readable text—a process known as decryption. Both encryption and decryption require a numeric code that is often simply referred to as the key.

Why the internet is inherently insecure?
The foundational technologies underlying the Internet can be described as a stack of protocols that were developed in the 1970s (Stallings, 2009). Often referred to as the 'Internet protocol suite,' many of these protocols are now common in most information systems (Brookshear, 2012). The TCP/IP protocol—a combination of the Transmission Control Protocol (TCP) and the Internet Protocol (IP)—plays an important role in Internet communication, because it facilitates end-to-end connectivity by specifying how data should be formatted, addressed, transmitted, routed and received at its destination. However, communication via the TCP/IP protocol is easy to intercept (Bosworth, Kabay, & Whyne, 2009). The reason for this is that TCP/IP has no inherent security—everything is plain text. Thus, packets can be sniffed or captured, and IP addresses can be faked.

The most common forms of cryptography are symmetric and asymmetric cryptography (Paar and Pelzl, 2010). Symmetric cryptography uses a single key (a series of codes), with the same secret key being used for both encryption and decryption. The symmetric aspect refers to the fact that the encryption key and decryption key are identical. However, there are two significant restrictions to symmetric cryptography:

1. Key distribution. How do the sender and receiver transfer the secret key to one other? If the sender sends the key over the Internet along with the encrypted message, this creates the risk of both the message and the key being intercepted. This method is also virtually unworkable if the parties do not know one other.
2. Lack of non-repudiation. Because both parties have the secret key, either party could have been the one who drafted and encrypted the message. Thus, it is not possible in this case to prove that the message was drafted by a particular party (Paar and Pelzl, 2010).

An alternative to symmetrical cryptography was developed in 1976: it is known as asymmetric cryptography (Diffie & Hellman, 1976). This form of cryptography is a 'two-key' system that uses two mathematically related keys: a public key and a private key. The asymmetric aspect refers to the fact that a single key can only be used for one function—either encryption or decryption—but not for both, as is the case with symmetric keys. A key feature of asymmetric cryptography is that a message that has been encoded with a private key can only be decoded using that same person's public key, the other key of the pair. Likewise, a message encoded with a person's public key can only be decoded using their private key. The private key is not solely used for encoding and the public key for decoding. Both keys can be used for encoding or decoding. The obvious restriction is that once the message is encrypted with one type of key (public or private), only the other key of the pair can be used to decrypt it. The use of two different keys for

encryption and decryption indicates who has sent the message and implies that decryption is only to be performed by the intended recipient (Kleve, 2004).

Although asymmetric cryptography solves the problem of key distribution in symmetric cryptography, it raises another issue. If, for example, actor A wants to communicate reliably with actor B using actor B's public key (actor A encrypts the message with actor B's public key), actor A must be able to establish that actor B's public key is really associated with actor B. The party guaranteeing this association is usually referred to as a 'trusted third party' (TTP). An environment that enables quick and reliable checks of key-actor association is called a public key infrastructure (PKI). We will come back to this concept in §8.4.3.

8.4.1.2 Certificates

A certificate is an electronic document that contains the identifying data (name) of a user (organisation or legal entity), its public key, the name of the party issuing the certificate and the certificate's period of validity. Certificates have various functions. The following three functions are relevant for this chapter:

1. Setting up a secure connection. This is needed to safeguard confidentiality and requires encryption at the communication layer.
2. (SOAP)message signing: this allows a recipient of a message (e.g., the generic infrastructure) to cryptographically verify (in the present) if the message was unaltered since it was signed and sent by the reporting party. This function and the next are associated with the encryption at the application layer.
3. Advanced Electronic Signature. Aligned with the provided messages, an electronic signature can be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. It requires the inclusion of a digital signature with the same legal consequences as a hand-written signature (a qualified electronic signature).

The term 'electronic signature' is a broad concept that also includes scanned signatures, document imaging, PIN codes and signatures using an electronic pen, as well as biometric identification methods such as iris scanning and fingerprints. These types of non-digital signatures are not within the scope of this chapter.

8.4.2 *Implementing encryption*

Considering the multiple functions of encryption, using it in information exchange would seem a simple choice. Why should we expose data to unauthorised entities, if we can protect it through encryption, thus ensuring the principle of exclusivity? From a conceptual point of view, encryption can be used in multiple layers of information exchange or information processing. Depending on the layered model we are using (e.g., TCP/IP, OSI), we can refer to encryption in the application layer, the data layer and the communication layer. The idea is that an encryption failure in one layer will be compensated for in the following layer.

This concept is sometimes referred to as 'defence in depth.' We will not be discussing encryption across all the layers in further depth. However, we do want to stress that although multi-layer encryption can improve security, it also requires additional computing power and may thus reduce the performance of information processing systems. Moreover, increased encryption often means more complexity, since multiple keys need to be managed and more agreements between actors must be made. These factors might explain why, in practice, encryption is often only used for the communication (transport) layer and the application layer above it. The following sections explain encryption in these two layers.

8.4.2.1 Encryption at the communication layer

Protocols such as the Secure Socket Layer (SSL) and its successor, Transport Layer Security (TLS), are often used for encryption at the communication layer. Both use X.509 certificates and hence, asymmetric cryptography to authenticate the counterparty in the communication and exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. SSL has been so widely used that it has become a synonym for a secure connection. Nevertheless, there are some technical differences between SSL and its successor, TLS, so it is necessary to be explicit about which protocol is used. Moreover, recently discovered vulnerabilities have rendered SSL insecure. TLS is a protocol (a layer above TCP/IP) that can be used by applications to set up a session between a client and a server, to exchange keys and to encrypt the data exchange. The solutions provided by TLS include encryption (session encoding), authentication of the server and, if required by the server, client authentication. While the latest version of TLS (version 1.2) is considered to be secure, we can expect new versions of TLS to appear as vulnerabilities are discovered and threats evolve.

A TLS session starts with what is called a 'handshake'—the exchange of data between the client and the server. The complete handshake is itself a comprehensive topic but for the purposes of this chapter, we will not discuss the complete handshake in depth. What is important here is that the two communicating entities—the client and the server—decide on a common TLS protocol and ciphers (i.e. Block Ciphers or Stream Ciphers) that they will use to perform the encryption/decryption. Public key cryptography is used to select the ciphers. Later on in the handshake, the client and server decide on session keys to use. Next, encryption/decryption are performed using the generated session keys. The following figure illustrates the basic interactions that occur in a handshake.

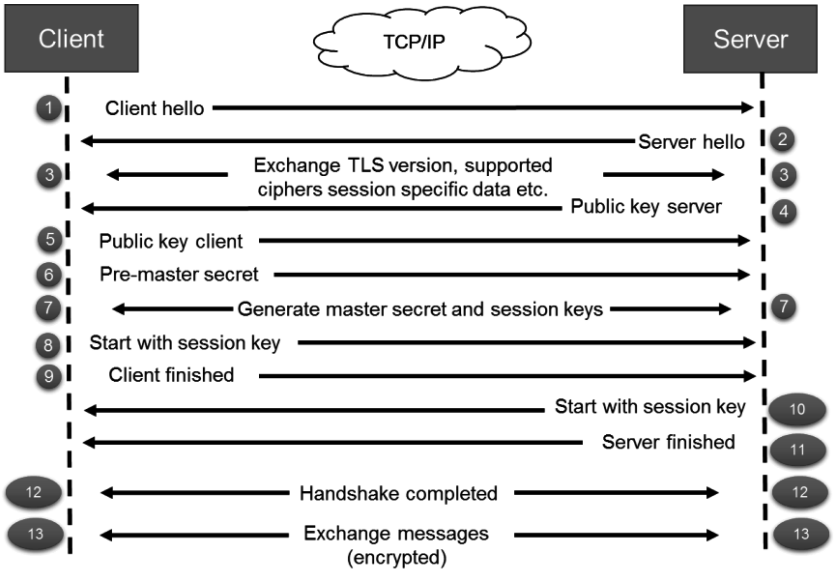


Figure 8.4 – Generic model for establishing a handshake with two-way authentication using certificates

The handshake allows the server to identify itself to the client using a public key. This can also be done the other way around: the server may ask the client to identify itself. When the server and the client each need to identify themselves and authenticate the other, it is known as two-way authentication (Kizza, 2009). Initially, asymmetric encryption is used to set up a connection. After that, clients and servers can jointly agree to use a symmetric key for quick decryption and encryption during the remainder of the session. The data packages are encrypted as they leave the local application/server. This is also known as setting up a 'tunnel.' The data packages are then sent from the sender's application to the server of the receiver, over the Internet. The authentication options for asymmetric encryption are combined with the efficiency benefits of symmetric encryption. A session is terminated actively or will stop after a timeout.

TLS is a generic solution to ensure simple exchange of encrypted information by applications. TLS is flexible – various encryption algorithms can be used. TLS is also independent of the application, which means that it can be implemented up to the level of a web page (and web service, if required). Encryption at the transport level is kept separate from the applications that want to use it. The applications using TLS and their data types can vary widely, from web browsers, e-mail and system-to-system information exchange, to voice and image data. Whereas relatively expensive leased/private lines were needed for information exchange in the past, all that is required now is an Internet connection. This makes TLS an attractive protocol for securing information exchange. Moreover, TLS leaves room for a number of agreements about the communication between

the sender and the receiver, including the specification of an encryption algorithm, the duration of the session as well as the permitted resources for identification. This protects the exclusivity of the session. Standard interface specifications can be agreed upon for the use of tunnels within a chain.

An alternative to the tunnel is a virtual private network (VPN). This option is particularly interesting if the communicating parties already know and are familiar with each other (e.g., two government organisations), if they communicate with each other frequently and if large numbers of messages are interchanged. A VPN can be seen as a protected network within an existing open network. A VPN can be set up entirely using software. Physical, self-managed components can also be used.

Diginetwork
The Netherlands has its own network for governmental purposes. It is called the Diginetwork and uses self-managed components. Some of these components allow messages to be exchanged between governmental organisations using a VPN. The advantage of a VPN is that information can be exchanged between multiple network partners. However, it should be taken into account that everything can be read by other network partners in the VPN if no additional measures (e.g., encryption at the application level) have been taken.

Tunnels are similar to a VPN in that they also create a protected connection within an available open connection. However, there are also differences between the two. A tunnel uses point-to-point encryption; a VPN uses many-to-many encryption. A tunnel generally has a temporary (short) session period, while the session period of a VPN is often longer. From outside the VPN, everything seems to be encrypted. Within the VPN, all communication seems open. VPNs and tunnels are not mutually exclusive. It is possible to use tunnels within a VPN to prevent other parties with access to the VPN (justified or otherwise) from viewing the information being exchanged.

8.4.2.2 Encryption at the application layer

An important characteristic of encryption at the application layer is that it allows security to be applied to the smallest element: the information itself. It can determine, down to a high level of detail, which information should be secured and which need not be. The big advantage of encryption at the application layer is that it creates integrity on an end-to-end basis. This means that the information is continuously secured from the moment of sending. The information should be readable only by the receiving party for whom it is intended. It is important for the successful implementation of such a security application that all communicating parties can handle the relevant application and that the requisite key management has been set up properly. This presents a challenge for encryption at the application layer, since agreements between the communicating parties are required in order to make sure that the information can be shared. One important encryption implementation at the application layer is the digital signature.

8.4.2.3 The digital signature and the hash function

The digital signature was mentioned in §8.4.1.2 as one of the main functions included in a certificate. We explain this concept in further detail by answering the following three questions:

1. What is a digital signature?
2. How is a digital signature placed?
3. What functions does a digital signature fulfil and why?

1. What is a digital signature?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message. It is not to be confused with a digital certificate. A digital signature is the encrypted (encoded using a private key) hash value of the data to be signed. Within the context of this chapter, 'data' refers to the content of selected fields of a certificate or message. The meaning of the 'hash value' is explained in the answer to the second question.

The fact that a signature can be placed on either a certificate or a message can sometimes be confusing, although the effect is the same in both cases. In addition, the term 'signing' is used in different ways for various sources. To avoid confusion where the distinction has to be made, we shall refer to the placing of a digital signature for authentication purposes as 'signing,' whereas the term 'qualified signature' will be reserved for the placing of a digital signature that has the same legal effect as a hand-written signature. Both signing and placing a qualified signature use the same technique: the hash function. One of the most significant differences between the two meanings of 'signing' is that placing a qualified electronic signature requires the certificate to be under the sole control of the signatory. If a certificate is under the sole control of a business, but can be used by multiple employees (i.e. an organisational certificate), a message can be signed using a digital signature, but this would not qualify as an electronic signature.

2. How is a digital signature placed?

One frequently used technique for placing a digital signature is by generating a hash value (also called a checksum) with a hash function and encrypting this value (see boxed text below). Encrypting the hash is done at the application layer. To summarise, the process involves generating a unique value based on selected fields from a message (certain fields in the header, the body or the payload). The value generated is often called a hash value, a 'fingerprint' or a 'message digest.' The hash value is then encrypted using the sender's private key and is sent to the receiving party along with the message content, which may or may not be encrypted.

Usually, the content of the entire message is not encrypted using the private key.[25] The hash value is a fixed set of bits that requires less computing power when encrypting or decrypting than the variable and larger set of bits in a message. Figure 8.5 illustrates the generic operation of a hash function.

How a hash function works
A hash function takes the input of a broad set of values and converts them into a smaller series of values. When the hash function's output gives the same value for a received message—H(b)—as the value supplied with the original message—H(a)—this can be taken to mean that the received message is indeed identical to the message that was sent.

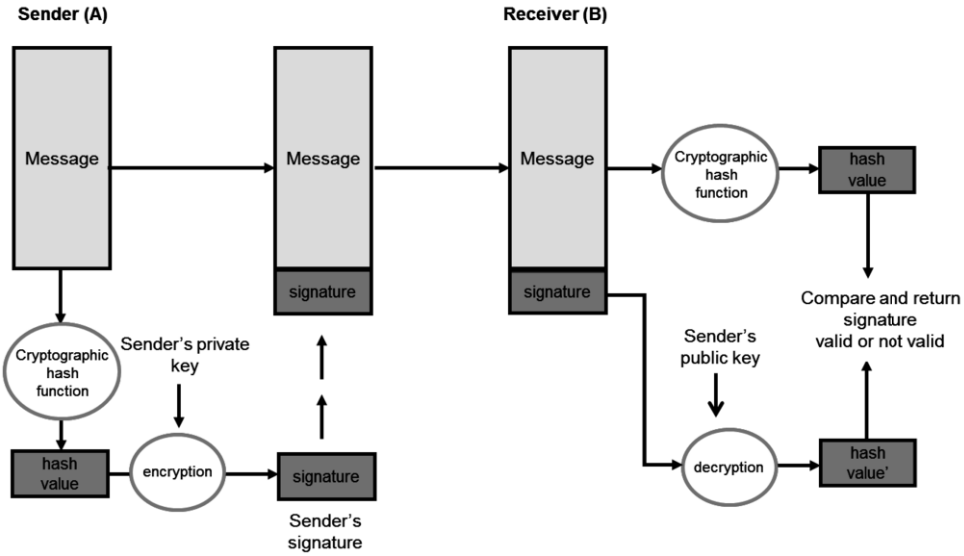


Figure 8.5 – Simplified depiction of using a cryptographic hash function to create a digital signature for authentication purposes (based on Stallings, 2011)

Upon receipt of the message, the receiver can use the sender's public key to verify whether the message was really sent by the sender. In other words, the hash value will reappear after the receiver has decrypted the message. The receiver

[25] In general, only the hash value is encrypted using the private key and not the entire message. If both the message content and the hash value are encrypted using the private key, this can be seen as redundant (duplication of work). Any change in the message content can be detected using the hash value. If only the hash value (a fixed set of bits) needs to be encrypted or decrypted, less computing power from the sender and the receiver is required. Particularly when the receiver must process a large volume of messages (such as for SBR message flows), it is recommended that only the hash value be encrypted or decrypted, rather than the entire message, because the hardware (and its costs) can be impacted. However, if exclusivity must be protected and is not ensured by additional measures, encrypting the entire message can be considered.

can then run the message through the same hash function. If both hash values are identical when compared, the receiver can be certain that the selected data has not been altered during transmission. A hash function calculates a unique value based on the message content. If any element in the message has changed, the hash function will output a different value. In other words, whenever the hash value obtained after decryption using the public key is the same as the locally calculated hash value, we can assume that 1) A is the sender and 2) the message has not been altered during transfer.

The hash function is based on an algorithm. One frequently used algorithm is the Secure Hash Algorithm, abbreviated as SHA (Burr, 2006). Several SHA variants are currently available, with various hash values and small design differences. SHA-1 creates a 160-bit hash value. In February 2005, cryptography experts detected theoretical shortcomings in SHA-1, which raised doubts about whether the algorithm would remain useful. Currently, SHA-1 is still secure, but its future usability is under question. It was therefore decided within the PKI-government system to follow the advice of the National Institute for Standards and Technology (NIST) to start issuing certificates based on the improved SHA-2 algorithm as of 1 January 2011. SHA-2 is a collective name for versions of the algorithm having various larger hash values. A number of versions are available, including 224-, 256-, 385- and 512-bit. PKI-government uses the SHA-256 algorithm.

3. What functions does a digital signature fulfil and why?

The digital signature allows the sender of a message to attach a unique value to the message or certificate (Brookshear, 2012). Here, 'unique' means that the value is linked with the message and/or certificate. In the case where a certificate is being signed, the function of the digital signature is to assure trust in the certificate. In the case where a message is being signed, the digital signature has the following functions:

- **Authentication.** As the encrypted hash value (the signature) can only be read through decryption using the sender's public key, the receiver can safely assume that the message can only be from the owner of the associated private key.
- **Guaranteeing message integrity.** If the content of the message changes *en route*, the attached encrypted hash value will always be different from the hash value calculated by the receiver using the same hash function following decryption. If the two hash values are identical, the receiver can be sure that the message (or its selected fields) has not been changed.
- **Non-repudiation.** The hash value can only be encrypted using the sender's private key, and decrypted using the sender's public key. If the hash values are the identical, the sending party cannot deny that it drafted and sent the message.

When placing a qualified electronic signature into a message, the digital signature has the following function:

- **Expression of intent.** Back in 1978, researchers stated that "if electronic mail systems are to replace the existing paper mail system for business transactions, signing an electronic message must be possible" (Rivest, Shamir and Adleman, 1978, p. 122). This quote emphasises the need in electronic data interchange for a digital signature with a certain degree of legality. As stated earlier, this function requires a certificate that is under the sole, personal control of the signatory. These and other requirements are embedded in legislation.

The above functions of digital signatures are not mutually exclusive and can be combined. However, they do assume that the sender's public key truly belongs to the sender and is mathematically related to the sender's private key. In addition, these functions only apply if the private key belongs exclusively to the sender. To ensure this is the case, the digital signature must be based on a 'qualified certificate': a certificate issued in accordance with rigid procedures and specific requirements. Such is the case with PKI-government certificates, which will be discussed later in the chapter.

Intermediary conclusion

One of the main purposes of cryptography (encryption and decryption) is to achieve exclusivity (confidentiality) in the information exchange process. The use of keys—symmetric and asymmetric—ensures that messages cannot be read by anyone other than the intended receiver. Depending on the level of security required, cryptography can be used at various layers. It is often applied to the communications layer, where 'tunnels' are created between the sender and the receiver that they can then use to transfer information. In addition, using cryptography at the application layer can help achieve a form of what is often referred to as end-to-end security, as the encryption takes place at the source (the sending application) and remains right through until the receiving application. However, encryption imposes requirements on computing power and the management of keys. Therefore, the question of whether or not to use of encryption at a certain level should be addressed by balancing all of the aspects that play a role information exchange and processing in chains. A PKI provides an environment for systematically using asymmetric encryption in information chains. We will discuss the nuts of bolts of a PKI next.

8.4.3 *Public key infrastructure*

Asymmetric keys are usually given to users as certificates. A public key infrastructure (PKI) is used to organise and manage such certificates. The word 'infrastructure' here implies a system of measures and procedures that enables the sharing of the public key in a practical and reliable way. As such, PKI enables parties within a single organisation, or parties between whom there has been no previous connection, to communicate with one other electronically in a reliable manner. This section provides a generic description of a PKI's function based on

its elements. Furthermore, the specific features of PKI-government compared with a PKI in general will be discussed.

8.4.3.1 Background

Usually, a PKI is broadly defined as a combination of software, hardware, roles, guidelines and procedures that are required to manage (create, distribute, use, store and withdraw) keys as digital certificates (see Ballad, Ballad and Banks, 2010; Roebuck, 2011). This is a broad definition that links a number of concepts together. We will begin by discussing the relationship of the PKI with encryption and the use of keys.

A PKI is a structure that relies on the function of a trusted and independent third party to remotely arrange the matters of identification and authentication between two parties (the sender and the receiver). This structure comprises the management of asymmetric keys (Adams and Lloyd, 2002), which, as stated earlier, involves two different keys that are mathematically related: a public key and a private key.

Unlike the use of symmetric keys, in which encryption and decryption is performed using the same key, asymmetric keys are only used for one of the two processes. One of the pair is used to performing the encryption and the other is then used for decryption. To illustrate this, let us consider the communication between two parties: the sender (A) and the receiver (B). In a PKI, at least one of the parties has both a public key and a private key. The public key is disclosed and the private key is kept secret by its owner. In a communication from A to B, three different applications of asymmetric keys can be distinguished for encryption and decryption:

1. A encrypts the message using B's public key. This message can then only be opened using B's private key. As the private key is secret and only B has it, we can assume that only B is able to decrypt the message.
2. A encrypts the message using his own private key. B (and other parties as well) can decrypt the message using A's public key. In this scenario, B knows that A is the only one who could have sent the message.
3. A first uses his own private key and then B's public key to encrypt the message. This scenario is called double encryption. B first needs to use his private key to decrypt the message. The result is a message that is still encrypted and can be decrypted using A's public key. This scenario of double encryption provides more certainty than either of the two preceding scenarios. A and B are both sure that the communication is taking place only between them.

The scenarios stated above assume an important precondition: that the keys are being managed properly. This management comprises a series of activities that include the following

a. Creation and issuance of keys
b. Determination of the lifespan of keys
c. Storage of keys

d. Distribution (publication) of public keys
e. Withdrawal of keys (e.g., in the event of theft or misuse)
f. Publication (announcement) of withdrawn keys.
g. Recovery of keys

8.4.3.2 Elements of a PKI

Various commercial and public PKI variants are used in practice. An in-depth study of PKI systems reveals the following recurring elements:

- Certificates
- Certificate Authority (CA). There are two types of CAs: root CAs and intermediate CAs
- Registration Authority (RA)
- Users (certificate holders)
- Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP)
- Certificate Policy (CP) and Certificate Practice Statement (CPS)
- Electronic storage location
- Chain of trust, root CAs and Policy Authority (PA)
- The digital signature and the hash function (see §8.4.2)

These elements will be discussed further below.

Certificates in a PKI

We will now discuss the content and functioning of a certificate in detail. The X.509 standard[26] is generally used for recording data in a certificate. The way in which the certificate is installed is also known as certificate profile. A certificate profile consists of a number of fields, which are the attributes of the certificate. An overview of the certificate profile is provided in Table 8.1.

The number and exact classification of fields depends on what has been agreed upon in relation to these items. In the Programme of Requirements of PKI for the Government, the fields are classified into mandatory, optional, non-recommended and non-permitted (Logius, 2011). The policy authority (PA) requirements and the specific certification authority (CA) requirements for a specific domain may be included in a certificate as additional attributes. To safeguard the reliability of a certificate, the X.509 standard requires the certificate's issuing party—the CA—to place its digital signature on the certificate.

[26] X.509: an IEFT standard that provides the basis for setting up certificates electronically. It is also recognised as a standard by ISO.

Table 8.1 – Certificate profile: generic attributes of a certificate (based on PKI-government 2012)

Attribute (field)	**Explanation**
Basic attributes	
Version	Describes the version of the certificate.
Certificate Serial Number	A serial number that uniquely identifies the certificate within the issuing CA domain.
Signature (Algorithm ID)	Determines the algorithm (e.g., SHA- 256 WithRSAEncryption), as determined by the PA.
Issuer (Distinguished Name)	Contains a Distinguished Name (DN) of the party issuing the certificate (the CA). This field has at least the following sub-attributes: Issuer.countryName, Issuer.OrganizationName and Issuer.commonName.
Validity (not valid before… not valid after…)	Determines the start date and end date of the certificate's validity in accordance with the applicable policy laid down in the CPS.
Subject (Distinguished Name).	The attributes that are used to define the subject (end user). This field has at least the following sub-attributes: Subject.countryName, Subject.OrganizationName and Subject.commonName.
SubjectPublicKeyInfo	Contains the public key, identifies the algorithm that the key can be used with.
Subject.serialNumber	Identifying number of the certificate holder. The Subject.serialNumber is also intended to ensure a distinction between subjects with the same commonName and the same OrganizationName.
Extensions	
CRLDistributionPoints	Contains the uniform resource identifier (URI) of a CRL distribution point.
AuthorityKeyIdentifier	Contains the hash value of the authorityKey (public key of the CA).
SubjectKeyIdentifier	Contains the hash value of the subjectKey (public key of the certificate holder).
KeyUsage	This attribute specifies the intended purpose of the public key included in the certificate. Various bits are included in the PKI-government's keyUsage extension for each type of certificate.
CertificatePolicies	Contains the Object Identifier (OID) (a row of numbers that unambiguously and permanently indicate an object) of the CP and the URI of the CPS.

Certification Authority as trusted third party (TTP)

The Certification Authority (CA) is responsible for issuing and managing key pairs and digital certificates. Signing an issued certificate is part of this function. It includes placing a digital signature on/in the certificate. Signing is done by generating a hash value from certain fields in the certificate. The certificate is then encrypted using the private key of the CA as the trusted party. Exactly how this is done was explained in §8.4.2.3. The signature is required to prove that the certificate is genuine. It will therefore be difficult to falsify the certificate, and it can be checked by anyone using the CA's associated public key.

The CA's private key should preferably be stored offline (not on a device that can be accessed via the Internet) to avoid the key being compromised. Once a key is compromised, no certificates from the CA can be trusted anymore. Such an event could have far-reaching consequences, such as the need to replace all of the certificates issued by that CA.

The CA acts as TTP within a PKI. This role gives the CA a number of responsibilities. For example, the CA must ensure that the identities of new users are checked before certificates are issued. In general, these checks are outsourced to the RA. This role will be explained below.

Registration Authority
The Registration Authority (RA) is responsible for providing user credentials to the CA that are needed for the issuance of certificates. The RA ensures that the identity of the user is established (via authentication). The RA does not sign the certificates or issue them – these tasks must be performed by the CA. This means that a relationship of trust must exist between the RA and the CA.

Users (certificate holders)
A user submits an application to the RA in order to obtain a certificate. To this end, the user needs to identify himself. The identification method depends on the type of certificate the user is requesting. Physical identification using a valid ID card is only needed for a few types of certificates, although it is often the case for the type of certificate used for communicating with administrative authorities (such as PKI-government—this will be explained later on). When submitting the request, the user also indicates the purpose for which the certificate will be used—such as digital signatures, encrypting information, etc. The user is expected to read the CA's Certification Practice Statement.

Certificate Policies and Certificate Practice Statements
CAs are expected to be explicit about the Certificate Policy (CP) and Certificate Practice Statement (CPS) used. These two documents provide insights into how the CA operates. A CP describes the minimum requirements imposed on the service—with respect to the certificates provided—by a CA within a PKI. A CPS indicates how these requirements have been fulfilled. In addition, a CPS often describes the procedures and measures adhered to by a CA when creating, issuing and withdrawing certificates.

Certificate Revocation List
A valid certificate is the basis of electronic trust. To reduce the risk of unauthorised use of private keys, certificates have a limited validity period of a few years. If trust is lost in the meantime, then—assuming the PKI is functioning properly—the certificate would have to be withdrawn. It is extremely important that the owner of a certificate report such a situation to the CA as soon as possible. CAs use a Certificate Revocation List (CRL) to state publicly which certificates can no longer be trusted. A CRL is a publicly accessible list of withdrawn

certificates. It is published and signed by the issuing CA, which is also responsible for maintaining the list. A certificate may be withdrawn for various reasons, such as theft or loss of a private key (e.g., in the event of a server crash or upgrade). Once the validity period of a withdrawn certificate has lapsed, the certificate is no longer published on the CRL. CAs must ensure that CRLs are available via an online facility. This is done via the Online Certificate Status Protocol in many PKI systems. Each certificate can be checked immediately in a system-to-system manner using this protocol.

Electronic storage location

An accessible electronic storage location is needed in a PKI. This repository, as it is often known, has to ensure access to the following:

- The CPS of the CA
- Agreement and applicable conditions of use
- Certificates (only containing the public key) of certificate holders
- CRL

The electronic storage location must be available to everyone on a 24/7 basis, except when maintenance work is being carried out. Access control to the electronic storage location is arranged such that read-only access rights are assigned to third parties who need to consult the information. Only the CA has write permissions for the electronic storage location. Public key certificates will typically (although not always) be stored in repositories and accessed as required. For example, most browsers keep a list of the certificates that they have come across.

Chain of trust, root CA and PA

A PKI assumes a chain of trust, meaning that trust is passed through a chain. This can be done using a certification path: an uninterrupted chain of trusted points between two users to let them authenticate one other via sub-certificates up to the root certificate. Various groups of users (sub-CAs) are created under the root certificate; those groups have a relationship of trust with the root CA. A certificate issued by a CA within the chain of trust is always trusted by others downstream in the chain of trust, since a higher-level CA assures this trust by means of signing the certificate containing the public key of the lower-level CA. An end user can therefore trust all CAs and certificates that are covered by the same root CA (master certificate).

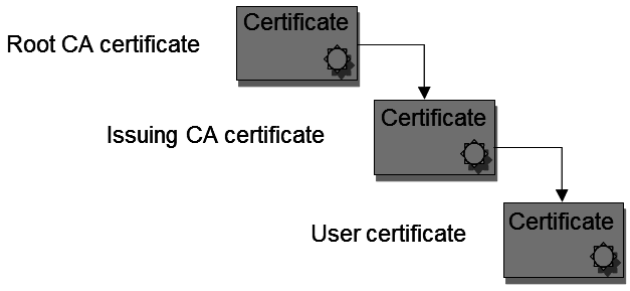


Figure 8.6 –Certification path in a CA hierarchy

But how can one be sure that the root CA is a trusted party? In principle, this can be ascertained in two ways: cross-certification and self-signing. Cross-certification means that root CAs sign each other's certificates. Doing so requires harmonisation between the various CPs and CPSs, which is the most complex part of the cross-certification. For example, if one root CA uses a higher security level for issuing certificates than the other root CA, certificate information cannot be exchanged, as it would constitute a breach at the root CA with the highest safety level. Once the CPs and CPSs become proper matches through harmonisation, however, the CAs can be said to have a relationship of trust. Self-signing, on the other hand, means that the root CA signs its own certificate. This is done by parties such as administrative authorities, who do not want to depend on commercial parties for maintaining a chain of trust. This option was chosen for PKI-government.

8.5 Information security measures in SBR chains

8.5.1 *Scope*

The previous sections have explained the requirements regarding information assurance as well as some enabling technologies. The remainder of this chapter will describe how some of the enabling technologies are used in SBR chains. We will specifically focus on the generic, inter-organisational, measures for information assurance in SBR chains. In order to discuss the measures systematically, we will use an extremely simplified overview of three typical I-processes that reporting and requesting parties might deal with when exchanging business reports and optional follow up messages (status descriptions and notifications) via the generic infrastructure:

1. Submission I-process: the reporting party (a business or its authorised intermediary) submits a message via the generic infrastructure.
2. Status information I-process:
    a. The requesting party submits a status update.
    b. The reporting party can automatically check whether there is a status update available and can retrieve with.
3. Notification I-process:
    a. The requesting party submits a notification regarding a business report (e.g., a tax assessment message).
    b. The reporting party can retrieve the notification if available.

Figure 8.7 provides an high level illustration of these I-processes, each of which is handled via the generic infrastructure.

The following sections indicate how specific components are used in each I-process to ensure reliable and confidential S2S exchange and processing of business information. When necessary, we will address specific features of a component that are important for information assurance. We start with the submission process (including the status request process), which emphasises the use of PKI-

government service certificates as a component for identification and authentication. This description will be followed by a discussion of the assurance in e-notification processes, where we will emphasise the authorisation facility used by some SBR chains.

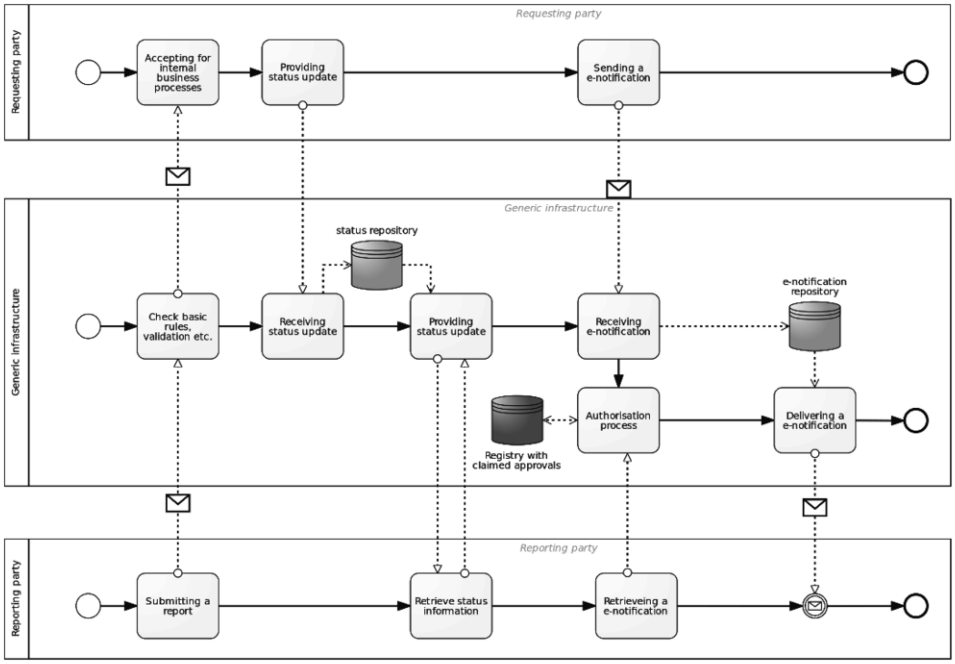


Figure 8.7 – Simplified representation of three typical secured I-processes

Push versus pull

From the perspective of the reporting party, interaction takes place in two ways: an information push (filing/submitting a message) and an information pull (picking up a message such as the status notification). The choice of whether to use a push or a pull depends on a number of factors. A push requires a stable and trusted delivery address (an endpoint) and a message handler such as a web service. Although the government might be expected to make the investments required for information exchange, the same is not necessarily true for the thousands of reporting parties. In addition, one wants to be sure in a push situation that the receiver really is who it claims to be. If a few requesting parties need to push a message to thousands of reporting parties, they would have to perform authorisation checks 'proactively' (for the push) and allocate trusted addresses to the reporting parties. The types of messages to be exchanged are another factor to be considered. The reporting party takes the initiative to send a message by choosing the information it wants to send and the moment for sending, taking into account any legal regulations on the message format (e.g., corporate income tax, financial statements for small or large businesses) and/or the period concerned.

While a reporting party can push a message to the generic infrastructure at any moment, a pull of information at any moment by the generic infrastructure is more difficult. For instance, reporting parties do not usually have a permanent online message box that can always be reached. Moreover, reporting parties may be represented by a

changing set of intermediaries. Most importantly, the generic infrastructure cannot automatically determine when the reporting party is ready to submit a message. Since many types of business reports can have consequences for the reporting business, submitted reports should include the consent/signature of the reporter. This implies that if Digipoort 'pulls' a report at a specific moment, the reporting party may deny that the report was ready for processing.

The difference between pushing and pulling information is also important when return flows are involved, in which messages are pushed to Digipoort by the requesting parties and pulled by the reporting parties. When the requesting parties are submitting return messages, Digipoort is continuously available for retrieval requests. Reporting parties cannot be expected set up a secure connection at any random moment that suits the administrative authorities, just so that they can receive a message. A pull offers the solution: the reporting party decides for itself when it will check the 'status repository' in Digipoort to see whether the requesting party has sent a message.

8.5.2 *Securing the information delivery process*

8.5.2.1 Setting up a two-way TLS connection

Any reporting party that wishes to submit a message via Digipoort must set up a secure connection over the Internet. In the Netherlands, several reporting software suites allow for this. Since the messages are being exchanged over the Internet (TCP/IP) and could thus be intercepted and altered, additional measures are required, especially considering the nature of the messages that are exchanged between reporting and requesting parties. Within SBR, it was decided to exchange messages via a two-way TLS connection (a tunnel) because this reflects an appropriate balance between the high-level of desired information security and the ease of implementation by software providers and reporting parties.

TLS is a mature and widely used standard that is supported by most software systems. Thus, the required knowledge is widely available. A TLS connection can be set up in various ways. SBR has chosen to use PKI-government service certificates. The 'two-way' attribute refers to a type of encryption in which both parties (the reporting party and the generic infrastructure) have a certificate. This means that the reporting party and the generic infrastructure need to identify themselves (using the certificate) and authenticate each other (by checking the other's certificate) before starting the exchange and processing of information. Two-way TLS ensures that both parties are who they claim to be.

In Chapter 7, the various functions of interface services were discussed extensively. For our purposes here, the following summary will suffice: an interface service specification describes how and under what conditions a connection can be set up between two systems. It contains logistical agreements for the correct addressing, reading, exchanging and processing of messages, as well as agreements for safe and reliable message transmission.

Communication with Digipoort can take place using various interface specifications, depending on message type and the party. For example, businesses can use SOAP2008 and WUS for Businesses (see Chapter 7). Governmental parties can use the ebMS interface specification. All of these interface specifications are based on open international standards, adding to the flexibility of electronic communication. SBR interface specifications contain agreements on:

- The safety protocol over which communication between the client and the server takes place (a version of TLS).
- The end-point (contact address) that must be included (an end-point in Digipoort is linked to one or multiple message types).
- The encryption standard to be used (e.g., RSA).
- The types of PKI-government certificates (from which domains and roots) that will be accepted during the connection.
- The message setup with mandatory fields, including the WS Security header. This is based on the web service security (WS Security) protocol, which also describes how a digital signature in a SOAP message is registered (Bertino, Martino, Paci and Squicciarini, 2010).

8.5.2.2 Use of PKI-government certificates in the delivery process

PKI-government certificates were chosen for SBR for a number of reasons, including their layered structure of requirements, strict issuing procedures for certificates and the stringent conditions CSPs must meet (see §8.3). These certificates therefore ensure a high degree of reliability and confidentiality in electronic data interchange. The choice of this existing and widely applicable system also aligns with the stated aim of SBR parties to reuse existing components whenever possible.

During message submission, Digipoort checks the integrity of the message, i.e. the validity of the digital signature. Furthermore, based on the CRL, Digipoort verifies with the CSP that a certificate has not been withdrawn. Using certificates assures Digipoort that the reporting party has undergone a number of checks on the claimed identity and has been issued a certificate by a CSP that is considered reliable. Since the currently recognised CSPs have an interest in only issuing certificates after having established the identity claimed by the applicant party (in order to maintain their reliable image), there is a reasonable degree of certainty about the authenticity of certificates used to sign messages.

Various types of certificates are issued under PKI-government. Service certificates in the organisation domain are required for information exchange via the generic infrastructure. In general, service certificates have three functions with regard to the security of message flows in SBR:

1. Setting up a two-way TLS connection with Digipoort.
2. Placing a digital signature in the WS security header of a SOAP message. This ensures increased certainty about the authenticity and timeliness of a message.

3. Placing a qualified electronic signature in the XBRL instance to verify the integrity of the instance document, enhancing end-to-end integrity. In practice, this function has not yet gained frequent use.

Functions 1 and 2 are mandatory when communicating with Digipoort. Function 3 is currently not a mandatory function and is not used much. However, in the future, Function 3 will be used more frequently when messages containing audit declarations are supplied via Digipoort (e.g., the financial statements of medium-sized and large businesses, for which an audit report is legally required). Such declarations must contain the auditor's signature. The auditor can use his personal professional certificate to place a qualified electronic signature.

Moving on, a filed report must always be signed by the reporting party using a PKI-government service certificate, as the use of this type of certificate for signing messages is technically accepted. Since these are not personal certificates, such signatures do not constitute qualified electronic signatures, but are rather considered as signing using a digital signature. The digital signature (which is an encrypted hash value – see §8.3.3) is calculated across the following specific fields from the SOAP message (see Chapter 7 for a detailed discussion of the SOAP message):

- The body.
- The header element 'Timestamp'.
- The header element 'WS-Addressing' (all elements).

Subsequently, the signature is included as the WS security element in the message header. This process results in the following:

- For the receiver: the possibility to check the integrity of the message.
- Certainty regarding the identity of the sender.
- Certainty for both parties regarding the moment of delivery.

The public key from the certificate used to place the signature must be supplied in the WS security header. When delivering the message to the requesting party, the plain text of the message (without the WS security header) is forwarded by Digipoort. Digipoort places a digital signature of its own on the message to reassure the integrity of the message from that moment until delivery to the requesting party. In the message submission process, the generic infrastructure records the identifying data from the certificate being used for message submission in the audit trail. This makes it possible to verify later on which certificate (from which organisation) was used to file a message and whether this certificate was used for justified or unjustified data interchange. If necessary, the requesting party can retrieve such information afterwards, as the retention period for the audit trail is five years. Furthermore, the processing activities for each message are also recorded in the audit trail. Digipoort stores the data based on a unique message identifier, which is also sent immediately to the reporting party (during the same communication session). The fact that the processes carried out by the generic infrastructure can be fully reconstructed safeguards both non-repudiation and transparency.

8.5.2.3 Identifying number in the certificate: OIN and HRN

Identification and authentication of government parties and businesses by means of certificates is not so obvious: how (in which field of a certificate) and with what identifying number should automated identification and authentication be realised? Looking into these questions once again reveals a challenge faced by SBR. Since the generic infrastructure should support several types of information flows to multiple requesting parties, there is a need for an unambiguous identifying number. Moreover, it is desirable for authentication in communications to be carried out using authentic data that can be consulted by services in the generic infrastructure. In the Netherlands, some administrative authorities possess authentic identifying data that is unambiguously recorded and its quality is being monitored. Looking to build on this, the SBR Programme decided to employ an authentication system that was already up and running: the Governmental Identification Number (or OIN in Dutch). This system ensures that various types of numbers can be included in a single format for use in digital certificates. This is done using a <prefix> and a <suffix> between which a <number> from the Trade Register[27] is placed, or—for government parties only—a number allocated by the SSC. The entire identification number is included in the certificate (subject.serialNumber field). Figure 8.8 below shows the structure of the identification numbers used in SBR for government parties and businesses.

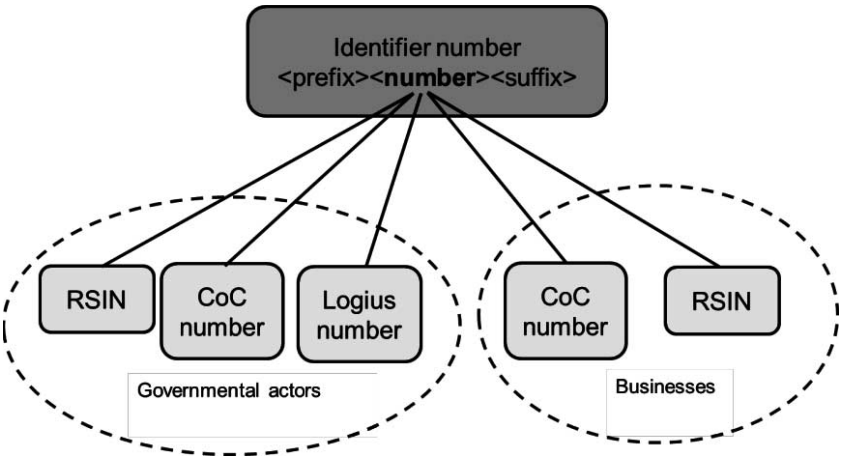


Figure 8.8 – The OIN/HRN system: an unambiguous format for identifying organisations, based on authenticated data from the government and business domains.

[27] In the Netherlands, registration in the Trade Register is compulsory for every company and almost every legal entity. This means that the Trade Register is able to provide reliable answers to questions like: does the company actually exist?

In practice, a government party's identifying number is referred to as an OIN and that of a business is referred to as an HRN (the Trade Register Number). This can be confusing, as the OIN can also be based on a number from the Trade Register. However, the distinction is needed because of the different procedures used to apply for certificates. To avoid confusion, we will use the term identification numbers (for both government agencies and businesses).
The difference between the OIN and HRN is explained in more as follows:.

- For government parties that are registered in the Trade Register, the <number> part of the identifier is derived directly from the RSIN (Legal Entities and Partnership Information Number, which is often the former fiscal number of the Tax Administration) or the Chamber of Commerce number.[28] Government parties that are not registered in the Trade Register will be allocated a <number> by the SSC. All governmental organisations are registered in the Digilink Service Register (DSR) with their identifying numbers. This facilitates the exchange of data between government agencies. The CSP verifies the identifying number using the DSR when an application for a certificate is made.
- Private organisations are identified based on a <number> in the Trade Register: their Chamber of Commerce number or their RSIN.[29] This number is checked by the CSP through consultation of the Trade Register.

The Citizen Service Number is not used in SBR
The Citizen Service Number (BSN) is not used as the <number> in PKI-government certificates. The BSN of entrepreneurs and heads of organisations (CEOs) is included in the Trade Register, but this number is not public. The BSN is intended as a personal number in the public domain and is therefore only accessible to government agencies via the Trade Register Act. Therefore, a CSP is unable to verify this number as identifying entity. As with other types of businesses, entrepreneurs always receive a Chamber of Commerce number, and SBR chains use this number in the PKI-government certificate. This solution fits with the current functions of the generic infrastructure, which is designed to support the information exchange between organisations and not between citizens and government.

[28] It is not clear whether OINs based on the Chamber of Commerce number are currently in use. The system makes it possible, as a prefix for Chamber of Commerce numbers has been defined, but the procedures for government parties in Digilink are based on either an RSIN or a number generated by the SSC.
[29]Various numbers are used for businesses in the trade register. The Chamber of Commerce number: the economic activity (the business); RSIN: the owner of a business, if the owner is a legal entity; BSN: the owner of a business, if the owner is a one-man business, or represents a person who holds a function within a business. The BSN is not a publicly available number; Office number: each branch or office of a business is given a unique 12-digit office number in the trade register.

To increase the certainty that a certificate offers, the identifying number is verified by the CSP when a certificate application is submitted and when the certificate is issued. In the delivery process at Digipoort, the supplier is identified by means of the identifying number in the certificate. However, this number is not re-verified. Nevertheless, the number can be used for reconstruction purposes later on. During the process, the validity of the certificate is also checked. A CRL check is performed to establish whether the certificate is still validly linked to an organisation. All parties that issue certificates are obliged to keep a CRL stating which certificates have been withdrawn, i.e. are no longer valid. This list must be updated by the CSP within 4 hours of a change. New or additional certificates for the same organisation may have the same identifying number but a different serial number. Organisations may assume that this number is correct as long as the certificate is valid (signed by the CSP, validity date that has not expired and not withdrawn).

Using the OIN/HRN system ensures that a certificate can be traced back to the organisation. This is crucial for realisation of the principle of non-repudiation within the SBR I-processes. Complementary to the practical security measures, the OIN/HRN system also has a protective effect against abuse. In principle, anyone who has a PKI-government certificate can submit a message. However, traceability based on the certificate holder's registration and the data in the audit trail guarantees the option of ascertaining the truth later on. As a result, it is less attractive to act in an unprofessional or dishonest manner using SBR messages (e.g., modification or fabrication, or submitting unjustified, corrupt or an exceedingly large number of messages). Furthermore, professionals (intermediaries, accountants) that support their clients in the business reporting process will effectively secure their own processes to avoid abuse on their account.

8.5.2.4 Between Digipoort and the requesting parties: Diginetwork

Specific Digilink interface specifications are used in the communication between Digipoort and the requesting parties, where the message exchange happens through Diginetwork. Digilink consists of interface specifications determined by the Standardisation Board. Diginetwork is the private network of the government that links governmental organisations with each other. Government parties can safely exchange data with other government parties through Diginetwork. The idea behind Diginetwork is to ensure that government parties (and their electronic services) can reach one other, irrespective of the physical government network they are linked to. The principle is that the requesting parties involved are known, operate professionally and are parties with whom one-time security agreements can be made and implemented. Within Diginetwork, PKI-government certificates are also used. Here, the OIN is used as the identifying number.

8.5.2.5 Security of the status request process

Picking up status information requires the same type of certificate as for submitting a message. With this certificate, the reporting party signs the request to

pull information regarding a report submitted earlier. In the status request process, it is checked whether the identifying number in the certificate is the same as the identifying number in the certificate that has been used to submit the report. This implies that persons cannot request status information about messages supplied using a different certificate (a different identifying number). As with message submission, Digipoort assumes that the identity of the requesting party can be retrieved at the CSP, based on the certificate that is deemed to be authentic. The actions relating to status information are not logged in the audit trail, since requests for status information regarding message delivery are frequently made. Thus, the logging of such actions has been deemed unnecessary.

8.5.3 *PKI-government*

Based on the resources discussed above, a number of governmental organisations were involved in developing the PKI-government component, or the PKI for the Dutch government. PKI-government is a framework of requirements and agreements that ensures the use of digital signatures, electronic authentication and confidential electronic communication based on certificates with a high level of trust. Technically speaking, there are a number of similarities between PKI-government and other PKI systems. However, a few aspects make PKI-government special:

1. The highest authority is the Kingdom of the Netherlands.
2. A layered requirements structure is used.
3. The certificates are classified by function.
4. Careful issuing procedures apply.
5. CSPs must comply with rigid requirements before they are allowed to issue PKI-government certificates.
6. The PA of PKI-government monitors the PKI-government suppliers.

Together, these special features make PKI-government certificates attractive for identification and authentication in electronic data interchange. We will explain each of these features in further detail.

Special feature 1: The highest authority is the Kingdom of the Netherlands

One major difference between PKI-government and other PKIs is that the highest authority in the latter is technically the root CA. In a commercial PKI, this could be a private party. For PKI-government, the highest authority is the Kingdom of the Netherlands. The Dutch government is responsible for the root certificate (root CA) and is therefore also responsible for the end point in the chain of trust. As a result, PKI-government does not depend on foreign commercial parties whose root CAs cannot be verified. The hierarchical structure of PKI-government is represented in Figure 8.9.

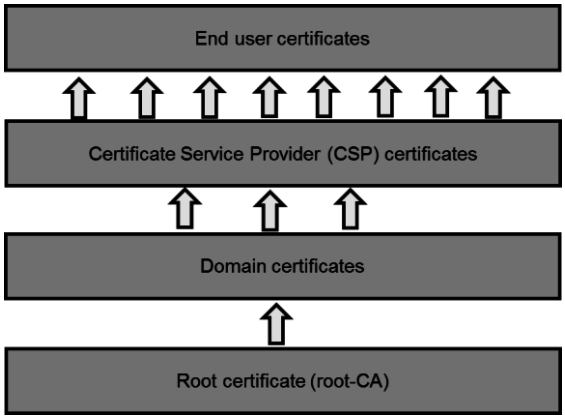


Figure 8.9 – Hierarchical structure of PKI-government, with the root CA being the Kingdom of the Netherlands

PKI-government is set up in such a way that governmental organisations and market parties can join the governmental PKI as certificate service providers (CSPs) under certain conditions. Participating CPSs are responsible for the service within the governmental PKI. The policy authority (PA) ensures the reliability of the entire PKI for the government. The PA function is performed by Logius.

Special feature 2: A layered requirements structure is used
Certificates issued in the PKI-government context have a layered requirements structure, consisting of the following:

- Legal requirements (abstract requirements from Directive 99/93/EC, *Besluit elektronische handtekeningen* and *Telecommunicatiewet*).
- Technical non-legal requirements (ETSI: European and international standards of the European Telecommunications Standards Institute)
- Specific PKI-government requirements
- Specific domain requirements within PKI-government

All qualified PKI-government certificates must comply with the legal requirements for qualified certificates. Directive 99/93/EC 30 (including annexes), the *Telecommunicatiewet* and the *Besluit elektronische handtekeningen* each impose specific requirements on the certificates and on the certificate service providers that issue them. According to these regulations, the following must be included in qualified certificates:

- A statement that the certificate is issued as a qualified certificate.
- Identification of the issuing CSP and the country where this SP resides.
- Name of the signatory or a pseudonym (identified as such).

[30] A new regulation is currently being drawn up: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

- Room for a specific attribute of the signatory, which can be stated if necessary and if required for the purpose of the certificate.
- Data to verify the signature, corresponding to the data used for the creation of the signature, which are under the control of the holder.
- Start date and end date of the certificate's validity period.
- The identity code of the certificate.
- The advanced electronic signature of the issuing CSP.
- Where applicable, restrictions regarding the use of the certificate.
- Where applicable, limits on the value of the transactions for which the certificate can be used.

Special feature 3: The certificates are classified by function
Within PKI-government, certificates are divided into 3 domains: 1) the organisation domain, 2) the domain citizen and 3) the autonomous devices domain. Various types of certificates can be issued within each domain (including ones for digital signatures, authentication and confidentiality). The technical requirements are different for each domain. Figure 8.10 below provides an overview of the functional classification of certificates.

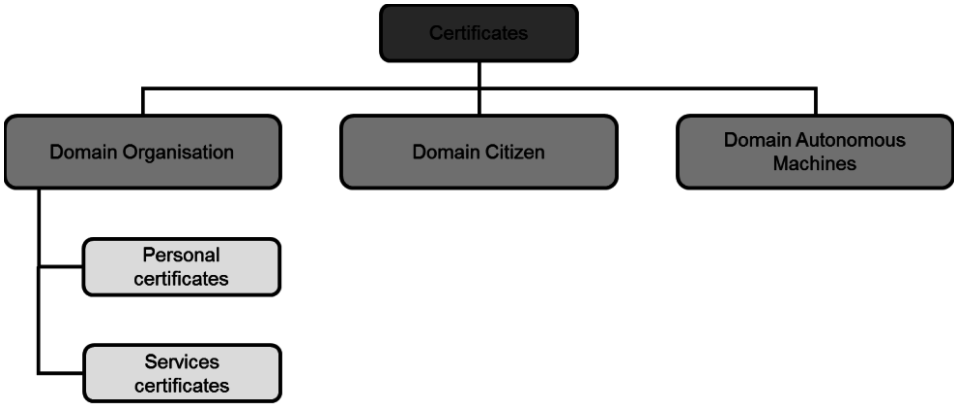


Figure 8.10 – Domains and types of certificates in PKI-government (technical requirements vary for each domain and type)

The certificates in the organisation domain are of particular interest for this chapter. There are two types of certificates within this domain: personal certificates and service certificates.

Personal certificates are related to an individual and one person may have multiple personal certificates. A variant of the personal certificate is the professional certificate, which requires that a person be registered with a recognised professional organisation. Recognised professions that allow for the application for a professional certificate include, for example, accountants, accounting consultants, lawyers and physicians. By using a professional certificate, accountants can identify and authenticate themselves as qualified accountants who are listed

in the official register. They can also sign a document or e-mail using an electronic signature to assure non-repudiation, and if necessary, add a digital signature with the same legal consequences as a handwritten signature, i.e. a qualified electronic signature. Finally, they can also use these certificates to guarantee confidentiality by encrypting the messages. Professional certificates are currently used in various private processes. They are not yet used in the public domain.

Service certificates are related to a system rather than a person and are sometimes referred to as system certificates. These certificates may also be linked to a function. In §8.4, we will explain the use of services certificates in the context of SBR.

Special feature 4: Careful issuing procedures apply
PKI-government uses more rigid conditions for the issuance of certificates than PKI systems not working with qualified certificates. One of the conditions imposed by PKI-government on the issuing of qualified certificates is that the user must physically identify himself to the CSP. These conditions do not only apply for personal certificates, but also for certificates at the organisational level. PKI-government aims to create a single high level of trust for all types of certificates. PKI-government certificates can be applied for at CSPs in the Netherlands.

The various CSPs use different procedures for a certificate application. However, in general, such a procedure consists of three steps:

1. The organisation must be registered with the CSP as a subscriber.
2. Certificate managers are appointed as the first point of contact for the CSP.
3. An application form is used to apply for a specific certificate with the CSP.

For the withdrawal of a certificate, certificate holders must contact the CSP and request a withdrawal. The requirements imposed on the CSP for issuing and managing these certificates are defined in the PKI-government Programme of Requirements (http://www.logius.nl).

Special feature 5: CSPs must comply with rigid requirements before they are allowed to issue PKI-government certificates
Within PKI-government, CSPs issue certificates to end users. CSPs must thus be included in the hierarchy of the PKI-government to ensure they can issue PKI-government certificates. In practice, this means that the public key of a CSP is signed by the governmental PKI's domain CA. In order to guarantee the reliability of the governmental PKI, CSPs must meet rigid PKI-government requirements regarding their operational processes, technical resources, information security, expertise, reliability of staff and information supply to their audience. The specific requirements that a CSP must meet before being allowed to issue certificates within PKI-government are stated in the PKI-government Programme of Requirements.

To ensure the continuous reliability of PKI-government, CSPs must continue to meet the requirements imposed on them even after their entry into PKI-government. To ascertain that this condition is met, the PA monitors new CSPs. The CSPs must also submit proof of conformity periodically.

Special feature 6: The Policy Authority (PA) of PKI-government monitors the PKI-government suppliers (CSPs)

The PA checks the extent to which the CSPs meet the requirements of the PKI in question. The PA is sometimes also referred to as a supervisory body. However, this is not a legally prescribed role with coercive measures and instruments (such as the role of the Authority for Consumers and Markets (ACM) in the Netherlands). Instead, the PA has a controlling role that checks whether the agreements and procedures in the PKI agreement system are being observed. This kind of monitoring consists *inter alia* of the following elements:

- Annually, the policy authority allows a third party to run penetration tests on the IT environment of the CSPs.
- Together with the ACM, the PKI-government PA visits the CSPs each year to discuss the findings of the external auditor's audit report.
- The PKI-government PA visits the CSPs once or twice a year to check whether new requirements from the Programme of Requirements have been implemented and if so, how it has been done.

Intermediary conclusion

The use of encryption and its effectiveness in security depends on whether the management of keys and certificates has been properly established. A PKI system is required for the appropriate establishment of certificate management. Here, 'appropriate' means 'in line with the relevant legal, technical and domain requirements.' Strict measures have been taken for PKI-government to ensure that the requirements are met. PKI-government certificates therefore guarantee a higher security standard for electronic communication with the government than non-PKI-government certificates. Assuming that the keys are managed appropriately, the certificates represent a strong instrument for identification and authentication. Due to the option of attaching a digital signature, it can be established with a high degree of certainty who the sender of the message is. High degrees of integrity and non-repudiation are also ensured. In other words, it can be established that the message has not been changed *en route* and that the transmission of the signed message was initiated by the owner of the private key, as he is the only one who has access to this key. Again, the degree of certainty depends on the quality of the key management. One issue that has not been solved sufficiently by a PKI is authorisation (and therefore, exclusivity; we will explain why in the third part of this chapter). Is a person or organisation authorised to send a message or to see the response? The following section describes a generic component that solves this issue: an authorisation facility.

8.5.4 *Securing the e-notification process*

8.5.4.1 Use of an authorisation facility

The e-notification process (see Figure 8.8) involves the exchange of return messages (e.g., a Tax Assessment Service Message) from a requesting party to a business or intermediary through Digipoort. A number of internal sub-processes are performed, such as the processing and preparation of the notification in Digipoort. We will not discuss the internal sub-processes within Digipoort. Instead, we will focus on the following sub-processes:

1. Supplying the e-notification from the requesting party.
2. Requests for e-notifications by an authorised intermediary.

The first sub-process involves the exchange of data via Diginetwork. Pursuant to its legal obligations, the requesting party sends Digipoort an e-notification that is intended for the reporting parting. The remainder of this section will concentrate mainly on the second sub-process, which uses an authorisation facility. A few design aspects of the authorisation facility have already been discussed in §8.3.

8.5.4.2 Authorisation for retrieval requests

E-notifications contain confidential information from the government that is intended for one specific party and which can have legal consequences. Examples are e-notifications containing tax assessments, provisional assessments or Tax Assessment Service Messages. It is extremely important to prevent interception of such notifications. Even if PKI-government certificates are used, and even if the government has a high degree of certainty about which party it is dealing with, it does not know, for example, whether a party is entitled to retrieve a Tax Assessment Service Message for another interested party. To ensure a high degree of exclusivity, it was decided to use the authorisation process for Tax Assessment Service Messages. Considering the principle of care, the government wants to establish beforehand whether the retrieving party is indeed allowed to retrieve these messages. Whether or not a party is authorised will become clear after an authorisation test, which checks—as part of the retrieval process—whether an authorisation relationship exists. Authorisation relationships are recorded in an authorisation registry.

The retrieval process for e-notifications consists of two steps. In the first step, the identifying number in the certificate is used to check which interested parties (fiscal numbers, citizen service numbers or RSINs) the retrieving party is authorised to retrieve information for. After that, a list of references to the e-notifications concerning the interested party in question is composed and sent to the authorised retrieving party (in a single session). In the second step, the authorised party submits a request containing the reference to the e-notification it wishes to retrieve. The authorisation facility then uses the identifying number of the retrieving party's certificate to check whether a valid authorisation exists

for this message. After these steps have been completed successfully, the retrieving party will receive the e-notification. This setup ensures firstly that unauthorised persons cannot inquire, on behalf of random parties, whether there are any messages or what authorisations exist. Secondly, it ensures that unauthorised persons cannot retrieve these messages. Furthermore, the second step includes a real-time check of whether an authorisation is still active (to confirm that it has not been withdrawn in the meantime). Thus, the authorisation is checked both when the list is queried and when the retrieval of the notification is requested.

Additional guarantees are obtained using a few design principles. For example, there are rules covering the scope of an authorisation: approvals are recorded for a specific client (represented party) and a specific service. This way, if interception does occur, it will only involve one or a few messages for one specific client and service. The authorisation itself is verified (an re-verified each fiscal year) with the represented party (the company with reporting obligations). Accordingly, any unauthorised filings or status notification pulls will not go unnoticed. Furthermore, the Tax Assessment Service Message may only be retrieved once, after which it become unavailable. Possible interceptions can thus discovered when the authorised accountant tries to retrieve the assessment and fails to obtain it. The identity of the intercepting party is then established through the relevant PKI-government certificate.

8.5.4.3 Audit trail

As stated earlier, all data interchange within SBR is recorded in an audit trail. The time and result of each activity in the data delivery or retrieval process is registered. The same also applies to the result of the authorisation registry check. The audit trail thus increases the transparency and non-repudiation of the actions with respect to the authorisation registry and the notification process.

8.5.4.4 Monitoring

In addition to the many preventive measures for information security, detection also plays a role. We have already seen this principle in the reconstructions that can be performed at message level using the audit trail and the certificate data. At an aggregated level, monitoring ensures the detection of security incidents. The data exchange and processing by the generic infrastructure is continuously monitored. Unusual activity patterns and increased volumes could raise suspicion, and the relevant parties can then check whether the data interchange is legitimate. Daily reports of all messages sent and received through Digipoort are composed and sent to the relevant requesting parties. These reports also list error notifications and any abnormal status notifications. Depending on the features of the messages in question, the requesting party demands a certain frequency and level of detail in these reports. Less strict reporting requirements are imposed on messages that are supplied in small numbers during the year

than on peak flows (large numbers supplied within a short period). The development of a dashboard for real-time monitoring of the I-processes is underway to ensure immediate detection of errors.

Service levels have been agreed upon between the chain parties regarding the continuity of chain facilities. The SSC monitors the service levels using the service level agreements (SLAs) and ensures that these are met.

8.5.5 *An authorisation facility*

8.5.5.1 The need for an authorisation facility

Communication requires at least two communication partners: a sender and a receiver. It can also involve an intermediary that is authorised to act on behalf of one of the communication partners. Intermediaries often become the communication partners in place of the stakeholder to whom the information relates. This raises issues about authorisation in the I-processes: is a person authorised to perform certain actions? The answer is difficult to determine if the interested party is absent. It is cumbersome to check for each information exchange whether the interested party is using an intermediary and if so, which intermediary it is and what actions it is or is not allowed to perform on behalf of the interested party. It is also quite a burden for the interested parties who were trying to outsource their workload to intermediaries in the first place. The dilemma is that, from the perspectives of exclusivity, authenticity and non-repudiation, such an authorisation relationship should be checked. This should be done in a manner proportional to the type and purpose of a message. To believe anyone who claims to be an intermediary on behalf of someone else without any proof of a valid authorisation relationship is not an option. Otherwise, malicious parties could obtain confidential information.

How can such an authorisation relationship be checked? What procedures and resources are required? These are just a few questions regarding the authorisation issue that the SBR Program was faced with. There were no off-the-shelf components available that satisfied the imposed requirements. Therefore, a new component was developed: an authorisation facility. This facility includes a registry with stored approvals: permissions that embody an authorisation relationship between the represented party and the intermediary. It also includes automated procedures for storing, verifying, modifying and removing approvals in the registry. For some predefined SBR messages, the authorisation service checks whether or not a message should continue to be processed based on the approvals in the registry. If there is no approval registered, further processing is halted. This component needed to be set up in a generic manner in order to be used for several S2S I-processes. The design of this authorisation facility will be described in the next section.

The role of the intermediary in reporting chains
A business can decide to handle its administration itself and thereby comply with all the administrative obligations imposed by administrative authorities. It can also choose to outsource these tasks to one or more specialist intermediaries. One task that is often outsourced is salary administration, in addition to the bookkeeping and subsidy applications. When a business chooses to outsource various tasks, its intermediary must be able to act on its behalf. The business 'authorises' the intermediary (see 'representation by an authorised person,' Art. 2:1 of the Awb, and 'mandate,' Art. 3:60 of the Dutch Civil Code). The government must be able to recognise such an intermediary and determine whether the intermediary is indeed authorised to perform the actions concerned. This applies to both submitting information to, and receiving information from, the authorities. Due to the confidential nature of the information, it is important that return information is only made available to the authorised intermediary. Therefore, the chain requires functionality that can be used to determine whether an authorisation relationship exists between the intermediary and the interested party to which the information being supplied or returned relates.

8.5.5.2 The design of the authorisation facility

The following five design aspects of the authorisation facility will be explained in detail:

I. The setup: a central authorisation facility.
II. The authorisation procedures.
III. The scope of the authorisations (recorded in the approvals).
IV. Registering an approval.
V. The authorisation processes.

Starting with the setup of an authorisation facility, two types of authorisation facilities can—in principle—be distinguished: centralised and decentralised (Kizza, 2009). Decentralised authorisation facilities have a distributed setup, with multiple approval registers that are managed by various organisations. These individual registries jointly form a single service. The approval registry is what is referred to in literature as an 'access control list.' It is a database containing approvals that link a party being represented to an authorised intermediary. The generic infrastructure does not use a decentralised authorisation facility because there is currently no need for it. In addition, designing and maintaining a decentralised setup requires a high degree of coordination. As a result, a central authorisation facility was chosen. A centralised authorisation facility has one approval registry and one managing organisation. Its setup is simple and can be designed and maintained easily.

The second design aspect concerns the authorisation procedure. The authorisation facility has three recurring actions for administering changes in the approval registry:

- Entering the approval
- Verifying the authorisation relationship claimed in the approval
- Withdrawing the approval

With the first action, intermediaries can claim to be authorised through a S2S submission of an authorisation claim to Digipoort. The second action, verifying the authorisation relationship, consists of a notification to the represented party with an opt-out option and a response period, after which the status of the approval is changed to active. The approval becomes active when the claim has been verified by the represented party (client) with reporting obligations. The relationship between a represented party and an intermediary can change because of various reasons (e.g., the represented party moves to a cheaper intermediary). Therefore, an approval is temporary and the verification process is repeated annually. With the third action, it is possible to withdraw an approval that was entered earlier. The approval can be withdrawn in a S2S manner by the party that had it registered (the service provider). The represented party also has the option of withdrawing the registered approval, or having it withdrawn, e.g., in the event that the relationship with its intermediary changes. This can be done by a letter (with a verification code) to the SSC.

The generic infrastructure uses PKI-government services certificates for identification and authentication when entering and withdrawing recorded approvals. It uses authenticated registries such as the Trade Register for verification of the authorisation and the party being represented.

The third design aspect is the scope of the recorded approval. The scope covers aspects such as the service, the timeframe and the types of actions that can be performed. The service can be defined broadly (comprising multiple types of messages) or narrowly (one specific type of message). The timeframe of the approval can vary from a variable period to a fixed period to an indefinite period. A longer timeframe is easier for users, but extends the time between the expression of intent to create an approval and the termination of that approval. Therefore, the represented party may forget that the approval is still registered. It is obvious that for SBR chains – in which confidential information with potential legal consequences is exchanged – there should be a limited period and a separate approval for each type of business report.

The fourth design aspect is the registration of the approval. The moment that an intermediary wants to act on behalf of a business, it is verified whether it has been permitted by that business to perform those actions. The authorisation facility makes it possible for Digipoort to check automatically—for each action by the intermediary—whether the required approval has been issued.

An approval consists of a combination of three components: the authorised party, the represented party and the service. As a result of an approval and the verification thereof, the authorisation facility registers an approval as ‘active’ or ‘valid’. After withdrawal or when the service has expired, it registers an approval as ‘non-active’ or ‘invalid.’ Another status may be assigned.

Possible statuses for approvals are shown in Table 8.2.

Table 8.2 – Possible statuses of an approval

Status	Description
S0	Does not exist in the registry
S1	Pending
S2	Rejected (final status)
S3	Active
S4	Not active (final status)

The transition from one status to another requires an activity. These are provided in Table 8.3.

Table 8.3 – Activities that trigger a change in the status of an approval

Activity	Trigger
A1	Entering an authorisation claim (approval)
A2	Rejection of an authorisation claim because the authorisation claim is non-verifiable
	Rejection of the authorisation claim after a letter from the represented party.
	Withdrawal request by authorised party (the intermediary)
A3	Status becomes automatically active after 19 calendar days, in the event of a lack of response by the represented party
A4	Service has expired
	Withdrawal request by authorised party

Status transitions, in relation to the activities, are illustrated in Figure 8.11.

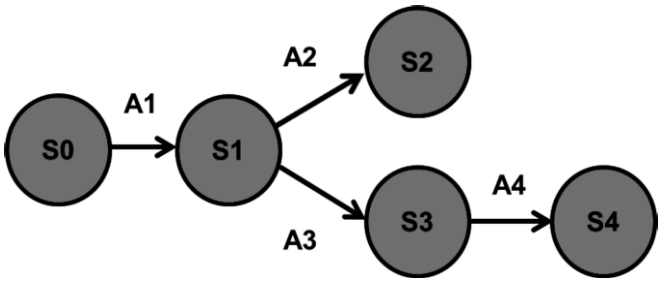


Figure 8.11 – Status transitions (S) for approvals resulting from certain actions (A)

The generic infrastructure is informed, via a signed electronic message from the authorisation facility, whether the claimed relationship appears in the approval registry or not. Digipoort only forwards messages (filed messages, certain status information or notifications) if the relationship has been registered and the approval is still active. In addition, it is not possible to record a second approval for the same service and the same represented party. This creates a higher level of exclusivity, which is appropriate for confidential messages. The approvals are

recorded in a centralised and secure registry. Only specific I-processes have access to this registry, with specific access rights that depend on their function.
The fifth design aspect involves the authorisation processes, which refer to the automated actions performed by the generic infrastructure to check whether a specific authorisation is active. One focus in the registration processes is the question of what information is provided to the authorised party. The principle of data minimisation is followed, meaning that the authorised party receives no more information than it should know for its own processes. Accordingly, Digipoort never provides new information from the authorisation facility. For example, when a certain party requests information on behalf of a represented party for which it has no active approval, it will only be informed that the approval does not exist. It will not receive any information about which intermediary is currently authorised by the represented party.

8.6 Chapter conclusion

The future of information security in chains remains clouded by numerous uncertainties. However, two things are clear: chain information systems are vulnerable and motivated attackers are always ready to exploit these vulnerabilities. The SBR case demonstrates that when the risks and the requirements imposed by law are understood and acknowledged by chain parties, effective measures can be implemented to safeguard end-to-end security in information chains.

This chapter has discussed three key security measures in SBR chains: identification, authentication and authorisation. These measures can be viewed as continuous processes that use several security components (e.g., cryptography, digital certificates, an authorisation facility). Together, these measures ensure that more chains and larger message volumes can be processed safely in the next few years. However, the parties participating in SBR chains must also have internal security measures and security policies in place. This implies that daily/generic IT security mechanisms such as firewalls and intrusion detection must be up and running. Parties' information security management systems must be in effect and up to date. The chain partners themselves thus have a paramount role to play in achieving sufficient information security.

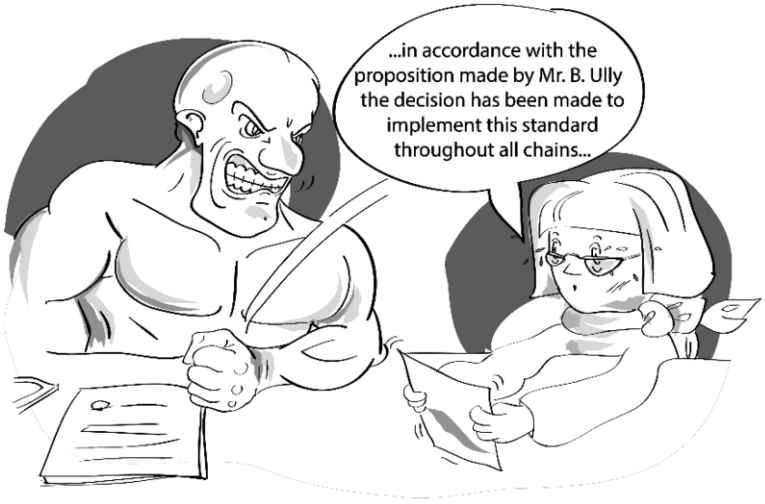
Furthermore, the I-processes include measures that strengthen information assurance. For example, validation as part of the message submission I-process ensures that only instances in XBRL or XML format that are based on the Netherlands Taxonomy will be processed. This greatly reduces the chance that malicious code will be received, processed and delivered to the requesting party. The fact that the measures taken in SBR chains are generic and are also used for information exchange with the Tax and Customs Administration, implies that the measures meet the highest possible requirements. This means that I-processes with less strict requirements (e.g. for non-confidential messages) can benefit from the high degree of security required for other message types. One example is the use of PKI-government certificates for very confidential and less

confidential interactions with the generic infrastructure. A differentiated range of security offerings for particular chains is only possible to a limited extent. For instance, in choosing whether to use the authorisation facility.

Despite all the measures implemented thus far, it must be emphasised that there is no such thing as 100% information security or information assurance for that matter. An effective approach demands an ongoing assessment of evolving threats and a review of the implemented measures. Internal and external/chain circumstances are subject to change, so 'finished' measures may require updates. When (re)designing measures, the principle of proportionality should be taken into account, so that there is a balance between the (lawful) goal of the message exchange and user-friendliness.

Since prevention can fail, it is also important to ensure early detection and to respond appropriately to security breaches. Dashboards, monitoring policies and incident management procedures are important additional safeguards. As final point, it is vital to perform end-to-end tests periodically, especially before implementing changes (e.g., updates, new interface specifications, etc.) so that new vulnerabilities do not go unnoticed.

9 Governance and Service Management



Chapter highlights

- Capturing the principles for governance
- Illustrating SBR's current governance from a horizontal, vertical and network perspective
- Introducing the service management triangle

9.1 Introduction

Standard Business Reporting (SBR) links the information systems of different organisations together to form a coherent and functional reporting chain. The result is referred to as an 'SBR chain.' Currently, several SBR chains are in production, meaning that they are fully operational in terms of automated information exchange and processing. Government agencies such as the Tax and Customs Administration use SBR chains for automated, system-to-system (S2S) information exchange with thousands of reporting parties. As was discussed extensively in Chapter 1, S2S information exchange increases the level of interdependency between all parties that form the chain. Chapter 1 concluded that the proper coordination[31] of such interdependencies was a neglected aspect of the SBR solution in its preliminary form. When addressing the issue of how to or-

[31] We use the definition of Malone and Crowston (2004) who define coordination as "a process for managing interdependencies between activities" (p.87).

ganise such coordination, we specifically refer to the creation of an 'SBR governance' and the formation of a Shared Service Centre (SSC)[32]. Drawing on the working definition presented in Chapter 4, governance refers to the solutions that individuals and organisations devise for problems of coordination. The goal of this chapter is to provide a comprehensive description of the SBR governance and the functions of the SSC. To do so, we should distinguish three types of integration that are at play:

1. *Horizontal integration* of reporting chains by means of inter-organisational S2S linkages between organisations.
2. *Vertical integration* using a SSC that is involved in several S2S chains. The SSC acts as an intermediate chain partner and provides shared services and standards to reporting and requesting parties.
3. *Network integration* through the use of international standards when integrating various S2S chains. This form of integration also covers the use of SBR-specific standards in other, non-SBR information chains.

As a whole, the SBR solution can be considered as a standard for all three types of integration. Each type has distinct coordination needs and the SBR governance should fulfil these needs. The following sections discuss these integration types and coordination needs in further detail. Please note that this chapter is focused mainly on the application of SBR in reporting chains that are rooted in legislation and regulations.

First, let us elaborate on the need for coordination in horizontal system-to-system integration. Figure 9.1 provides a simplified overview of horizontal integration, without an SSC.

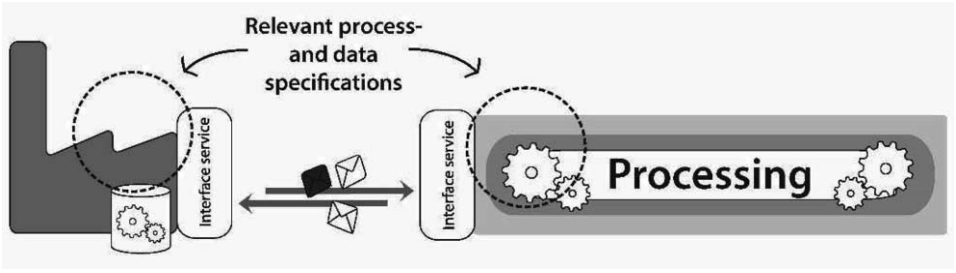


Figure 9.1 – Horizontal integration of the reporting chain

Consider the example of filing business taxes. Reporting parties, software providers and tax specialists can connect their systems directly to the government systems for specific types of tax declarations. These system-to-system linkages

[32] In the Netherlands, Logius is the SSC for the public SBR domain. Logius works for various ministries and executing agencies in the management and development of services and standards. This chapter focuses on the services offered for reporting chains.

can only work when reporting parties and software providers have implemented the required specifications on time.

Since tax legislations are subject to change and technical issues may arise, it should be possible to implement a change in the specifications in all systems within a short timeframe. The way that a change is implemented can have a major impact on the parties sending in business reports. For a tax specialist, who may be responsible for thousands of tax declarations, it is essential to know when and how such a change is handled. The same applies to software providers that may need to play a large role in the implementation of a change.

It is in the interest of both the requesting party and the reporting party that they are able to interact and communicate with the systems as efficiently as possible. That is why, for instance, the Tax and Customs Administration and the other stakeholders in the information chain meet on a regular basis to discuss intended decisions or to consult each other about how to deal with the change process. In Chapter 1, we discussed how the reporting parties, their software providers and their tax specialists also need to align efforts in order to ensure that a SBR chain works properly.

The second type of integration is vertical integration. In Figure 9.2 below, an SSC stands between the reporting and requesting parties. Consequently, the requesting parties that share the services provided by the SSC depend strongly on the SSC for system-to-system information exchange and processing.

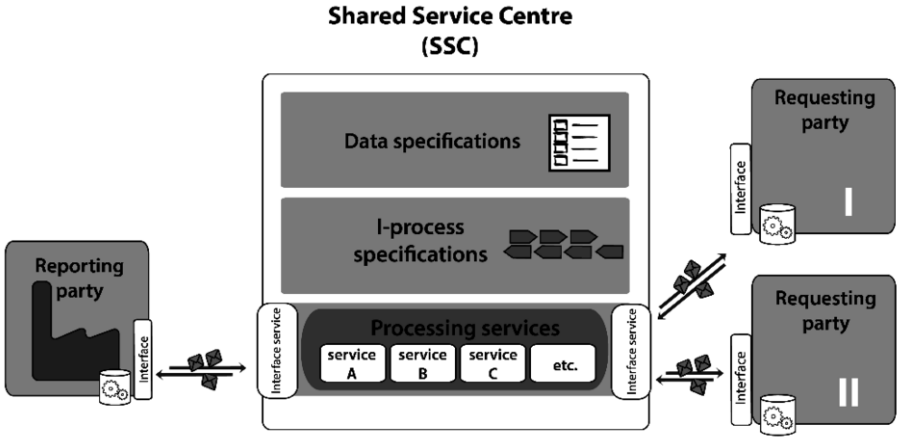


Figure 9.2 – Vertical integration of the reporting chain

Figure 9.2 depicts only a single reporting party that is linked with the SSC in a S2S manner. In practice, there can be thousands of information providers in a given SBR chain. This highlights the interdependencies created through horizontal integration. In the public domain, the SSC will be more efficient when it maintains a single/generic set of specifications and processing services for all the reporting and requesting parties in the various SBR chains. More variety means

more development and maintenance costs. More variety also implies that I-process specifications and data specifications that can be used in several reporting chains need to be in place. The requesting parties need to acknowledge this fact and agree on minimizing variety and sustaining genericity. If agreement cannot be reached, actors must decide who will bear the additional development and maintenance costs for new interfaces and/or processing services.

Obviously, the requesting parties should be able to employ the generic information processing services offered by the SSC to facilitate their own internal business processes. Other questions that arise are what service levels the SSC can offer for handling the information processes. How is the SSC helpdesk function organised? The SSC can operate more cost-effectively and offer higher service levels if it is able to perform tasks for several requesting parties in a standardised way. Nevertheless, for some requesting parties, customisation can be more attractive or even necessary. The coordination in terms of vertical integration will often spark discussions about whether or not the standard specifications and services offered by the SSC are adequate for all requesting parties. This might lead to the decision to develop 'special' services or extend the standard service offering. In the case of such additional offerings, the question of who will bear the cost needs to be addressed.

The third type of integration is network integration. It is important to distinguish two perspectives in this regard. On the one hand, SBR employs standards (e.g., BPMN, SOAP and XBRL) that are developed and managed outside of the SBR community. These are, in fact, open international standards. Agreements about which standards are used and how they are used in SBR chains are laid down in the SBR framework of agreements. On the other hand, SBR itself includes several standards (e.g., the taxonomy, interface specifications) that can be at least partially used by actors in other/non-SBR information chains. Figure 9.3 illustrates the situation in which SBR standards are used in multiple types of information chains, with or without an SSC.

The broader (network level) usage of SBR standards for information exchange creates network effects for reporting and requesting parties (also known network externality or demand-side economies of scale). When a network effect is present, the value of a product or service is dependent on the number of parties using it. The typical example is the telephone: the more people who own telephones, the more valuable the telephone is to each owner. This creates a positive externality because a user may purchase a telephone without intending to create value for other users, but does so regardless. Accordingly, SBR 'products' (standards) can be used in a single, horizontally integrated business reporting chain as well as in business-to-business information exchange, with or without an SSC. In the Netherlands, this can be seen in the banking domain.

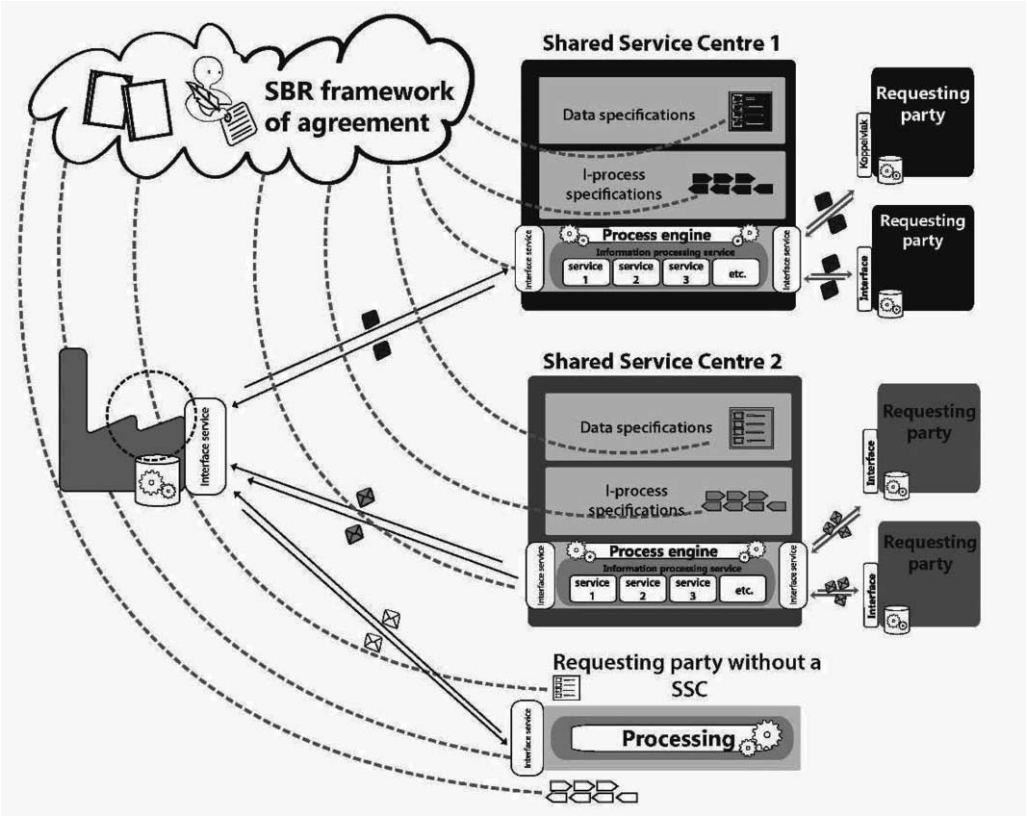


Figure 9.3 – Network integration

Basically, all SBR business reporting chains use the framework of agreements as the basis for setting up system-to-system information exchange and processing. In this context, all parties involved in reporting are stakeholders in the framework of agreements. These agreements made at the overarching level largely determine how much autonomy the parties have when setting up their own reporting chains. There are some restrictions. For instance, the framework of agreements states that any party creating a taxonomy must comply with the prescribed XBRL standards and the architecture of the Netherlands Taxonomy. However, the framework does not dictate what elements the parties are allowed to request. Nevertheless, the boundaries between 'what' and 'how' may be blurred.

The necessity for a change in a horizontal chain may affect other forms of integration. The same applies the other way around: a change in the framework of agreements may have substantial consequences for the horizontal chain. This is why the SBR solution requires chain governance for the various integration forms, as well as overall governance and coordination to manage the interdependencies. Chapter 4 discussed in depth the notion of chain governance, referring to the agreements between the parties about who will be involved and how

in decisions regarding aspects that determine the interdependencies within the chain. This chapter will discuss how the governance of SBR along with public involvement has been organised. It will also discuss how Logius, as an SSC, has organised service management within SBR. The remainder of the chapter is organised into three parts:

1. The first part outlines the principles for governance with regards to the three forms of integration. The topics covered include the following:
   a. Generic principles for governance (**section 9.2**). Public agencies should always stick to certain rules in everything they do. This also applies when setting up or taking part in governance. These generic principles are derived from the frameworks for good governance.
   b. Specific principles for the governance of each chain integration form:
      - Horizontal integration (**section 9.3**)
      - Vertical integration (**section 9.4**)
      - Network integration (**section 9.5**)

      For each form of integration, we will discuss the aspects the concerned parties should agree upon in SBR: 'what is on the agenda?' We deliberately use the vague concept of an 'aspect' here, as the relevant variables are not necessarily comparable between integration forms. Overall, the characteristics of SBR chains for the three integration forms define the coordination agenda for the SBR forums. For example, at the network level, a key question is whether or not SBR should be compatible with Digilink. A possible question regarding vertical integration is what pricing model Logius should employ for its services. Both questions—though very different in nature—are on the agenda of the SBR forums and are relevant for the implementation of SBR. We shall describe the principles for each integration form as they apply to the chain governance, given the characteristics of SBR.
   c. **Section 9.6** elaborates on the coherence of the governance over the various integration forms.

2. The second part of this chapter starts with **section 9.7**, which provides a detailed description of SBR governance in its current form. Over time, the SBR governance has been shaped by the emerging needs for coordination and agreements. Through agenda setting and differentiation between the public-private and the purely public components of SBR, the integration forms were taken into account. It is important to note that the established governance structure is still evolving.

3. The third part of this chapter (**section 9.8**) reflects on the essential role played by the SSC in terms of ensuring that the governance is operational, effective and consistent. The SBR Programme has defined an appropriate service management model for Logius that enables it to fulfil its role as an SSC in a cost-effective manner. The chapter concludes with a broad outline of this service management model.

9.2 Generic principles of governance

Government agencies that initiate or take part in the governance of SBR chains are subject to the legal frameworks for good governance. Good governance is a democracy-intensifying concept that looks to make public administration more open, transparent and accountable. Due to the involvement of government agencies in SBR, the principles of administrative law determine the relationship between the government, and citizens and businesses.

The following principles apply:

- The precautionary principle. When preparing decisions, public agencies gather the required knowledge, including the relevant facts and interests to be considered (Article 3:4 paragraph 1 of the Awb[33], translated: General Administrative Law Act). A public agency weighs the interests of the stakeholders who will be affected by a decision. One way to do this is to hire a specialist to advise on choices related to the design and setup of SBR chains. Another option to ensure that all stakeholders are given the opportunity to express their opinions and concerns regarding SBR-related developments.
- The principle of proportionality / prohibition of arbitrary decisions. The consequences of a decision that are disadvantageous for one or more stakeholders should not be disproportionate in relation to the objectives of the decision (Article 3:4 para 2 of the Awb[34]). This is also referred to as 'proportionality of objectives and means.' In addition, the policy should be consistent and not be based on random factors. Proportionate representation of all stakeholders in the public-private SBR forums can help safeguard this principle.
- The principle of equality. Identical cases are to be handled in the same way. The meetings and procedures of the forums should guarantee that all members are allowed to express their opinions (equal treatment in coordination discussions). Safeguarding the principles mentioned so far requires that all other groups without direct representation in SBR forums (e.g., minority interests, small groups with extraordinary requirements) be given the opportunity to express their ideas and concerns. This form of inclusion can be implemented, for instance, through written appeals. Additionally, groups without direct representation should have access to the supporting SBR services (i.e. connection support and application support). The support provided in the context of SBR should satisfy

[33] Article 3:4 paragraph 1 Awb: "An administrative authority shall consider the interests directly affected by a decision, subject to any limitations following from a provision of law or the nature of the power to be exercised."
[34] Article 3:4 paragraph 2 Awb: "The adverse consequences of a decision for one or more interested parties may not be disproportionate to the objects to be served by the decision."

the needs of these other groups to the same extent that the needs of stakeholders exerting more influence in SBR forums are satisfied.
- The principle of transparency. Transparency requires the publication of government documents, as well as the ability of all involved to access to these publications, express their opinions, and be heard. Information regarding the preparations for decision-making as well as the outcome should be available to the public.

The above listed principles should be taken into account when allocating tasks, responsibilities and authorisations to the SBR forums.

9.3 Governance of SBR reporting chains: horizontal integration

Horizontal integration occurs when human/manual operations (i.e., data rekeying) are minimized in the chain information system. Looking at business reporting chains, we often assume a principal-agent relationship between parties. Backed by laws, regulations or contracts, the requesting party has some form of legitimacy that permits it to request information from companies. As the requesting party often determines the requirements for business reporting, it should comply with the prevailing legislation and regulations in doing so. Different regulations and legislation can lead to reporting chains with different requirements regarding the format and content of business reports.

In the Netherlands, the so-called '*openstellingsbesluit*'[35] specifies how and via which channels reporting parties must submit/file information to a specific requesting party. This directive refers to the usage of the Netherlands Taxonomy and the interfaces of the generic infrastructure.

Figure 9.4 represents one horizontal chain within the SBR solution that highlights three 'chain linkages.' From left to right, we see the following:

1. The chain linkage between the parties involved in compiling and submitting business reports (illustrated in the circle).
2. The chain linkage between the SSC and the reporting party. This linkage could be seen to represent the legal interface between the party with reporting obligations and the requesting party. For the sake of simplicity, we simply refer to it as the linkage between the information provider and requester.
3. The chain linkage between the SSC and the requesting party.

[35] An example is the formal announcement of the Tax and Customs Authority Netherlands regarding the format and content of filings (published in the *'Staatscourant'* no. 3384, February 25 2011).

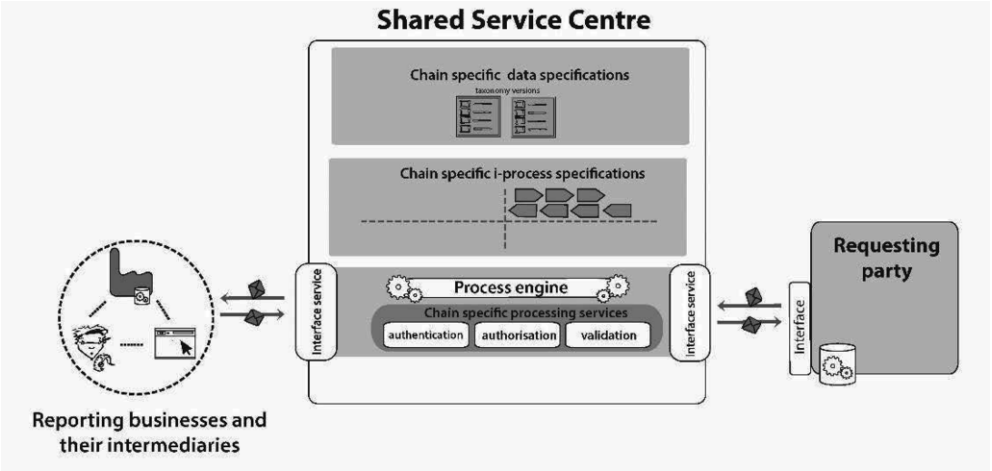


Figure 9.4 – Horizontal SBR chain and three chain links

For the operation of an SBR reporting chain, the chain linkage between the SSC and the requesting party is of primary importance. The linkage between the private parties depicted in the circle form an important aspect of the SBR business case. However, the parties involved in the information delivery are free to decide how they will implement their linkage. This linkage is outside the scope of governmental coordination.

9.3.1 *Relevant aspects from a horizontal integration perspective*

In essence, every reporting chain (whether integrated or not) contains the same aspects that require alignment. Reporting parties—and the service providers who support them in their reporting processes, such as software providers and intermediaries—need to know what information they should provide, what time to provide it, and how. If changes to any of these points are imminent, or if problems are anticipated, the chain partners will want to discuss this with the requesting party. The requesting party must make sure that the reporting organisations can meet their obligation to report without unnecessary burdens. For integrated chains, this responsibility also extends to the chain partners. The basis for public reporting is laid down in administrative law. Of course, it is in the requesting parties' interest that a reporting party submits information correctly. Given the scope of this chapter, we will discuss chain governance only for those SBR reporting chains that have a public requesting party, with the note that the market provides a large number of models that can be used to set up the chain governance for a private reporting chain.

Focusing on business-to-government reporting within the SBR context, Logius manages the chain components that integrate the systems of the reporting and requesting parties. It is important to note that when it comes to business reporting, Logius itself has no administrative mandate. Instead, Logius acts on behalf of the requesting parties that employ its services. This means that a message is considered to have been received by the requesting party once it reaches their

business processing system and the requesting party performs the final assessment of the message content. Nevertheless, from a legal perspective, the intermediate technical checks performed by the generic infrastructure that is operated by Logius are considered to be 'information processing.' In SBR, the time of reception is therefore when the message reaches the generic infrastructure.

From a horizontal integration perspective, coordination efforts should include the following:

1. The framework of agreements as the basis for setting up a reporting chain.
2. The Netherlands Taxonomy, as a container of the data specifications for a specific reporting chain.
3. Other chain specifications at the message level (e.g., FRIS rules).
4. The process specifications of the business reporting process.
5. Configuration of the interface services.
6. Support for establishing connections and applying SBR standards.
7. Support in the event of incidents.
8. The applicable service levels.
9. The governance of the relevant aspects of the horizontally integrated reporting chain.

Each of the aspects listed above will be elaborated on in the following subsections.

9.3.1.1 The framework of agreements as the basis for setting up a reporting chain

If a requesting party is linked to SBR, it should use the framework of agreements as the basis for setting up the reporting chain. This means that the reporting party should be able to use the SBR standards that are relevant to the reporting chain they are part of. They therefore need to be able to use an XBRL taxonomy that is constructed in accordance with the Netherlands Taxonomy Architecture. In addition, the service providers and software developers in particular need to implement the appropriate interface specifications for system-to-system information exchange. Not all aspects of the framework of agreements are necessarily relevant for all parties. For instance, the e-notification interface is irrelevant to a software party that only creates reporting software for financial statements, since the Chamber of Commerce does not send any return notifications.

Nonetheless, it is highly important to the chain partners whether the requesting parties decide to use SBR as the basis for the reporting chain. This particularly applies if SBR is going to be the exclusive method for system-to-system information delivery. In 2013, the Tax and Customs Administration was the first to take the step toward SBR for corporate income tax declarations. The decision was announced after extensive consultation sessions with the chain partners. Here, we see the relationship between the governance for the horizontal integration and the governance of the framework of agreements.

9.3.1.2 Specific elements of the Netherlands Taxonomy

The Netherlands Taxonomy includes both generic components and chain-specific components. Chain-specific components prescribe the exact specifications of what a requesting party wishes to receive in a reporting chain. This is done by referring to both generic and specific elements. System-to-system information processing is a cost-effective solution if the elements or sub-elements being requested have already been gathered and administered in software solutions during business operations. In this context, the chain partners should be informed about the content of the message specifications in a reasonable amount of time. In addition, all parties involved depend on the technical form and quality of the taxonomy, because they have to map it onto the software systems. Should an element of the taxonomy contain an error (which could be a technical error or a missing element), it would be preferable for the chain parties to find out about it well before the actual information exchange and processing takes place.

9.3.1.3 Other chain specifications at the message level

Requesting parties may impose additional requirements on the messages, such as the FRIS regulations, on top of the Netherlands Taxonomy. Therefore, chain parties should be aware of which, if any, additional specifications apply to messages in a specific chain.

9.3.1.4 Process specifications

In SBR chains, business reports go through predefined processes. It is important that chain partners be aware of the process results that are relevant to their task, and that they know how to respond to these results. For instance, it is important that the reporting party know whether it has fulfilled its obligations or that its report did not comply with the requirements imposed upon it. Technical systems need to be adjusted to handle any possible process outputs from the systems they are integrated with. Such outputs could include an acknowledgement of receipt or a rejection message and status information. When setting up their activities and products, reporting parties depend on how the processes have been organised. Another aspect is that part of the automated processing is done at Logius. Therefore, the detailed process specifications can be regarded as functional task descriptions for Logius.

9.3.1.5 Configuration of the interface services

For SBR, the specifications of the interface services are described at the level of the framework of agreements. The framework refers to Digilink and imposes some restrictions on the specifications of the interface services. In addition, the operation of the interface services (the dialogue) is included in the process specifications. Interface descriptions are available for interface services, as the technical implementation can involve multiple layers. It is important for specific chains to know which interfaces have been implemented for the chain, which end-points apply, what types of certificates (what roots) are accepted and what the unique reference identifier is for proper reporting. For SBR, the message

type is what matters. Horizontal chains in SBR have interface services between Logius and the reporting party and between Logius and the requesting party.

9.3.1.6 Support for establishing connections and applying SBR standards

If reporting parties are expected to implement changes to components in the reporting chain, it is important to test them extensively beforehand. The SSC offers test facilities and support for establishing a connection with the generic infrastructure. In the event of complex changes, the reporting parties may need other forms of knowledge transfer about the change.

9.3.1.7 Support in the event of incidents

Chain partners can make mistakes and machines can break down during the reporting process. Additional support should be available when the chain suddenly stops. Moreover, information providers should be able to report disruptions and receive notifications in the case of disruptions. This requires agreements between the various chain partners regarding incident management.

9.3.1.8 The applicable service levels

In addition to the previously listed points, reporting parties require certainty not only about format and content, but also about the service quality targets set by requesting parties regarding the prescribed communication channel. For example, what degree of availability can they assume the interface services will have? How often is maintenance performed? How often can changes be expected? The requesting party's service quality targets are very important for Logius, since Logius is responsible for a number of the quality parameters. The quality levels require optimum alignment if the chain is to be cost-effective. After all, the chain is only as strong as its weakest link. It is not practical for the government to staff a helpdesk at night if the reporting parties would hardly use it. On the other hand, it might be annoying if the information delivery service were not available by default at night, a time when some software systems might be able to process the day's message traffic more efficiently.

9.3.1.9 Governance of relevant aspects for horizontal integration

How decisions are made with regard to setting up relevant aspects of the prescribed communication channel is relevant to all chain parties.

9.3.2 *Principles of governance*

The principles of governance for horizontally integrated SBR chains require a clear distinction between the three chain linkages illustrated in Figure 9.4 above.

9.3.2.1 The chain linkage between the reporting and requesting parties

Legislation, regulations and policy statements by the government form the foundation for chain governance on the interactions between the reporting and requesting parties. The requesting party should formally 'open up' the prescribed

communication channel and—as long as it is done carefully and in line with expectations— the requesting party actually becomes a powerful decision-maker in the information chain. If any party feels it has been treated in an unfair manner—for instance, if it feels that complying with the reporting obligation imposes a disproportionate burden—it could consider taking the case to the civil courts (to claim that the policy is unlawful). If a large number of chain partners feel they have been treated unfairly, the issue will become political and the stakeholders will take steps through the political arena to change the actions of the requesting party.

This scenario is certainly not one that would provide any appeal for the requesting party. The question then arises of whether the requesting party can determine whether a taxonomy can be implemented, whether the maintenance times for the opened communication channel have been sensibly planned, and whether the communication regarding errors is sufficient, without consulting the reporting parties and software developers first. In practice, the requesting party—and certainly so for major changes—will want to consult the reporting parties and software developers to gain support for the chosen approach. This starts with the determination of whether a requesting party should in fact use SBR as the basis for setting up the reporting chain. During the consultations, the requesting party gets its first taste of the pluriform information delivery chain. This consultation should take into account the various interest groups within the reporting chain. There may be differences between small and large reporting organisations, as well as between organisations that use intermediaries and those that submit their own declarations (self-filers). The intermediaries and software providers have their own interests as well. Furthermore, differentiation between service providers is possible. Intermediaries are often represented by sector/trade associations. In that case, the trade association is a logical point of contact for the requesting party. Nevertheless, proper coordination requires customised work within a chain. For instance, the question should be asked of whether all relevant parties are sufficiently represented by the trade association, and the requesting party should give serious thought to the way that it organises the consultations. For example, if competing software providers were gathered in one room are asked whether they had problems with the application of a new technology, they might not say what they really think.

The SBR case provides a clear example of a requesting party taking into account the interests of the intermediaries and software providers when determining the policy for opening up the communication channel. This was done by the Tax and Customs Administration when they investigated the exclusive use of SBR, on the request of the market parties. Before we describe the current governance of SBR, it is important to note that the Tax and Customs Administration also maintains its own infrastructure for reporting chains in the fiscal domain.

Based on the consultations with chain partners, the Tax and Customs Administration deliberately chose to carry out the first implementation of SBR in the corporate income tax chain, as the number of software providers active in this

chain was limited, and because most of the system-to-system information exchange in this chain was handled via intermediaries. For the launch they had a clear and well-organised group of stakeholders to make agreements with and whose interests to base their decisions on.

Principles for governance of the horizontally integrated chain (public/private):

- The requesting party develops the frameworks for the governance. In doing so, the requesting party determines the extent to which it includes chain partners when setting up the chain. The requesting party should also comply with the legal frameworks for opening up the communication channel, including any supplementary expectations raised by the government.
- Reporting parties in the chain who feel they are being treated unfairly can always take the issue to the courts or the political arena. Neither escalation is considered desirable by the parties.
- It is in the interest of the requesting parties to inform and consult the private parties in good time regarding intended changes affecting the information chain. The purpose of this is to make sure that parties can 1) change their working methods, services and technology in time, and 2) communicate what the impact of the intended change will be.
- It is in the interest of the requesting parties to hold consultations where the relevant parties can discuss suggestions and complaints about the existing setup of SBR chains.
- The discussion opportunities provided by requesting parties can have a broader scope than just SBR and therefore do not have to be part of generic SBR forums.
- The requesting parties might benefit from holding customised consultations for certain decisions.
- Sector associations are logical points of contact to include in decision-making. The requesting parties should always evaluate whether involving sector associations is in the interest of all chain actors.
- If governance is to function properly, it is important that the requesting party provides as much clarity as possible about its intentions beforehand. For example, it should be communicated whether the parties are being consulted or merely informed.

9.3.2.2 The chain linkage between Logius and the requesting party

The chain governance for the linkage between Logius and the requesting party is based on a service relationship: the requesting party partakes of the services offered by Logius. Current legal frameworks assume a strong controlling role of the public agencies that purchase such services and that Logius, as the SSC, will be following their lead. An assumption in such a model is the prescriptive role of the requesting party, while Logius is expected to implement the specifications prescribed. However, a knowledge gap is created between the principal and the agent as Logius becomes specialised in setting up the automated processing of business reports and S2S integration with information providers.

Because of Logius's unique expertise in this area, requesting parties will turn to the SSC provider for advice on how Logius's part of the reporting chain should be set up. Logius may impose requirements, for instance, regarding information security. Providing advice and imposing requirements creates a responsibility in the reporting chain that will acquire so much significance over time that a governance model in which the requesting party holds a fully prescriptive role over the allocation of responsibilities becomes inappropriate. As a result, the requesting parties will want Logius to report about its actions independently, as responsibility over that part of the chain can no longer be taken by the requesting parties. This situation is further reinforced by vertical chain integration, which will be discussed in §9.4. The requesting party remains responsible for setting up the integration between its own solution and Logius's, but can partially rely on Logius's assessments and expertise when choosing the setup. This gives Logius more responsibility, which should be accompanied by increased authorisations for managing the setup. This situation results in the following principles for the governance of this linkage:

- The requesting party is responsible for choosing whether it will use Logius for processing business reports. For this choice, it can partially rely on the fact that Logius already has this special role in the Dutch government.
- As a specialist in automated processing of business reports and S2S integration, and as an SSC, Logius assumes independent responsibility. From this position of authority, it can impose conditions on its collaboration with requesting parties. The decisions regarding important aspects within the setting of a client and contractor relationship are agreed upon on equal grounds.

9.3.2.3 The chain linkage between the reporting party and its service providers

When adopting SBR, market parties face further information system integration. In this regard, the market parties must determine how they want to set up decision-making. It is possible that intermediaries will prescribe certain software that supports the entire integration between companies, intermediaries and administrative authorities. In that case, the company with reporting obligations must decide whether it will collaborate with the intermediary on this, or whether it will meet its obligation in a different way. The company, as one of many clients of the intermediary, has a limited influence on the further development of the software package in such a case, and decisions are effectively made via the constraints of market forces. If a software package is not user-friendly, it could cause a party to switch to another intermediary. This would be a signal to any intermediary who uses the package as their standard. Intermediaries have a content-based role in some business reporting chains and are sufficiently specialised to have knowledge of their own professional rules. This applies to tax specialists to some extent, and even more so to accountants. In such cases, the professional rules for governance should also be considered in the decisions to be made regarding the setup of the integrated chain. Such professional rules may make a party decide that it does or does not want to be involved in a decision. An example of a more complex control issue in the market is the question of who will

be responsible for administering the taxonomy and mapping the elements from it. This responsibility could go to the software provider, in which case, the intermediaries and parties with reporting obligations will rely on the expertise of that provider. This is possible in the tax chain, but there are enough tax specialists who prefer to take care of the mapping themselves, seeing it as part of their professional responsibilities. Auditors, on the other hand, may not want to be involved in choosing the mapping, as this can be seen as giving advice about the setup and such a role could conflict with their monitoring task. If problems arise in the business reporting process, the parties with reporting obligations will have to respond first. However, they could hold a service provider liable for the damage if the provider has been negligent. One example could be a software provider that reports the successful submission of a VAT return when the interface service actually gave an error response. Against this background, the following principles are derived:

- Companies and their service providers determine how to make decisions regarding chain integration. There are various models for this.
- All parties have the responsibility, first, to determine what their role is in the SBR chain, and second, to be aware of what responsibilities are imposed on them by the legislation and regulations. In areas where they have responsibilities, they must also claim the associated rights that ensure their involvement in the SBR chain setup, while not participating in decisions that conflict with their role.
- If a dispute arises due to a decision regarding chain integration, the parties can have recourse to private law. They could be proven right and demand compensation.

9.4 Vertical chain integration

As an SSC, Logius plays a central role in SBR for the public domain, striving for cost-effective e-Government. Logius firstly carries out the programme-related work focused on further development and implementation of SBR as a broad standardisation initiative. In addition, Logius is responsible for the continuous operation and further development of the generic building blocks (see section 1.5) for specific reporting chains. This can be considered vertical chain integration because public agencies employ these generic building blocks to handle some of their information processing for multiple reporting chains. The requesting parties that use the shared services depend on the building blocks for a part of their primary processes. That is why requesting parties want to have a say in how Logius operates and evolves as an SSC.

9.4.1 *Relevant aspects from a vertical integration perspective*

The extent to which the requesting parties can outsource their reporting chains to Logius is determined by Logius's resources. The price of Logius's services is relevant here, as cost savings are one of the reasons for using an SSC. Quality is another relevant factor. In addition, it is important for parties to know what

organisational and technical measures they need to take in order to use the services of Logius. The relevant parties should agree on how they want to realise these shared services and which responsibilities and mandates are allocated to the SSC.

9.4.1.1 Logius's services

In the context of SBR, Logius provides two types of services:

1. Coordination services, focused on ensuring that SBR works as a coherent solution.
2. Reporting services, focused on delivering services for specific reporting chains.

Coordination services refer to managing the SBR framework of agreements, promoting the SBR solution within the government and facilitating governance in terms of content and process. Reporting services have the following functions:

1. I-process management: designing, implementing and ensuring availability of process specifications and the underlying interface services and processing services.
2. Data management: designing, implementing and ensuring availability of taxonomies.
3. Application support: providing support to parties in the use of the chain and management in the event of chain incidents (front and back office support).
4. Connection support: providing support to chain partners in implementing the elements of SBR for the chain integration.

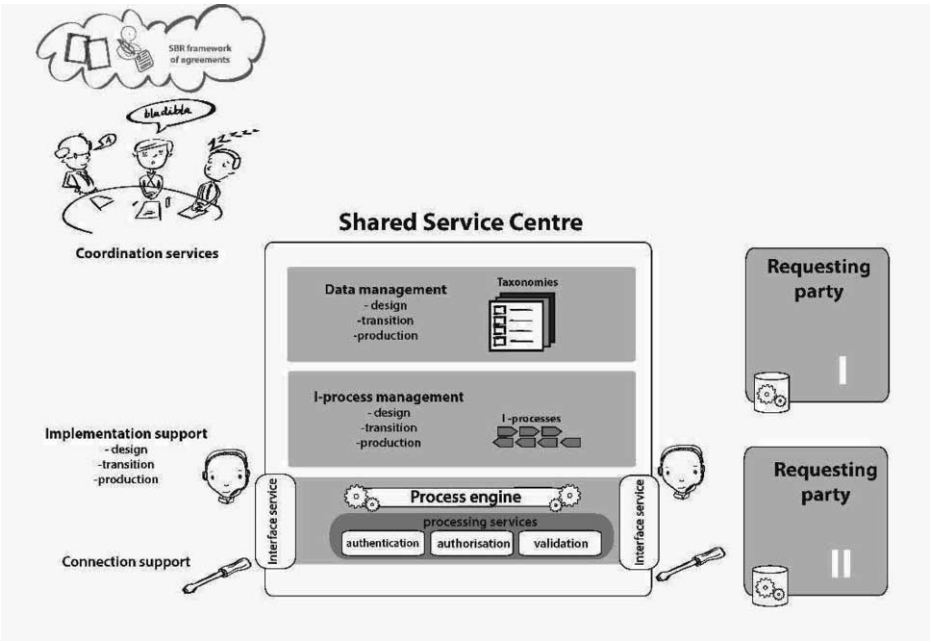


Figure 9.5 – Coordination services in SBR

Section 9.8 on service management discusses both types of services in more detail. For now, it is important to note that chain partners need to decide on the design of these services, their scope and the extent to which they are made standard, as well as whether there is room for customisation. Here, the following questions are relevant: what are SBR services? And which of Logius's services should be designed primarily from the SBR perspective? In order to make a distinction between the management relationships for the two main service types, Logius is seen as an SSC that is commissioned to perform coordination services, with the requesting parties being the 'receivers' of the reporting services. Figure 9.5 shows the areas that require coordination in the context of SBR.

Quality
The quality of the services is extremely important for the requesting parties, as these services largely determine whether the integrated reporting chains are able to operate at a sufficient level.

Price and costs
The aspects stated above—i.e., the choice of which services and with what quality—are particularly relevant because of the price perspective. Put simply, the way services are realised largely determines their price. That is why the parties do aim to achieve sufficient quality rather than maximum quality. The rules regarding price vs. quality are the following:

- Increased customisation of services is generally more expensive.
- Increased availability is generally more expensive.
- Services that are more flexible are generally more expensive.
- Higher levels of security in services are generally more expensive.

The costs of the SSC should be distributed over the principals (government agencies/departments) and the requesting parties (as service consumers). Various models can be chosen for this. For instance, the parties can distribute costs proportionally, based on usage. However, a precondition for this is the ability to determine which costs are be attributed to which level of usage. Establishing an appropriate pricing model is a formidable task. Whenever development is involved, the parties may choose to bear the full costs for the development of a service, and then share the operational costs of the services with multiple users.

9.4.2 *Principles of governance for vertical chain integration*

The principles for the governance of the common services within the public domain are based on the general interest: after all, the situation involves a single government that has to carry out its total range of tasks. The assumption for the governance of the SSC is also strongly determined by its formal position. Logius is a SSC and therefore has limited equity and resources of its own. For further development of its services, Logius needs to find one or more governmental parties that are prepared to invest in the SSC's services. This affects the governance. The involvement of the clients in processes that still have an element of uncertainty and that are only used to a limited setting will be large relative to the

development of the SSC and its service catalogue. The authorities involved (including the policy-making ministries acting as principals/SSC customers) will require a form of governance that reflects their investments and interests. As they say, "He who pays the piper calls the tune."

A programme such as SBR involves a double uncertainty. Firstly, the business case for requesting parties is determined by the usability within their own reporting chains. If Logius's services turn out to be insufficient, it will create a problem for the requesting parties that invested in it. Secondly, the business case for the SSC is determined by the wider adoption of SBR. If the use of SBR is limited to a few reporting chains, the enormous efforts associated with network standardisation and the complex organisational setup of the generic building blocks will not be viable. Based on the interests of overall burden reduction for *The Netherlands, Inc.* and cashing in on the investments made, the Ministry of Economic Affairs and the Tax and Customs Administration act jointly in controlling the positioning of the vertical chain integration. The fact that Logius's services for SBR reporting are becoming more and more mature reduces the risk for new participating parties. It is, in fact, attractive for these parties to connect to a generic service that will take various compliance issues out of their hands. They would rather not deal with the in-depth material required for operational decisions, preferring to leave it to the SSC. It is also convenient for a requesting party to assume that the employment of Logius for its horizontal harmonisation also implies that key responsibilities vis-à-vis the Online Administrative Business Act are properly dealt with. And as long as the expected quality is delivered, these above parties will want to be involved in decisions much less frequently. However, there is one significant 'but' associated with that observation. A requesting party, in its role as receiver, must be highly aware of the role played by Logius in the chain that it is responsible for. The requesting party must always be kept up-to-date about the way that its own reporting chain operates. This requires a requesting party with a very strong content-related and conceptual knowledge, especially at the tactical level.

The following principles apply to the chain governance of the SSC for SBR:

- The maturity of the shared service strongly determines how the chain governance is organised. Launching customers, who are running a risk by getting involved, will want to be intensively involved in decision-making regarding the setup of the shared services. With a mature service, a governance model that takes the problems out of parties' hands is attractive.
- Efficient and balanced governance of Logius as the SSC continues to benefit from a level playing field in terms of knowledge of the reporting domain and the integration of information systems.
- "He who pays the piper calls the tune" is an important assumption in chain governance. Because Logius is a service agency, the launching customer is often the determining party when the services are being set up.

9.5 Network integration

Network integration using multiple standards occurs when multiple parties decide to build links for information exchange in the same way, without all the information chains being linked up to one other in practice. This form of standardisation can also be seen with the Internet. In theory, one can reach any website from a browser and exchange information using various standards. In practice, most of the existing sites on the Internet will never be visited. Such a picture can also be created for SBR. Let us assume that a requesting party (public or private) uses the SBR interface and a discoverable taxonomy that has been set up in accordance with the Netherlands Taxonomy Architecture. If this requesting party asks for concepts that have already been mapped in the database of the reporting party, fully automated system-to-system reporting should be possible. In addition, similar to the URL of a website, the reporting party needs to state the end-point of the interface and the type of message that it wants to exchange.

Based on the history and drawing of legislation, reporting chains are set up in such a way that integration of information systems is based on the chain perspective. The concrete chain approach (with horizontal and vertical types of integration) has therefore been assumed for this book. The perspective of the network approach is also important for the chain governance. This is firstly because SBR (or components of it) are used as network standards in practice, which implies a form of network integration. Secondly, the network perspective may end up taking a dominant position in the final realisation of an open and flexible reporting system (and the ideal of a store once, report to many architecture).

The success of 'standards' to be used for network integration is also determined by the following elements:

1. **Availability**: the extent to which the standards are accessible (i.e., can be found and are affordable) for the users.
2. **Effectiveness**: the extent to which the standards are usable for the purposes for which they are applied.
3. **Efficiency**: the extent to which the standards are applicable in terms of the required money, effort and knowledge needed to implement and apply them.
4. **Relevance**: the relevance to the field they are adopted in.
5. **Stability**: the extent to which the standards are subject to changes.

How a standard scores on the points listed above must be considered by comparing the standard to competing specifications that provide a solution for the same need. In practice, efficiency (simplicity) triumphs over effectiveness almost every time. For example, VHS won out over Betamax. These were the two standards for videotapes, where the latter was technically better, but the first was easier to apply. Ethernet also won out over Token Ring (network standards, where the same pattern occurred as with videotapes).

9.5.1 *Relevant aspects from a network integration perspective*

The relevant item for SBR as a network standard is the SBR framework of agreements. This framework describes what standards must be applied when setting up a business reporting chain. In practice, the framework consists of various sub-agreements, which can mostly be found in the decisions made by the joint consultative bodies. Looking at the components from the framework of agreements, we must distinguish between SBR-specific specifications and those that are not SBR-specific. The latter 'specifications' are already standards that are used outside of SBR. The SBR-specific specifications often refer to a set or a sub-collection of non-SBR specific specifications.

SBR-specific specifications:

- Netherlands Taxonomy Architecture
- SBR Process Architecture
- SBR Technical Architecture
- Netherlands Taxonomy
- SBR governance description

Non-SBR-specific specifications used by SBR:

- TCP/IP
- XBRL 2.1 (and an entire set of additional XBRL specifications, as discussed in Chapter 5)
- TLS
- WUS (Digilink 3.0)
- PKI-government

Figure 9.6 illustrates the scope of the framework of agreements in practice.

The above-mentioned standards each have their own route for further development and management. SBR uses open standards (specifications that meet certain standards in terms of management, changes and availability) as much as possible to simplify the acceptance of SBR. The resulting dependencies, now widely discussed, must be managed by the actors connected to SBR. The way this is done is different for each standard, as the actors are committed to following SBR in some aspects. For example, they are not likely to put much effort into the further development of the Internet standards, whereas participation in the further development of Digilink is almost assured.

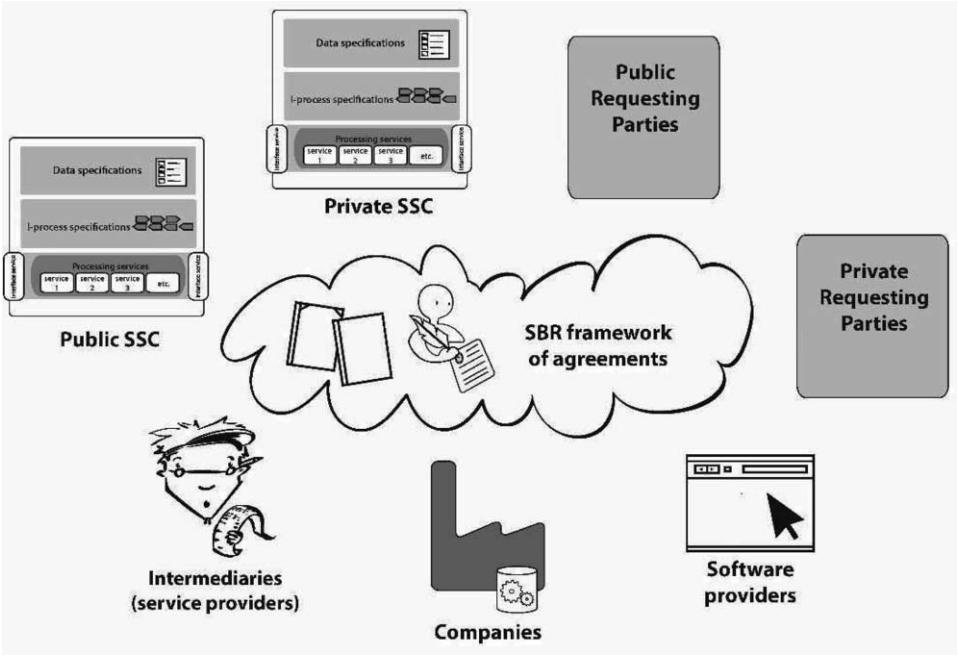


Figure 9.6 – Stakeholders in the framework of agreements

Developments in XBRL are also closely monitored by the architects involved in SBR. The SBR-specific specifications (which jointly form the SBR standard) partially consist of instructions about which open standards must be used when setting up a reporting chain, and a description of the way that an open standard must be used. Another part of these specifications is related to content-based aspects of reporting (with regards to concepts and processes). All actors who are linked to an SBR reporting chain are stakeholders in the framework of agreements and are thus involved in some way in the alignment of the relevant aspects. Brief explanations of the various parts are given below.

The Netherlands Taxonomy Architecture
This is the clearest and most accepted object at the network level. If a party creates a taxonomy for a business reporting chain and wants to work in accordance with SBR, the Netherlands Taxonomy Architecture will be used. The name might give rise to the assumption that there are no other taxonomy architectures in the Netherlands. This is not the case. Those involved in the data standard claim that the name Netherlands SBR Taxonomy Architecture (or the SBR Taxonomy Architecture) would better reflect the position of the NTA.

The SBR Process Architecture
There are two agreements that can be placed under the SBR Process Architecture. Firstly, agreements have been made about how the SBR processes are to be shared with the relevant parties. The BPMN standard is used for this. In practice, this agreement is used for the process components of common solutions

(the generic infrastructure and the BIV, the 'Banking Infrastructure Provision'). The second agreement concerns how status information is handled. Parts of the status information and error notifications have been harmonised. It should be noted, however, that software providers want to make more detailed agreements about this with the requesting parties and are asking the requesting parties to further harmonise how they deal with status information and error notifications. Within this context, the requesting parties have already agreed to communicate clearly about what the final status of an information delivery process is in order to make sure that the parties know when they have met their obligations. The various parties have suggested finding a standard for an expandable and discoverable taxonomy for status information. Its advantage would be that the parties could implement certain new control services without the software providers having to make changes to their software due to new types of status messages.

The SBR Technical Architecture

In effect, the 'permissible' interface specifications of SBR describe the new technical agreements and therefore jointly form SBR's technical architecture. Digilink 3.0 is now the basis of the framework of agreements, whereas the government parties in the framework only want to allow WUS 2.0 version 1.2 to be used as an interface. Digilink 3.0 is a government standard and initially banks—as private requesting parties—have indicated that they will follow the administrative authorities when it comes to specifying interface standards. It has recently turned out that the banks are not satisfied with the Digilink developments. Because they do not see why the interfaces need to be developed further, they now want an earlier version of the interface component to remain part of the SBR framework of agreements. There is also the issue regarding portals. SBR does not lay down any rules about input portals. This does not mean that portals cannot be used for information delivery in SBR. In they are used, the portal operates as SBR-compliant 'software.' Such a human-to-system linkage can be interesting for data that is not included by default in the administration. As an SSC, Logius can provide such a portal for chains. Changes in such a portal can be implemented quickly because known SBR standards are used. The banks maintain a common portal as well. However, such a human-to-system interface is not covered by the SBR framework of agreements. A requesting party might also prefer to maintain a portal of its own with an underlying non-SBR linkage for a certain target group.

The Netherlands Taxonomy

The Netherlands Taxonomy can be seen as a standard at the network level because the extensions of the parties are based on the Netherlands Taxonomy. Requesting parties reuse concepts from the taxonomy for defining the information request to businesses. In practice, this reuse has turned out to be particularly effective within business reporting domains. There, the data from various fiscal business reports overlaps. The same applies to reports in the domain of financial statements. Particularly with the more advanced financial statements that serve society at large, the concepts used in these reports largely correspond with fiscal

concepts, yet they do not fully coincide, which is contrary to what might be expected. Because reuse of concepts turns out to be domain-related, alignment needs to be coordinated at this level as well. Given that the parties may operate in multiple domains, it is important to avoid creating homonyms. The reports in the Netherlands Taxonomy provide chain-specific specifications, and the extensions will therefore become objects in the horizontal chain integration.

SBR Governance
The governance of the SBR framework of agreements is an important aspect within the framework that involves all parties. Here, the parties involved in SBR describe how they can systematically revise agreements or reach new agreements. Ideally, the governance also describes how the governance can be changed. The Dutch Constitution, for instance, defines the procedure for changes to the Constitution. However, while the SBR governance provides for periodic evaluations, it does not describe the further course of action with regard to changes.

9.5.2 *Principles of SBR governance for network integration*

The principles for the governance of SBR as a standard for network integration (public/private) can be formulated from two extremes. In the first extreme, one party is responsible for the governance of the network standard. This party maintains the specifications based on its own needs and then publishes them. After that, other parties can use the specifications in their reporting chains. This is a valid model as long as the earlier criteria for the adoption of a specification are met so that the specification can be used as a network standard. The other extreme assumes full participation in which all parties with the potential for using the specifications are jointly responsible for the governance of the specification. It is important to note that in the model with a single determining party, that party may need to discuss changes in the specifications with chain partners to ensure continuity of its own information exchange. A crucial restriction in the single-party model is that utilisation within the determining party's own chain given priority in its considerations.

Hybrid models that lie between the two extremes are also possible, where the number of parties responsible for governance and decisions is limited, but where consultations do not only take place based on the applications within the parties' own chains, also taking into account the specifications being used in other information chains. In such a case, the parties make an effort in the general interest. As such, public parties prefer to adopt this model.

The policy of the SBR Programme was to ensure hand-in-hand adoption of the framework of agreements by both public and private parties. The resulting application of SBR by large banks has caused SBR's scope to move from the solely public domain to the public/private domain. However, this has not affected the scope of shared specifications. Although the accession of the banks into the SBR Programme gave the network perspective much greater relevance, the contrast

of the requirements on information processing between the public and private domains has imposed limits on the depth of the overarching framework of agreements. For private parties, differentiation is a necessity required by the market environment. That is why the degree to which market parties can comply with certain agreements is limited. If the participating banks were to create uniformity in the entire information processing system for granting loans, this would greatly reduce the scope for differentiation. While uniformity would be suitable for franchising, the Authority for Consumers & Markets would probably deem it unacceptable for three large banks in the Netherlands to actually operate in that way.

In contrast, it is quite useful for public parties to set up comparable components (functions) uniformly, as this would increase efficiency and controllability, consistent with the principle of efficient government. The public domain can therefore be seen as a domain with detailed standardisation agreements. When considering the semantic harmonisation of concepts, public parties are often faced with legal requirements that make entering into a participative governance model with other requesting parties difficult. This is because the law defines their requests and they cannot change a legal definition independently. It is thus easier for private parties to standardise definitions, and they can form a domain with detailed standardisation agreements. The figure below illustrates the scope of the framework of agreements.

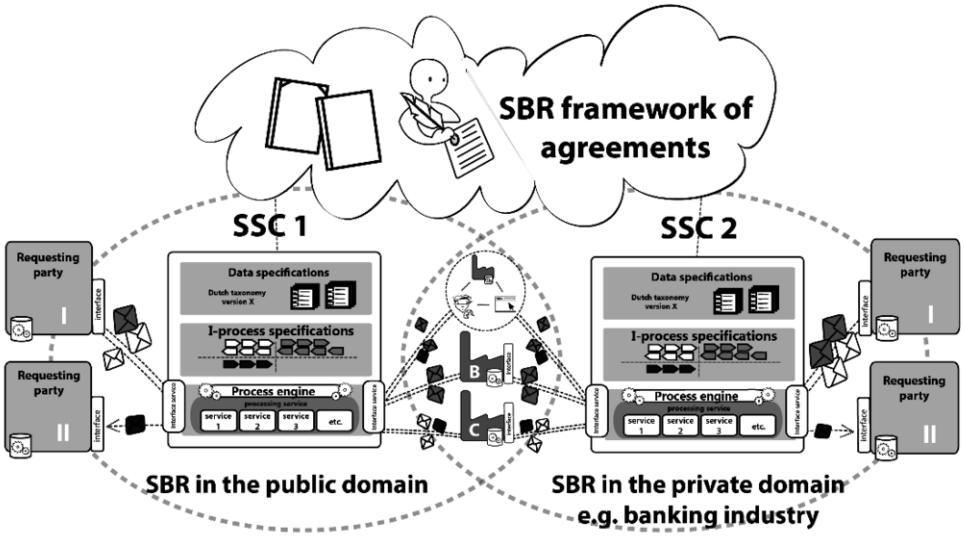


Figure 9.7 – Representation of the scope of the framework of agreements

The following principles can be formulated for the governance of SBR as a standard for network integration:

- The scope of the public/private framework of agreements and the included governance structure need to allow for the possibility of adoption

in the domain as a whole. In practice, this means that substantive choices are particularly limited at this level. Substantive components can be standardised further within an SBR application domain.

- A model with a single dominant party determining the full set of specifications based on its own chain perspective does not fit with the current setup of SBR. At the highest level, this means that a coordination structure based on mutual adjustment must be set up, rather than a consultative structure.
- Where parties have the option to ensure further alignment, they can do so within a specific domain. The SBR banking taxonomy is an example of this. The relevant parties in the banking domain have their own governance structure for decisions regarding the common specifications. Note that this creates an additional forum for alignment discussions. The government parties (public requesters) impose additional requirements on the way the banking domain should apply SBR standards. In principle, this could result in the creation of interconnections (vertical domains), for example, in case public and private parties involved in information requests regarding payments make additional agreements about using the network standards.

9.6 Coherence between the governance of the three integration forms

Explaining how chain governance of the three integration forms fits together can be done using either a simple or complex approach.

The simple approach sees the three forms of control as separate components, each with a clearly delimited area. With regard to horizontal integration, a requesting party either does or does not comply with the SBR framework of agreements when setting up the business reporting chain. For requesting parties who comply with the framework of agreements, this framework becomes the bedrock for developing an SBR-powered reporting chain. With vertical integration, the requesting parties who use the shared services determine the scope and extent of the shared service. It is obvious that the shared services must comply with the framework of agreements for SBR chains. Finally, in terms of network integration, anything is possible within the requesting party's own frameworks. The more organised one becomes at the network level, the easier it becomes to control of the relevant aspects of horizontal and vertical integration. If the SBR framework of agreements states that a taxonomy should always have a dimensional structure, this is a choice that a requesting party no longer needs to make when setting up its business reporting chain. The SSC will ensure that its data management services will always be based on a dimensional taxonomy. As an example, if the SBR framework of agreements were to state that an SBR-compliant interface service must always be at least 99.8% available, the organisations processing the business reports—including Logius—would know that the service organisation of every existing SBR chain must be set up to meet this service level. However, there are limits to the one-size-fits-all approach, as has already been

discussed with regard to SBR as a network standard. The parties cannot work with just a single information chain because their objectives for reporting may be different, or because their own responsibilities may require a different setup of comparable reporting flows. It is important for parties who want to comply with the SBR framework at the network level to assess whether they are able to work with the standard when setting up their business reporting chain. However, doing so increases complexity.

The complex approach takes into account the snowball effect that occurs when a problem in one chain affects all the other integration forms. Figure 9.2 illustrates this integration. If the requesting parties comply with a given decision regarding further standardisation, they must immediately consider their responsibilities to the SSC, the reporting parties and the software developers in the various chains. The decision-making regarding network integration will now depend on the decisions to be made about aspects that apply to horizontal and vertical chain integration. Because the various chain partners—and the SSC—operate in multiple reporting chains, they will have to consider their interests from a broader perspective when assessing the standardisation options for one business reporting chain. This is where the decision-making becomes intertwined.

In practice, the intertwined decision-making implies that actors will speak from a variety of perspectives during alignment discussions. For instance, in discussions where the actual usefulness and need for change in a specific reporting chain are on the agenda, the actors will discuss the need to implement this change integrally for all SBR chains. While this is a valid idea, but it may cause confusion for any parties who are only concerned with a single dimension and who do not recognise the broader interests other parties. In this situation, decision making is also complicated by the fact that the aspects regarding chain integration are almost always technical and content-based in nature. Not every requesting party has the opportunity to study the technical material and the probably impact of standardisation in their own chain. For example, not all organisations automatically have the in-house knowledge to determine whether an enveloping signature, enveloped signature or an externally detached signature is a standard that they can work with. When in doubt, the parties will thus be reluctant to declare something as a standard. They will probably want some leeway for deviations from the SBR framework of agreements. Please note that the interdependencies between various alignment areas are the strongest in the case of fundamental changes (see also Chapter 4).

To ensure progress in the standardisation of information chains, it is therefore important that actors with sufficient specialist know-how to unravel the technical impact of decisions from different perspectives, and who are trusted by other parties to act for the common good to at least a certain degree, are involved. These actors have an overall picture of the puzzle and can help create a consistent whole.

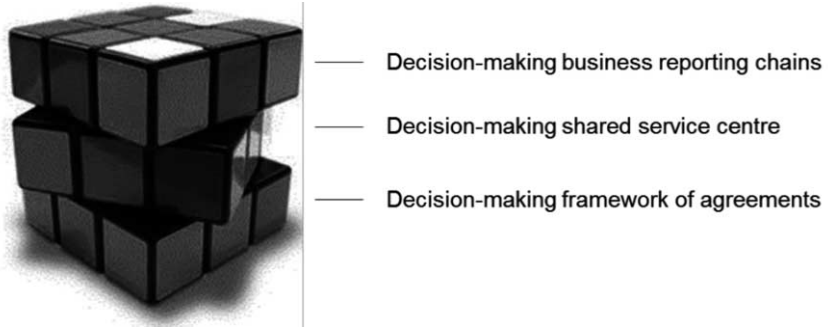


Figure 9.8 – Cohesion of the governance of the three integration forms

Such authority is earned, and is a role can be fulfilled by multiple parties. Because the SSC can specialise in the material and because they are responsible for important components of the chain, they are one of the parties with a particularly good picture of this complex field. In practice, the success of standardisation will depend on the extent to which the SSC is able to acquire the required position of authority. In SBR, the Tax and Customs Administration is a major requesting party with a great deal of expertise regarding system-to-system information processing. The Tax and Customs Administration has invested in sharing knowledge and served as an important launching customer of the SSC. It has thus accumulated authority regarding SBR among the requesting parties. The confidence of the Tax and Customs Administration has helped the SSC acquire its own status as an authority. Finally, the governmental manager of SBR (see the introduction or below) has turned out to be an important actor in SBR in terms of management and streamlining of the decision-making at various levels.

9.7 Current SBR governance

9.7.1 *Structure and connections*

Currently, several public-private forums have been set up to operate jointly within the SBR framework of agreements. Typically, the aspects dealt with concern the use of SBR for network integration. The requesting parties and the SSC also use the forums to obtain agreement about horizontally integrated chains. Obviously, the public-private forums do not handle the issues that apply to horizontal and vertical integration in the public SBR domain. Such issues are handled by a public governance structure within SBR that has been set up to make decisions about the following:

- What the administrative authorities do for public-private governance in SBR.
- How the shared services that these authorities receive should be further developed and managed (vertical integration).
- The horizontal integration between the SSC and the requesting parties.

The public-private governance and the public governance are linked in various ways. For instance, the SBR Board and the SBR Steering Committee (the two

highest bodies in the governance) are presided over by the Director-General of the Tax and Customs Administration. A governmental manager has also been appointed to speak with the public SBR parties, other governmental organisations and market parties to explain the meaning of SBR, to create support and to make sure that any broader issues are handled. The governmental manager has a certain independency, is approachable, and is therefore an important figure when setting the agenda. He coordinates proposals towards the appropriate decision-making organ and manages further standardisation.

9.7.2 *Public-private SBR forums*

The SBR Board
The SBR Board members representing market parties and those from the government define the common frameworks and strategic lines for using SBR as a network standard in the longer term. The Board thus generates the required support among all those involved in the decisions made in other forums and gathers details about how the generic solutions are managed from the sides of the administrative authorities and private parties. All stakeholders take part at an aggregated (national/sector) level. This includes those who are represented in the SBR Platform as well as the other – smaller – stakeholders. For example, the Board includes one joint representative of all intermediaries and trade associations, one joint representative of all the service providers/software providers, the Confederation of Netherlands Industry and Employers, and so forth.

The SBR Platform
The SBR Platform is the forum in which the various interests of the parties involved in SBR are represented. At the start of the SBR Programme, proper exploration and involvement of the market was a very important function for the assurance that the SBR goals are still shared by the parties involved. As SBR has grown into a more permanent method that has been formalised by the government, the representatives in the Platform pay particularly attention to ensuring that any bottlenecks in SBR's progress are detected at an early stage, and that opportunities to move SBR forward are present on the agenda. The broad representation of interests in the Platform is in line with the principles of care and proportionality. However, in order to create a workable forum and ensure equal treatment of stakeholders, it is important to impose an additional condition: participants must represent a substantial interest. As such, what a 'substantial interest' means needs to be formulated with clear and explicit criteria. In practice, participants have substantial interest because they can speak on behalf of interest groups.

Expert groups
Specialists from the market parties and the government take part in the expert groups regarding data, processes and techniques, and marketing and communication. Under the supervision of experts from Logius, these groups work to develop proposals and recommendations based on their expertise about the setup, management and maintenance of standards. They also identify new trends or

trends that have not yet been properly addressed and provide advice on how the SBR parties can realise defined standardisation targets. Expert groups require active contributions from their participants and expertise in specific subject areas. Public consultation—for instance, regarding taxonomies—provides input from the broader community. The contribution of expertise in SBR decisions helps ensure the work is carried out with due care. Results, reports, documents and so forth are made public and published on the SBR site for other stakeholders to view.

Others involved
The smaller groups within the interest groups represented in the Platform must also be given the opportunity to give input (following the principles of due care, proportionality and equality). This could also be done by setting up a 'counter' and/or an annual SBR day, where these groups can provide input, discuss their interests and make an assessment of the Platform's output based on their own perspectives. For the sake of transparency, the minutes of the Platform are made public.

Independent sessions for governance
The requesting parties and other stakeholders independently organise sessions with stakeholders within their own reporting domain, since they are responsible for the setup of horizontal integration within those chains.

9.7.3 *Public SBR forums*

The SBR Steering Committee
In the SBR Steering Committee, decisions are made by the government parties regarding the strategic plans for the future of the SBR framework of agreements (the contribution in the Board) and the shared services. Each of the government parties involved in SBR is represented: the ministries of Security and Justice, Finance, Economic Affairs and Foreign Affairs, the requesting parties (including the Chamber of Commerce, Statistics Netherlands, Tax and Customs Administration) and Logius. The Director-General of the Tax and Customs Administration is the chair of the Steering Committee.

Project Leaders' Meeting
The Project Leaders' Meeting, made up of the requesting parties, Economic Affairs and Logius, realises the path set by the Steering Committee. The Project Leaders' Meeting draws up a tactical plan and a budget for SBR each year. It prepares the methodology for the costs and monitors the execution of plans and activities at the operational level.

SBR working groups
At the operational level, there exist working groups for processes & technology, data, marketing & communication, and compliance. These are governmental teams in which experts from the requesting parties, Ministry of the Interior and Kingdom Relations and Logius do the following:

- Specify needs.
- Design processes, taxonomies, communication instruments and procedures.
- Align efforts regarding the development and management of solutions.
- Determine the impact of changes on the chain.
- Resolve issues with services.

Project Board for expansion and internationalisation
In the Project Board, Logius and the requesting parties who have given instructions for expansion look into ways to use the Logius's services more broadly within government departments. This board is chaired by the governmental manager. The activities of parties who are interested in using the generic infrastructure (see also Chapter 10) are controlled from within this Project Board. Logius and the requesting parties also discuss relevant opportunities for, and threats to, international standardisation of business reporting.

9.7.4 *Relevant developments*

Recent developments, particularly the growing numbers of messages and the mandatory use of SBR for system-to-system information delivery, have created the need for a more permanent SBR structure. Thus, the standards, the chains and the generic services are becoming increasingly stable and widely used., leading to the demand for procedural governance (see Chapter 4) to ensure cost-effectiveness. Fewer control moments are necessary and many decisions can be made at the operational or tactical levels. However, this does not apply to all aspects of SBR. Further differentiation is envisaged between the governance of 'business-as-usual' activities and that of elements under development, such as encouraging the use of SBR.

9.8 The central role of the SSC in SBR chains

9.8.1 *The relationship between governance and management*

The difference between the organisation of governance and the organisation of management is whether the decisions are made for steering or for execution purposes. However, this differentiation between chain governance and chain management requires a clearly defined frame of reference. As depicted in Figure 9.9, the boundaries between steering and execution are arbitrary and recursive. In this figure, two organisations are steered by a single board. One organisation has a board of its own, which steers multiple departments. In turn, these departments are steered by the departmental management, etc.

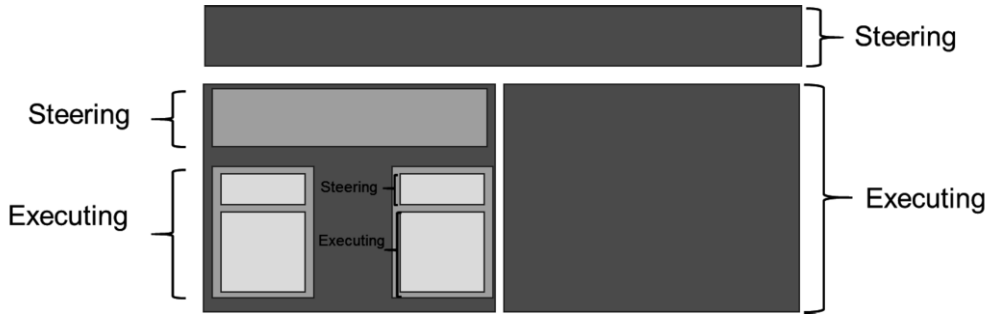


Figure 9.9 – The boundary between steering and executing

The decision-making power of a department can be large or small, depending on the organisational setup (e.g., professional organisation, bureaucratic machine, a business unit or franchise, etc.). The role of the SSC as the executing party is steered by the instructions it formally receives from the various policy clients and requesting parties.

9.8.2 *Instructions for the SSC as part of SBR*

The services provided by the SSC as part of SBR are twofold and include the following:

1. **Coordination services**: public agencies want a standardised approach to system-to-system information exchange and processing so that they can carry out their public task. They have laid down the standardised approach under the name SBR in a framework of agreements. This framework requires facilitation of decision-making (chain governance). Coherence with the other fields of governance should also be coordinated. Versions of this framework should be available to the relevant parties. Logius is responsible for the delivery of a large part of the technical/content-related and administrative support.
2. **Reporting services**: the requesting parties hire an SSC to provide generic, automated processing of business information. This requires the generic operationalization of a number of building blocks, i.e., message specifications, I-process specifications, interface services and message processing services. If disruptions occur or if anything is unclear during the reporting, the organisations must be supported by the SSC. The SSC must also maintain the infrastructure to support parties when the SSC implement changes.

A consequence of this role is that the SSC must be an authority in standardisation, and that it must monitor which developments in standardisation are relevant for SBR. In addition, it should actively manage the demands of the various requesting parties and continuously couple their needs to the architecture, so that those specific requirements can be met using generic building blocks. The way in which the SSC enables parties to set up an entirely new chain in accordance with SBR is discussed in detail in Chapter 10.

9.8.2.1 The service-oriented architecture

Logius is a service agency that works for multiple clients. As a result, it needs to set up its services in such a way that the costs of its services can be allocated fairly based on the orders it receives from clients. The shared services therefore assume a service-oriented approach. How the services are defined and the aggregation level that is used to determine whether the system will be accepted and whether it will work. A fine-grained subdivision (low level aggregation) might permit specific services and a high degree of specific accountability, but the tendering process and the justifications could generate a high level of bureaucracy. Such a situation would not help in terms of timeliness or efficiency. On the other hand, a coarse-meshed subdivision (high level aggregation) leads to a reporting model, but then support for the clients might not be sufficiently specific and the accountability for the services might not fit well with the clients' frameworks. Logius defines a service as a clustering of functionalities with a fixed input and output. The individual services can or should be employed separately by a client. Each service must meet the requirements imposed by Logius as well as those imposed on it by the SBR framework of agreements. The requirements for reusability, flexibility and cost-efficiency—and the architects—determine how a service is defined and its scope.

The characteristics of each service should be defined accurately. It is important that the following elements are described:

- The conditions that apply to receiving the service, in the form of its input requirements.
- The results delivered by the service, in the form of output requirements.
- How the service can be ordered.
- The units (magnitude or quantity) in which the service can be supplied and the associated costs.
- The throughput times for delivery of the service.
- The KPIs for the service.
- The method and techniques used for the service.
- How quality management has been implemented for the service.
- How disruptions in service provision are recognised, acknowledged and resolved.
- How escalation takes place in the event of serious abnormalities in the service provision.
- How the need for changes in the service is recognised and acknowledged, and how it can be met.
- How financial control of the service is organised.
- How reports about the service provision are drawn up.
- How the supplied services are evaluated.

The services provided by Logius in the SBR context are related to the two assignments undertaken by Logius in its role as an SSC. These assignments and the associated services are briefly explained in the sections below.

9.8.2.2 Coordination services

To facilitate the chain governance, Logius provides manpower, resources and expertise for the following services:

- Preparation, coordination and substantive facilitation of SBR discussion forums.
- General support for PR and communication about the SBR framework of agreements.

9.8.2.3 Development and upkeep of business reporting building blocks

As the SSC for SBR in the public domain, Logius uses an extensive service catalogue for the development and maintenance of SBR reporting chains. Figure 9.10 illustrates Logius's current service catalogue for Reporting Services.

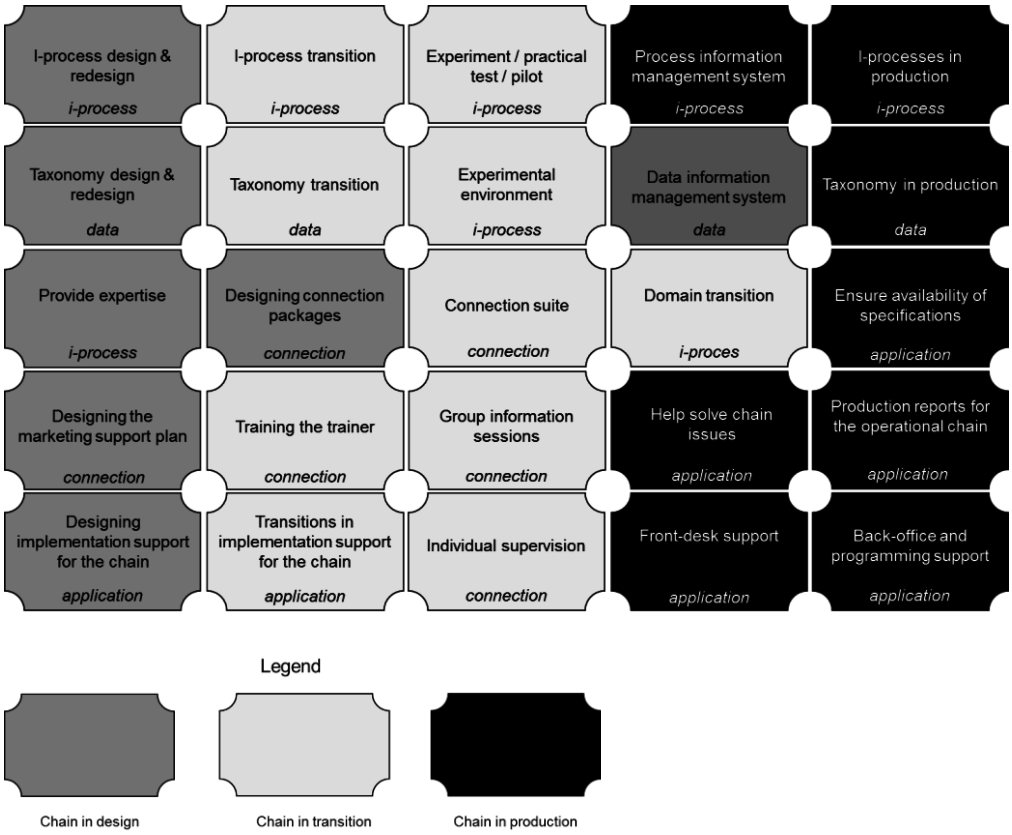


Figure 9.10 – The Logius service catalogue

The services in the catalogue are classified based on four basic functions:

1. I-process management
2. Data management
3. Application support
4. Connection support

Starting with the first function, I-process management focuses on the realisation and operation of the I-processes (information processing). Messages that are disclosed via an interface must be processed in a structured way. I-process management makes sure that processing has been defined precisely for each type of message and that the interface services and processing services are operational and working properly. Continued development of an I-process starts by looking into how the existing interface services and processing functionality can be used to meet new requirements. If necessary, new functionality (a new service) will be defined and realised. To summarise, I-process management is responsible for developing and operating the following building blocks for S2S information exchange and processing:

- Data processing processes
- Interface services
- Processing services

The second element, data management, focuses on the realisation and availability of taxonomies. A taxonomy provides structured descriptions of the exact definitions of the concepts requested in a message, for instance, the concept of 'profit.' The structure of the description makes it possible to set up software in such a way that messages that meet the required specifications can be generated easily using the information from a package. In addition to the data specifications that must be included in a message, taxonomies can also contain simple or complex rules about the content. For example, if an organisation indicates receipt of income from additional activities, details of the scale of these activities may be required. In summary, data management is responsible for the development and operation of the taxonomy used for an I-process.

With regard to the third function, application support focuses on the realisation and execution of support for organisations (including software providers) that are involved in system-to-system information processing. Application support has a 'do-it-yourself' component for those involved as well as an interactive component. The do-it-yourself component contains the information and facilities that are required in order to study and test any questions or application possibilities on matters that may occur. The interactive component is a support counter where targeted questions about the application can be asked or where problems with the application can be reported. In the event of a disruption that could create problems for multiple organisations, application support provides proactive information. From within application support, an incident solution and any required back-office or technical support can be initiated.

The final function, connection support, provides intensive, interactive and do-it-yourself support for setting up and/or maintaining system-to-system information processing between organisations. Connection support is particularly important when the organisations involved have insufficient knowledge to apply system-to-system information processing or related techniques, if the chain or chain functionality is still immature, or if the government has a special duty of care regarding the provision of support. The last would be the case if parties are required *de facto* to link up to the system-to-system information handling for their communication. Connection support is a temporary intensification of otherwise regular support, which for a short period of time is given for a certain target group.

In sum, the generic services are used to support the system-to-system information processing required for various reporting chains. It has been noted before that multiple I-processes can be in effect within a single reporting chain. This would automatically mean that multiple message specifications are used for the task and must all be maintained (e.g., different service messages for tax assessments, declarations, deferral requests, etc.). As the information processing is often done for information from a specific period, it is possible that the same I-processes will support message specifications over a number of years. For example, the same process can be used to declare corporate income tax for the period of 2011 and the period of 2012. Here, application support and connection support must be set up while taking into account the perceptions of the organisations involved in the specific public task.

A user that reports problems with filing its profits may suggest that an error report was received when requesting a deferral of the filing. When requesting parties experience problems in their system-to-system processing, Logius is also a logical point of contact. Logius must therefore coordinate the specific application of the generic services from the perspective of the horizontally integrated chain to ensure that it can be identified by the reporting organisations and requesting parties.

9.8.3 *The service management triangle*

To fulfil the various functions described above, Logius uses a management triangle. This model is centred on the architecture function that is the juncture between the three forms of chain integration found in SBR. Figure 9.11 provides a diagram of the service management triangle.

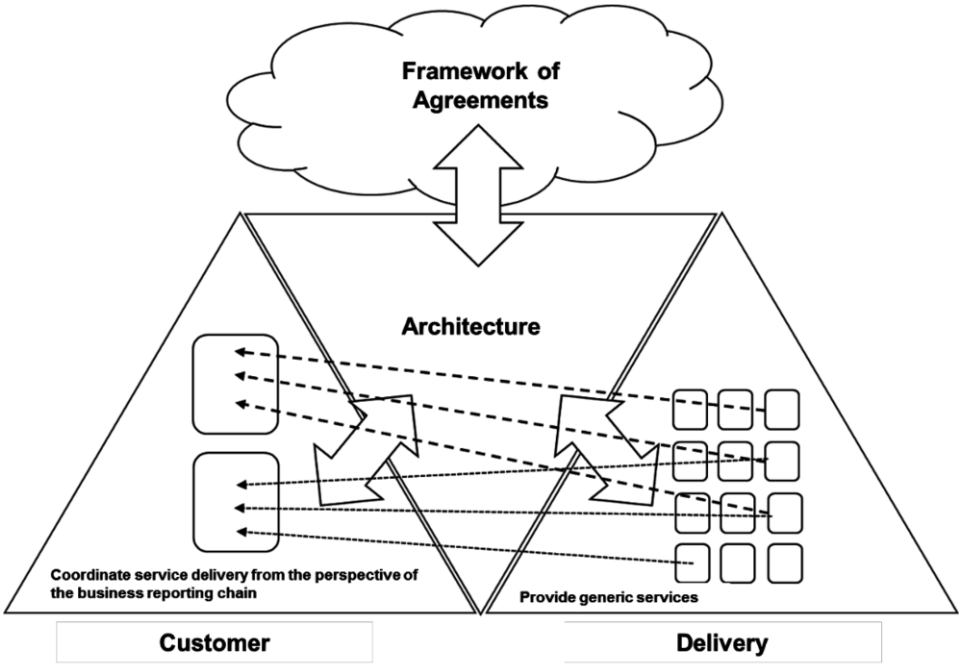


Figure 9.11 – The service management triangle

The customer side (on the left of the figure) is focused on streamlining the current demand for system-to-system information exchange and processing. The perspective of horizontally integrated reporting chains dominates this side. Based on its tasks and needs, the customer shapes the demand for on-going development of system-to-system information exchange and processing for specific reporting chains. Demand management focuses on appropriate demand fulfilment for the reporting chains.

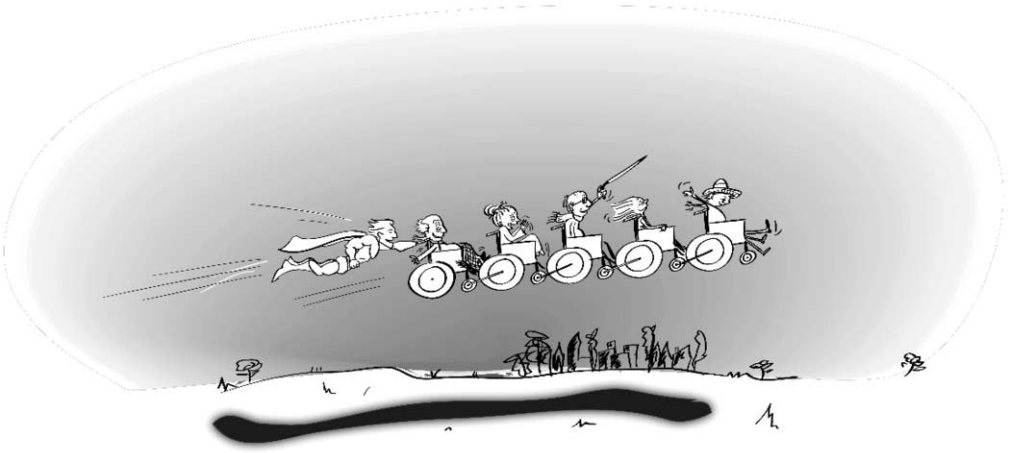
The delivery side (on the right of the figure) is focused on providing the basic generic functions for system-to-system information processing. Here, the vertical chain integration perspective is central. The 'delivery' side makes sure that the service organisation and infrastructure are operational to support the system-to-system information processing for various reporting chains. The orders for services are awarded by the customer organisations and are always linked to a specific horizontally-integrated reporting chain. The solution for a business reporting chain is made up of generic services (shown in Figure 9.11 by the dotted lines from the various services towards the customer side). If system-to-system information processing in the chain is disrupted, delivery management will help normalise the services as quickly as possible. Delivery will be in line with the frameworks imposed by the horizontally-integrated reporting chains. Architecture ensures that the working method of the entire management organisation has been defined and that it fits in with the SBR framework of agreements. On the one hand, this is realised by adopting the standards. On the other hand, the

architecture component also participates actively and contributes to the standardisation forums that are important to SBR. The architecture component monitors compliance with the defined working method and standards from the framework and estimates the consequences of any discrepancies.

9.9 Chapter conclusion

The SBR solution highlights three forms of integration in chain information systems: (1) network integration, (2) horizontal integration and (3) vertical integration. These forms of integration render a variety of interdependencies, creating the need for chain governance. Each form of integration suggests different principles for chain governance. Decisions can become interwoven, since the various chain partners—and the SSC—are active within multiple reporting chains and therefore have an interest in all forms of integration. This entanglement occurs for fundamental changes in particular. Because Logius is specialised in the field and because it is responsible for managing particular components of SBR chains, it is the most suitable candidate to provide orchestration of this complex playing field. In practice, the success of standardisation will depend on the extent to which Logius is able to acquire the required position of authority. Nevertheless, the SSC's organisation must also be suited to the role. In the SBR context, Logius has developed a service management triangle for service delivery, in which architecture plays a central role. Furthermore, this model makes a clear organisational distinction between the customer perspective, which is focused on the horizontally integrated chains in the form of solutions, and the delivery perspective, which develops and delivers generic services.

10 Reporting Chain Reengineering Methodology for the Implementation of SBR



Chapter highlights

- Guidelines for realising the full potential of SBR in candidate reporting chains
- The challenges that are likely to be encountered when implementing SBR and how to deal with them
- Where the SSC can help

10.1 Introduction

Standard Business Reporting (SBR) has progressed into a proven solution for business reporting to administrative authorities. As highlighted in Chapter 1, SBR provides private, semi-public and public organisations with an efficient and effective way to handle various components of their reporting chains. Starting with Chapter 5, various building blocks of the SBR solution that are available for implementation have been discussed in detail. Perhaps, the list of benefits to be gained from SBR has also caught your attention (see section 1.5). This chapter proceeds by addressing the obvious question: how can a reporting chain be reengineered to reap the benefits of SBR?

At first, the answer may appear to be straightforward—something like the following: implement the SBR building blocks and start working with them. However, those who have read the first four chapters of this book will probably disagree with this simply answer. Recall that challenges may arise due to all of the following: mutual dependencies between legislation, policy and technology; coordination between the multiple parties impacted by the implementation of SBR

in the reporting chain; a mismatch between costs and benefits for individual parties when implementing SBR; various forms of strategic behaviour; and the paramount importance of gaining acceptance for the future governance and technology. Fortunately, as SBR has already been introduced into several reporting chains (see Chapter 1), some guidance is available on how to deal with these challenges. The guidance is provided using what we call the 'Reporting Chain Reengineering Methodology for the Implementation of SBR,' from now on, 'the methodology'.

This methodology refers to a coherent set of phases, activities and instruments for implementing SBR in a reporting chain that has not previously made use of the SBR building blocks. The term 'reengineering' is carefully chosen, not only because the methodology includes elements of business process reengineering (Hammer, 1990), but also because the term highlights the need to thoroughly understand what is going on (the 'as-is') before deciding to proceed in transitioning to the 'to-be' situation. Since some reporting chains may not have the characteristics required for SBR, the methodology also includes fixed requirements and decision points. The two main goals of the methodology are the following:

- To facilitate step-by-step decision making regarding the application of SBR in the candidate reporting chain, including development of the business case
- To promote a controlled implementation of SBR in the candidate reporting chain by following a phased approach, and to minimise risks along the way in areas such as IT implementation, organisational change, acceptance and financing.

In order to achieve these goals, the methodology provides guidance for activities such as analysing the as-is reporting chain; redesigning the to-be SBR chain; determining the gap (as-is vs. to be); determining the change strategy; experimenting with SBR building blocks; and scaling up to full use of SBR. Considering the two goals and their underlying activities, this chapter is structured as follows:

- **Section 10.2** sketches out the SBR chain in the to-be situation. This section should give readers an immediate sense of the scope of the methodology. By providing the sketch for Situation B (see Chapter 3 for the terminology used), it becomes clear who (which chain actors) should implement which building blocks in the candidate reporting chain.
- **Section 10.3** provides an outline of the methodology by briefly introducing the relevant phases and providing a substantive guide. The substantive guide allows chain actors to gather all required information to facilitate decision making and promote a controlled implementation.
- **Section 10.4** addresses Phase 1: the exploration phase. This phase is focused on exploring the candidate reporting chain using a Quick Scan. If the results of the Quick Scan are promising, preparation for the following phase can take place.
- **Section 10.5** describes the detailed analysis and redesign phase (Phase 2). The section provides a set of tools and guidelines for analysing the

processes, data and technical building blocks of a reporting chain, including governance. The redesign of a reporting chain in accordance with the SBR building blocks is also described. The resulting views gained regarding the as-is and to-be situations lay the foundation for further decision-making on whether or not to experiment with the SBR building blocks.

- **Section 10.6** outlines the various activities during the experimental phase (Phase 3). These activities promote the real life—yet carefully scoped and controlled—application of the SBR building blocks. Previous experiments have revealed that this phase also might result in minor updates of the business case. In the case of a successful experiment, the subsequent phase—scaling up to higher volumes—can be prepared for.
- **Section 10.7** discusses the fourth and final phase of the methodology: scaling up to higher volumes, meaning the full-scale deployment of the SBR building blocks.
- **Section 10.8** closes this chapter with a reflection on the presented methodology.

Given the goals, scope and depth of the methodology, the primary target audience for this chapter includes the governmental parties that request business information, such as administrative authorities and ministries. However, we expect that the insights captured in the methodology will also prove helpful and relevant to businesses, semi-public organisations, software developers, intermediaries, accountants, trade unions, banks and other typical stakeholders within reporting chains. Since this chapter assumes some understanding of the concepts described in the previous chapters, the reader will be referred to other relevant chapters for the broader descriptions of concepts. We recommend that readers who are interested in the material discussed in Chapter 10 also read Chapters 3, 4 and 9, as they contain complementary insights that are relevant to this chapter.

10.2 Sketch of the SBR chain in Situation B

Thanks to the experience gained from implementing SBR in several reporting chains, we now have a good sense of what the to-be (B) situation will look like for any reporting chain that wishes to make use of SBR. As we saw in Chapter 4, there are two high level components of the change to SBR:

(i) Technology: the chain actors must use at least some of the SBR building blocks (e.g., data standards, interface specifications, use of digital certificates) for their business reporting activities and incorporate these into their systems.

(ii) Governance: the chain actors need to align their decision making with the SBR Framework of Agreements for the various integration forms (horizontal, vertical and network – see Chapter 9).

The following sections briefly elaborate on the above components, focusing on the impact of adopting SBR building blocks. Detailed descriptions of the building blocks can be found in Chapters 5 through 9.

10.2.1 *SBR technology to be implemented*

What are the implications of adopting SBR (the building blocks) for business reporting? Figure 10.1 illustrates the various building blocks of SBR that might have implications for the chain actors in a candidate reporting chain. These elements are numbered and will be discussed according to their numbers.

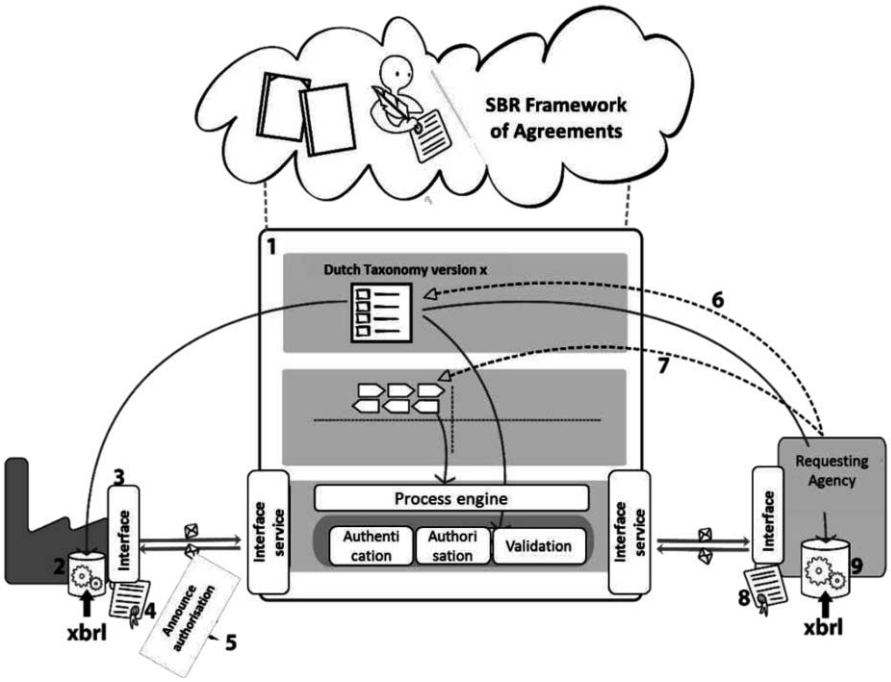


Figure 10.1 – Situation B for an SBR chain

1. In Situation B, the shared service centre (SSC) handles various components of the reporting chain. Thus, the SSC will be introduced as additional chain party in the candidate reporting chain. During the implementation of SBR, the SSC provides the services needed to help chain actors design and implement the SBR chain. This support is offered on a per-project or programme basis.
2. In Situation B, the reporting parties' software should support the SBR data standards (syntax and semantics). If the software already supports an SBR data standard for another reporting chain, it will be easier to meet this requirement. In addition, the principles of the Netherlands Taxonomy that apply to the specific SBR chain should be mapped onto the source systems of the reporting parties.

3. In Situation B, reporting software should incorporate SBR interface specifications that allow for information exchange and pre-processing (the I-processes) using the generic services and infrastructure (see Chapter 7). A large installed base is currently present thanks to the mandatory fiscal reporting using SBR.
4. In Situation B, the actors that submit business reports and receive notifications about them should have a public key infrastructure certificate. As discussed in Chapter 8, SBR prescribes the use of several security measures and procedures in order to safeguard information integrity and confidentiality. One of the measures is the mandatory use of certificates under the Dutch government public key infrastructure regime. A large number of parties have already acquired such a certificate in order to meet fiscal reporting obligations.
5. Depending on the reporting chain, government agencies may provide intermediate notifications on the status of the delivered report (e.g., accepted for processing, rejected) or a final notification (e.g., a content-specific response to a Tax declaration). In the case that notifications are received by an intermediary, the reporting party should provide an electronic authorisation claim to the SSC.
6. In Situation B, the requesting agency publishes which data it wishes to receive by means of a taxonomy and the specific reports (see Chapter 5). Most likely, the taxonomy is an extension of the Netherlands Taxonomy. The SSC provides taxonomy development services, including promoting the reuse of existing definitions of data elements.
7. In Situation B, the requesting agency defines the information processes (I-processes) that it wants to be handled by the generic services. Examples of such services include authentication, authorisation, validation, and archiving. The SSC offers support in designing or redesigning the required I-processes.
8. The requesting agency should possess a valid digital certificate (in accordance with the Public Key Infrastructure of the Dutch government). It is not unlikely for the requesting party to have already acquired this certificate for other reporting chains.
9. The requesting party's processing software should accommodate SBR data standards. If the processing software has already been adapted for other chains, the impact of this modification will be very limited. In addition, the components of the Netherlands Taxonomy that apply to the specific SBR chain and the requesting party's processing systems should be mapped onto one another.

When looking at a specific candidate reporting chain, we might find that several of the listed elements have already been implemented. Consider, for instance, the use of interfaces, certificates and software applications. After all, many actors are typically part of more than one reporting chain. In general, an increasing number of already-implemented building blocks suggest a smaller gap between the candidate reporting chain and a full-fledged SBR chain. If, on the other hand,

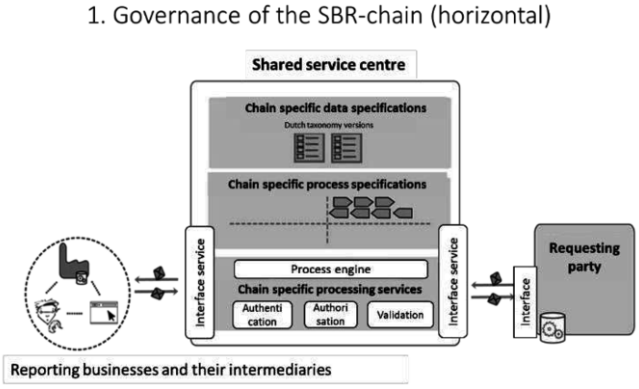
the candidate reporting chain is currently paper-based, the impact of the change will be much more substantial. Fortunately, the transition from paper to digital reporting implies a rapid reduction in reporting costs, and as such, larger benefits in the business case. As this chapter progresses, it will become clear how the differing starting points should be dealt with.

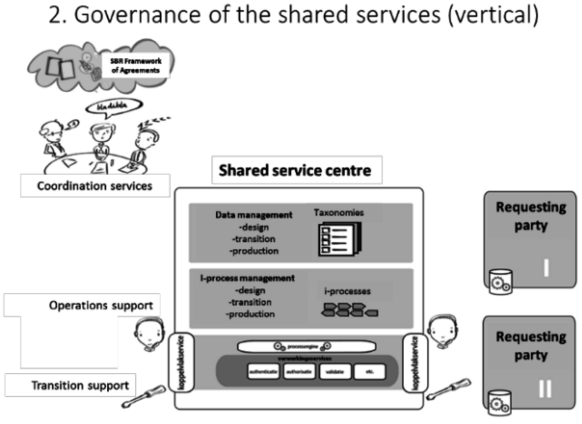
10.2.2 *Aligning with the different forms of SBR chain governance*

With regard to the technological implications, adoption of SBR has implications on the governance of the candidate reporting chain—i.e., the agreements on who will be involved in decision making and how responsibilities in decision making will allocated. Figure 10.2 illustrates the various chain governance structures that actors in an SBR-chain need to align with.

Conceptually, three governance structures are vital for ensuring coherent and cost-efficient SBR service delivery: horizontal, vertical and network governance structures. Each structure corresponds to a type of integration and interdependency amongst chain partners and SBR building blocks. The three structures help distinguish and understand the focuses of the various SBR governance bodies on the strategic, tactical and operational levels. Chapter 9 provides an in-depth elaboration on each perspective.

The first structure is that of horizontal governance. The requesting party that is responsible for the reporting chain and that wants to switch to SBR should take the lead in setting up the governance for the S2S-integrated reporting chain. This means that the requesting party is responsible for the definition of the decision-making structure that governs the implementation of SBR in the candidate reporting chain. Note that there will probably already be some form of collaboration occurring between actors in the reporting chain, either formal or informal. If the candidate reporting chain is paper-based or human-to-system-based, the logical consequence of implementing SBR is that changes in the governance are needed. The requesting party should be aware of the fact that some actors in the chain may already be active in SBR forums for other reporting chains they participate in.





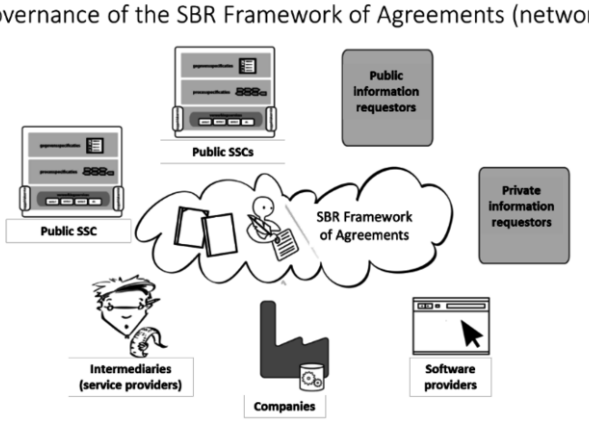


Figure 10.2 – The three chain governance structures that actors in the SBR chain need to align with

The second structure is that of vertical governance. When SBR is implemented, the SSC will handle several components within the reporting chain by utilising the building blocks on behalf of its client. This situation impacts the business case of the SSC and the decision-making rights of its other clients. For instance, when one client of the SSC's services desires major modifications to the building blocks for its own specific chain, the other clients will potentially also have to face a transition. Thus, from a vertical perspective, overarching governance is needed regarding the building blocks shared by multiple clients for SBR. Requesting parties in candidate reporting chains will be incorporated into the vertical governance body that includes all the clients of the SSC's services. In this way, the new parties can take equal part in the applicable decision-making structures.

The third structure is that of network governance. As an SBR chain partner, the requesting party—and perhaps other chain partners as well—will be involved in governing the further development of the overarching governance. All partners in the chain may take part in expert groups and arrange representation for their own organisations in the SBR Platform or the SBR Board (see Chapter 9). Via the public chain and governance mechanism (currently the SBR Steering Committee, the Project Leaders' Meeting and the working groups), the requesting party in the candidate reporting chain can make standardisation agreements with other government agencies regarding the application of SBR. These forums are also the arena for developing policies on public-private cooperation regarding SBR and its underlying standards.

10.2.3 *The impact on the SSC is kept to a minimum*

We will now use an example to illustrate why and how the impact on the SSC is kept to a minimum when a candidate reporting chain is implementing SBR. For our example, take the fact that there are currently no agreements regarding the use of Inline XBRL in the Netherlands Taxonomy Architecture. Suppose that a new requesting party desires support for embedding XBRL tags in HTML documents using Inline XBRL. For both the SBR technology and the SBR chain governance, this additional feature will trigger a substantive impact on the SSC. Both the technology and governance in Situation B must be altered, a business case should be developed and backing needs to be obtained from all the other requesting parties that collaborate in the SSC. This will make the change considerably more complex for the actors in the candidate reporting chain. Therefore, for the initial implementation, the principle is that the changes in the building blocks should kept to a minimum. The great benefit of leaving the building blocks as they are is that actors of the candidate reporting chain leave resources for other more important aspects of the change. Once the chain is in production, there remains, after all, the option for further development, for which some experience with SBR might also come in handy.

10.3 An outline of the methodology

Reengineering a reporting chain is never easy, not even if some of the chain partners have done it before and/or when Situation B is, to some extent, known beforehand. The starting point of any candidate reporting chain will differ. For example, some candidate reporting chains will be S2S-based, whereas other candidate reporting chains may exchange data on paper or by means of a human-to-system solution. On top of that, the specific technical, political or administrative, historical, legal and organisational characteristics of the candidate reporting chain must be considered. Consequently, when implementing SBR, each chain follows a unique path. That is why our methodology provides leeway for addressing chain-specific characteristics. This means that there is room to tailor the methods and techniques for analysis, design, testing and gaining stakeholder commitment along the way. Nevertheless, the leeway is restricted through some elements of the methodology:

1. Four fixed phases and their corresponding deliverables and go/no-go decision points.
2. A substantive guide to be used as the actors progress through the phases, in order to gather all the required information for decision making and implementation.

This chapter will provide an outline of the methodology. In Section 10.3.1, the four phases of the methodology are presented, with special attention paid to decision making and hurdles in gaining acceptance. In Section 10.3.2, the substantive guide is presented.

10.3.1 *Implementing SBR in four phases*

The path taken by chain actors in implementing SBR always progresses through four phases: exploration, detailed analysis and redesign, the experiment, and scaling up. The exploration phase starts when chain partners express their interest in SBR and make contact with officials from the SSC. For the SSC, the chain then becomes a candidate reporting chain for SBR implementation. The goal of the exploration phase is to determine whether or not a reporting chain is suitable for the application of SBR. This is done using a Quick Scan, which results in a recommendation of whether or not to progress to the second phase. If the answer is affirmative, the ambition for one or more reporting types within the candidate reporting chain is defined. The subsequent phase translates this ambition into a roadmap with clear goals.

The second phase includes a detailed analysis and redesign of the reporting chain. This phase is started if the Quick Scan has suggested that applying SBR could potentially be beneficial. A redesign of the reporting chain is made, consisting at a minimum of an extension taxonomy, a process redesign for I-processes in BPMN and the design of operations support. In addition, a market lobby plan is drawn up. The market lobby plan needs to encompass the requesting party's long-term vision of SBR's role in satisfying its overall reporting needs (e.g., which other reporting flows and chains can be transformed?). It is perfectly

conceivable that a requesting party will initially use SBR only for a certain subset of actors with reporting obligations. In terms of the chain governance, it is important that the partners in the candidate reporting chain reach a vision for participation in the SBR forums and that the partners also pay sufficient attention to their organisational governance. In short, the deliverables of the second phase (including a detailed analysis, a feasible redesign and a concrete roadmap) should contain sufficient information for decision making regarding whether to proceed with reporting chain reengineering.

The decision to begin the third phase (the experiment) is the most crucial point in the methodology. In the experiment, the chain actors will put SBR into actual use in their chain. The companies and intermediaries (e.g., accountancy firms, bookkeepers, software providers) that are going to experiment with SBR will therefore increasingly require clarity regarding future policy so that they can justify the investments required. In order to properly manage expectations, the principle in effect when the experiment commences is that *if no significant issues arise during the experiment, the application of SBR within the candidate reporting chain shall be continued in the years that follow, with the aim of implementing SBR in accordance with the ambition set for the chain(s).* The critical chain partners—particularly the requesting party and the relevant policymakers—should be committed to realising this vision.

This commitment is the first of two acceptance hurdles that the chain partners will come across in the chain-reengineering programme. Sufficient backing among critical chain partners provides the green light for starting Phase 3. The experiment is then used to test the redesign. Actors connecting to SBR for the first time can test information exchange via their software using an SBR interface specification. Ultimately, different interactions will be tested, including the connection to the generic infrastructure, the delivery of reports to the requesting agency and the accessibility of return information such as status updates and notifications provided by the requesting agency. If specific services in the generic infrastructure have been developed for the candidate reporting chain, these will also be tested. Emerging incidents, disruptions and problems in the candidate reporting chain will be sorted out during this phase. Carrying out the experiment allows the chain actors to see that the SBR chain is functioning as it should. If the experiment is completed without any hitches, it can be assumed that implementation of SBR in the candidate reporting chain will proceed according to plan. During the experiment, the implementation programme governance should gradually shift to the designed chain governance.

During the fourth and final phase—scaling up—the target community of users is gradually connected to SBR. Connecting the users is the second acceptance hurdle that the chain partners will likely encounter. As explained in Chapter 4, in order to realise the ambitions of the programme, all actors belonging to the target community should implement SBR. Experience has revealed the quintessential importance of demonstrating the reliable application of SBR in the candidate reporting chain during the experimental phase. It is just as important for

the SSC to help the actors not yet connected to SBR to incorporate SBR specifications for interfacing and data (syntax and semantics). Reporting chain reengineering is complete once the entire target community can exchange information according to the SBR specifications. This will generally mean that the legacy solution is discharged. Figure 10.3 provides an overview of the four phases.

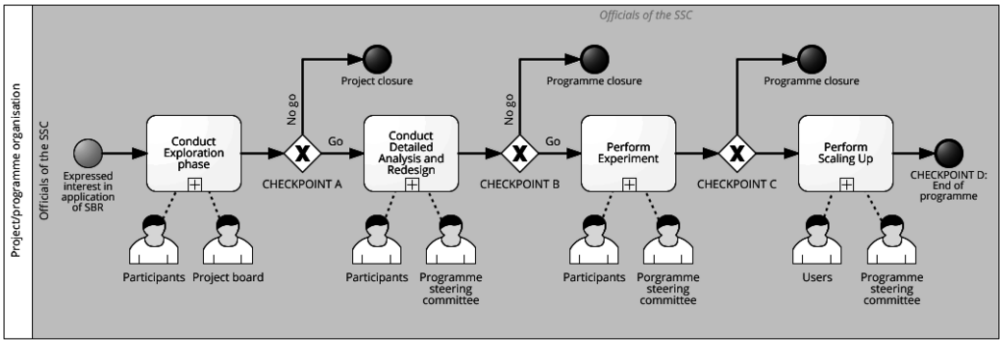


Figure 10.3 – The four phases for implementing SBR in a candidate reporting chain and the associated checkpoints

Specific targets are set for each phase along with a specific approach (see Section 10.3 to 10.6). As they progress through the phases, the chain partners will encounter Checkpoints A through D (see Figure 10.3). Each checkpoint symbolises both the completion of one phase and the commencement of the next. These checkpoints have the following functions:

1. The first function of the checkpoints (with the obvious exception of the final checkpoint) is to make a **go/no-go** decision about whether or not to proceed to the next phase. Using decision points like these helps the chain partners to determine whether the process has delivered the anticipated results and whether it will continue to do so.
2. The second function of the checkpoints is to make sure, before the new phase is launched, that the activities of the previous phase were completed with sufficient depth, scope and quality. 'Softer' requirements can also be imposed at a checkpoint. For example, Checkpoint B has the requirement of there being sufficient backing among key chain actors for the intended application of SBR before starting the experiment. The reason for this function is that chain actors in the candidate reporting chain might choose to conduct elements of each phase without the help of the SSC. For example, the requesting agency will develop the taxonomy by itself or will deal with the market lobby. In this case, the SSC serves as 'intake agent' before starting the next phase in the methodology.

Those who have experience with project management methodologies (e.g., Prince2, Scrum) and programme management methodologies will encounter familiar techniques when using the proposed methodology. Techniques such as specifying gateways and checkpoints, prioritising, scoping, setting up a project board, escalation risks registers, quality management, and so on, are common in

most methodologies for a good reason. They are also relevant for chain reengineering. Instead of repeating the information from many books that cover these techniques in great detail, we assume here that sufficient knowledge about these methodologies and how to apply them in practise are available. An interesting note with respect to such methodologies is the transformation that occurs between the first and second stages. A project organisation paves the way of a programme organisation, instead of the other way around which is more common. As was discussed in Chapter 4, an undertaking as comprehensive and sophisticated as implementing SBR in a candidate reporting chain with its own legacy can only be realised through a prudently designed programme. However, even more so than in the other phases, the required effort and resources in the first phase should be kept to a minimum. Thus, a project organisation is more suitable.

Thus far, we have only discussed the process-related aspect of the methodology. There is, however, a more substance-oriented aspect to reporting chain reengineering that should not be neglected. The following section provides the substantive guide for reporting chain reengineering.

10.3.2 *Substantive guide for reporting chain reengineering*

Chain actors can make use of the substantive guide in order to gather all the information required during reporting chain reengineering. First, the substantive guide will help chain actors to develop their business case, which is needed for decision making. In the business case, the current chain (Situation A) is compared to the SBR chain (Situation B). Thus, information on both situations should be gathered and the need for change should be established. Second, following the substantive guide will help chain actors to promote a controlled implementation and to minimise risks during the process by gathering information regarding how to get from A to B. This includes the change undertaking (the actions required for the change) and the change strategy. Gathering information about both A and B, and how to get from A to B, will help bring forward the implicit knowledge of the chain experts and contribute towards a commonly shared picture. Those who have read Chapters 3 and 4 will recognise the importance of these matters. An additional benefit is that the chain actors involved will be able to improve their awareness of the interdependencies within the reporting chain from the very first day.

Let us now take a closer look at the three areas of information to be gathered in order to get from A to B during reporting chain reengineering:

1. The change desire. The change desire consists of the difference between Situation A and Situation B for the fulfilment of the reporting chain's public function. This difference is expressed along the following axes: data (Chapter 5) – I-processes (Chapter 6) — technology (Chapters 7 & 8), which together make up the technology dimension, and the chain governance component (Chapter 9). Trends, developments and factors that could affect the need for change are also examined.

2. The change undertaking. The actions required for the change should be examined for each actor, making a distinction between the knowing-ability-motivation areas (see Chapter 3) along the technology and chain governance dimensions (see Chapter 4).
3. The change strategy. The change strategy refers to the dynamic set of assumptions for realising the desired change in the candidate reporting chain, taking into account the actions required for the change. Distinctions needs to be drawn between the following:
    a. Potential starting points for the change, such as a specific business reporting flow or the actors who should be involved in order to allow the change to commence.
    b. How to financing the resources required for reporting chain reengineering.
    c. The roadmap for the implementation of SBR building blocks, including a proper planning.
    d. Transition support offered by the SSC to the candidate chain actors during the change.

For an implementation to be successful the actors' desire to change should be proportionate to their individual actions required for the change and all chain actors should deem the chosen change strategy sufficient to realise the changes. The change desire, change undertaking and change strategy are interrelated: Any choice in the area of change desire is likely to affect the change undertaking, which is likely to affect the change strategy. Choices regarding, for instance, the scope, the functionalities, the actors involved, the transition support offered, the chosen throughput times and the fit with other projects will be made continuously. The substantive guide helps actors with aligning the change desire, the change undertaking and the change strategy in order to keep the three in balance along during the reengineering process.

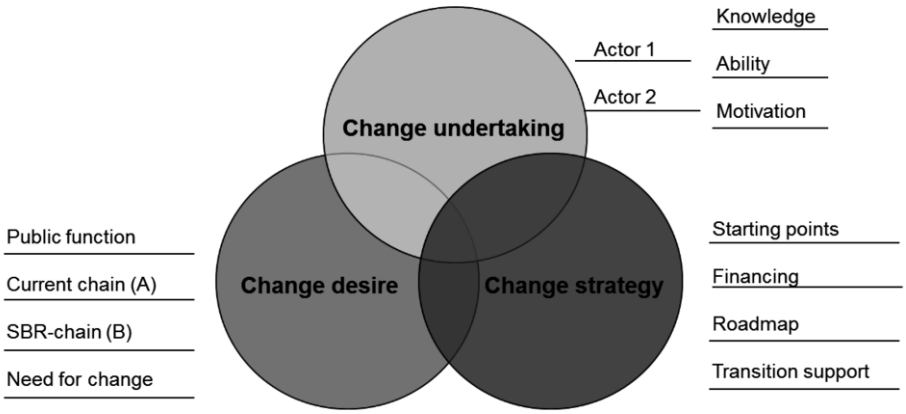


Figure 10.4 – Change desire, change undertaking and change strategy: Three areas that chain parties should balance during reporting chain reengineering

Each of the four phases of the methodology emphasises different areas. The exploration phase is focused on gathering information about the chain's public function (the function of the business reporting chain in society), the current situation (Situation A) and the need for change. The detailed analysis and redesign phase is focused on specifying the A and B situations in greater depth, and on the change undertaking and some aspects of the change strategy (such as financing). The SBR chain, the change undertaking and the change strategy are determined during the experiment. When scaling up, the chain actors, in principle, stick with the defined change strategy, unless exceptions and/or unexpected events require an adjustment.

The following diagram provides an overview of each phase's emphasis on information gathering in the areas of change desire, change undertaking and change strategy.

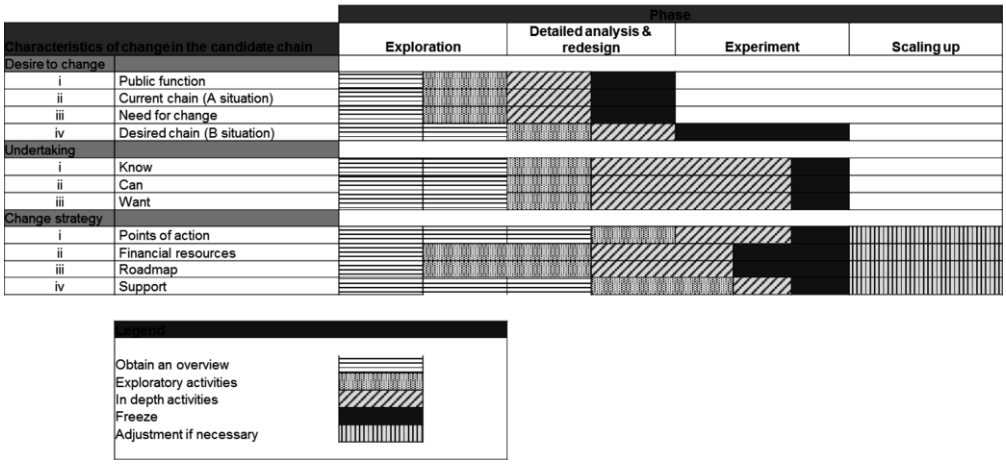


Figure 10.5 – The emphasis of each phase on change desire, change undertaking and change strategy

In each phase, the chain partners examine the change desire, change undertaking and change strategy in further detail. The following tables offer generic questions by which to gather the information for each area. Each phase allows the chain actors to address more questions and obtain more detailed answers. The number of generic questions regarding the change undertaking and change strategy are more limited, because the questions that are appropriate depend on the insights obtained as the programme evolves, and are therefore more difficult to predict in advance.

Considering the public function of business reporting as part of the desire to change, the chain actors should look for answers to the following questions.

Table 10.1 – Relevant questions regarding the public function of the candidate reporting chain

Change desire: Relevant questions regarding the public function of the candidate reporting chain	
The function of business reporting	• What goal is achieved through the disclosure of business information? • Which requirements does this goal impose on the quality of business information (i.e., its correctness, accuracy, timeliness and reliability)?
Legal basis for business reporting	• What is the legal basis that commands business to provide business information? • Which laws and regulations legitimatise the requesting actor's claim to business information?
Compliance requirement (will vary by country/ continent)	• What are the requirements under the Online Administrative Business Act? • What requirements are derived from the unwritten general principles of good governance? • What are the requirements under the Public Records Act of 1995 and its subsidiary regulations? • What are the requirements under the Personal Data Protection Act? • What are the requirements under the Services Act? • What are the requirements under the Competitive Trading Act? • What are the requirements under the Telecommunications Act? • What are the requirements under the Personal Public Service Number (General Provisions) Act? • What requirements are derived from the Guidelines for Annual Reporting and Book 2 of the Dutch Civil Code? • What requirements are derived from the standard frameworks regarding assurance? • What requirements are derived from the regulations regarding information security? • What are the requirements under sector-specific legislation and regulations?

Table 10.2 provides a supplementary set of questions regarding the candidate reporting chain itself. Answering these questions should result in a deeper understanding of the actors, chain governance, processes, data, technology and cost-efficiency of the chain, in its current state.

Table 10.2 – Relevant questions regarding the current chain (Situation A)

Change desire: Relevant questions regarding the current chain (Situation A)	
Chain organisation	• Who are the requesting actors in the reporting chain? • Who is/are the policymaker(s)? • Who are the reporting parties in the reporting chain? • Which intermediaries/service providers operate in the reporting chain (e.g., accountants, software providers, business administration offices)? • Which other public actors are involved (e.g., regulatory bodies, supervisory agencies, supporting agencies, etc.)? • Which umbrella organisations are involved (e.g., sector associations, etc.)? • Which other actors are involved (e.g., Council for Annual Reporting, etc.)? **For public and semi-public actors:** • What is the public task of the organisation? • Which legislation and regulations legitimise the execution of this public task? • What are the financial and societal impacts of the organisation's operations? • How fixed are the defined tasks and the budgets of the governmental actors? • What relevant historical events have shaped the current organisational situation? • What additional public tasks are there in relation to the reporting parties? • Is information processing the core business?

	For privately-owned actors: • How can the market environment be described (monopoly/oligopoly, number of providers and customers)? • What demands are imposed on newcomers (technical, legal)? • What is the turnover in numbers of actors? • How much pluriformity exists, for instance, in culture and scale (e.g., turnover, head count, strategy, earnings model, customers)? • Is information processing the core business? • Do privately-owned actors include reporting parties with offices abroad, or who are themselves foreign entities?
Chain governance	• Which aspects (e.g., standards, technology, process, data model) determine interdependencies within the reporting chain (see Chapter 9)? • Who is the policymaker? • Who finances the operation of the reporting chain? • Is there a central chain governance or are there formal consultative structures? • Which actors and stakeholders are part of the chain governance or the formal consultative structures? • Which actors and stakeholders are currently not part of the chain governance, but might be impacted by the reporting chain reengineering? • To what extent are decisions taken by consensus or imposed from above? • What is the balance of power within the chain? • How are changes (e.g., standard changes, development, major changes) managed? • Are the agreements made soft (informal) or hard (formal)? • Do the agreements in place apply to all aspects that determine interdependencies between chain parties? • What are the consequences if actors do not stick to the agreements made? • To what extent do the actors realise that they are part of the chain, or do they merely focus on their own part in it? • To what extent are there applicable covenants or agreements? • To what extent do international standard frameworks or cooperative agreements play a role?
Processes	• What message flows can be distinguished? • How do the message flows fit together (incorporate other business reporting domains)? • To what extent do the message flows utilise the same components in the chain? **For each message flow:** • How are the data elements that are to be reported published? • How are the standards (e.g., interface specifications, identification mechanisms) provided to the various actors in the chain? • Are there multiple routes for the same information request? • How is access provided to the electronic pathway? • How does the reporting party record, store and collate the requested data? • Which of these activities are performed by staff and which by IT systems? • How is cooperation with the accountant arranged (if applicable)? • Who are the various process owners? • How is a secure connection initiated? • Is there a simple data flow (fire and forget) or a conversation/dialogue (request and response)? • Are notifications also issued? • Are return flows pushed or are they accessed/retrieved by the recipient? • Do notifications only follow the delivery of a business report? Are there other triggers for notifications? • Which data processing steps are executed? • Are there stages or steps in the chain that are optional? • How many messages are expected each year? • What is the frequency of the messages? • Are there particular peak moments or deadlines?

	• Are business rules executed in the chain and if so, at which moments? • What happens if the information delivered contains errors? • What happens if an error occurs in the information pre-processing? • Is business information disseminated to a specific community or society, and if so how? • What happens if reporting parties fail to meet their business reporting obligations?
Data	• How are the data elements to be reported defined? • What is the content of the submitted business reports and what aspects of the content are identical between multiple business reporting flows? • What kind of information is submitted on paper and what is sent in electronically? • In what format is electronic data submitted? • Do the reports have a fixed reporting structure? • Do all chain partners use the same reporting structure? • Is there a central data model / taxonomy providing definitions for the relevant data elements? If so, who manages it? • Do electronic messages have a fixed syntax? • Does this syntax offer the desired degree of standardisation on one hand and flexibility on the other? • How often does the syntax change? • Do all actors interpret the meaning of the definitions in the same way (semantics)? • Do actors collectively decide on agreements? • How often does the set of definitions change? • Is an automated check of the completeness and syntax of the messages possible? • Are data elements being requested that have already been included in the Netherlands Taxonomy?
Technology	• Do reporting parties already process business information automatically? If not, is there a business case for automated processing in the sector? • Do requesting actors already process submitted business information automatically? • Is system-to-system information exchange already a possibility? • How is the secure connection established? • What is the scope of the message exchange (number over time)? • What demands are imposed on the message exchange in terms of delivery intervals, processing times and correctness of processing? • Is it possible to include multiple entities with business reporting obligations in a single message, or should they be sent in separately? • What is the scale of IT support and its associated procedures? • How mature is IT support? • How is information security guaranteed? • How good is the quality of the software used in the various stages of reporting? • Is the software to be used developed in-house or bought in?
Cost-effectiveness	• What are the estimated costs to the public actors of running the reporting chain? • Is there a cost structure and if so, what efforts are defined and what are the proportional costs for management, continued development and unassigned costs? • Which party or actors provide the required funds? • What are the costs to the reporting parties for complying with business reporting requirements (a good approximation)? • What are the overall costs within the reporting chain (a good approximation)? • To what extent does the information acquired through the existing reporting chain permit the requesting actors to carry out their tasks, and to what extent does the reporting chain fulfil the public function in the broader sense (effectiveness)? • How appropriately are the people and resources utilised within the reporting chain (efficiency)? • Are the current costs reasonable, given the targets (cost-effectiveness)? • Are there any anticipated changes in future costs, given the expected future targets?

Considering the view of Situation B as part of the desire to change, the chain actors should also seek answers to the following questions.

Table 10.3 – Relevant questions regarding the desired chain (Situation B)

Change desire: Relevant questions regarding the SBR chain (Situation B)	
Chain organisation	• What links and actors will comprise the future reporting chain? • What other actors will have relevant roles around the chain?
Chain governance	• Which actors will be included in the SBR chain governance? • What will be the responsibilities of each actor?
Processes	• Which message flows will be distinguished (I-process)? • Which generic services will be addressed in each message flow?
Data	• What are the elements of the future taxonomy? • Which entry points will be used?
Technology	• What are the service levels for the generic services used? • How much capacity should be available?
Cost-effectiveness	• What will be the costs of operating SBR? • What is the cost structure for the operational costs? • From which party or actors will the budget be obtained?

Considering the need for change is also part of the desire to change. Thus, the chain actors should also address the following questions.

Table 10.4 – Relevant questions regarding the need for change

Change desire: Relevant questions regarding the need for change	
Push factors	• How cost-effective is the reporting chain as-is? • Are there significant bottlenecks in the as-is reporting chain that necessitate changes? • Have developments occurred at the national level that necessitate changes within the reporting chain (social developments, economic developments or political developments)? • Is the domain subject to changes in terms of content, for example, because of technological advances (e.g., the rise of ERP, Software as a Service, open data)? • Is this domain currently in the political or social spotlight (for example, because of a lack of transparency)? • Is there any legislation or regulations that are forcing changes within the reporting chain? • Is there backing for the reporting chain, or is it a point of debate amongst stakeholders? • Do particular actors express the need for change more strongly than others? • Is the domain subject to changes in technology (e.g., the rise of ERP, Software as a Service, open data)?
Pull factors	• Can synergy be achieved by taking on multiple business reporting flows (reducing the administrative burdens)? • How great are the benefits for the requesting actors if the SSC is used (thus allowing for S2S information exchange, shared costs, mature services, compliance by design, information quality assurance through automated pre-processing, best practices chain governance, expected improvement of data quality, facilitate changes in legislation)? • Which potential opportunities can be created for service providers in the sector (e.g., the introduction of new services and products)? • What other potential benefits are there (e.g., benchmarking, open data, predictive analytics)?

In considering the magnitude of the undertaking, the chain actors should look for answers to the following questions.

Table 10.5 – Relevant questions regarding the magnitude of the undertaking

Change undertaking: Relevant questions	
'Knowledge' (per actor)	• How familiar is the chain actor with S2S integration of reporting chains? • How familiar is the chain actor with the technology used in SBR? • How familiar is the chain actor with the SBR Framework of Agreements? • How certain is the chain actor about its ability to meet internal preconditions for, and the impact of implementing, the SBR technology? • How certain is the chain actor about its ability to meet the internal preconditions for, and the impact of implementing, the SBR chain governance?

'Ability' (per actor)	• Competencies and capacity required:
	  • Has the actor been through comparable chain-reengineering programmes? If so, what were the results?
	  • Which SBR building blocks has the actor already implemented (see Section 10.2)?
	  • Can the actor free up the requisite capacity?
	• Resources required:
	  • Is the required investment proportional to the budget or turnover?
	  • Can the requisite resources be made available?

'Motivation' (per actor)	• What are the business goals set by the actor? • Will implementing SBR help attain these goals? • What alternatives are available for achieving these goals? • Does implementing SBR help the chain party achieve the set goals cost-effectively?
Coordination	• What dependencies need to be allowed for during implementation? • Which of the chain actors' activities need to be carried out sequentially during the implementation? Which can be carried out in parallel? • Who coordinates the actors' activities?

In considering to the change strategy, the chain actors should look for answers to the following questions.

Table 10.6 – Relevant questions regarding the change strategy

Change strategy: Relevant questions	
Starting points	• Is there a business reporting flow in which it would be particularly suitable to apply SBR? • Which actors want to take a pioneering role? • Where can implementing SBR produce quick wins with minimum effort? • Which points does everyone agree about and which are contentious?
Financing	• What is the expected investment for implementing SBR? • How are the costs spread out over time? • From which actors can budget be reserved for implementing SBR?
Roadmap	• How can synergy be created between implementing SBR and policymaking related to information management in the broader sense in the related business field? • How does implementing SBR fit in with other projects/programmes? • Along what lines can implementation of SBR be realised? • Which stages can be seen in the implementation? • What throughput times would be realistic?
Transition support	• Which chain actors' capabilities need to be supported in what way? • Which chain actors may need some kind of concessions to encourage them to take part? • What services from the SSC will be used?

The three areas that should be balanced—change desire, change undertaking and change strategy—and the associated questions form a substantive guide that chain actors can use to examine the candidate reporting chain. The insights

obtained in Chapters 3 and 4 are particularly evident in these questions. To get the best possible view of a reporting chain, open-ended questions are used as much as possible. A yes/no checklist might seem easier for answering and assessing the questions, but it would restrict the potential array of answers. The disadvantage of using open questions is that they require greater expertise of whoever is conducting the Quick Scan. It should also be noted that although the questions are instrumental, the list is not exhaustive.

With insight the insight above provided regarding the four phases and the substantive guideline, we can now discuss each phase in further detail.

10.4 The exploration phase

The starting point for applying the methodology is when one or more actors of a reporting chain express interest in the application of SBR for their reporting chain and are in contact with representatives from the SSC. These can be policymakers, reporting parties, requesting actors and/or service providers. The exploration phase aims to achieve the following goals:

- Interested actors are provided insights into the benefits and limitations of applying SBR and the supplementary methodology.
- Interested actors have a structured view of how the business reporting in the candidate reporting chain would work and whether any bottlenecks would be present.
- Interested actors have a good idea of whether or not the candidate reporting chain is suitable for the application of SBR.
- Interested actors are provided a reasoned recommendation about whether or not to carry out the detailed analysis and redesign.
- The intended requesting party and/or policymaking principal responsible for a reporting chain has a clear goal in mind for SBR within the candidate reporting chain(s).
- The programme organisation and the associated forums for the upcoming projects have been set up.
- The detailed analysis and redesign phase has been prepared for.

Three sets of activities occur during the exploration phase: the exploratory meetings, the SBR Quick Scan and the preparations for the follow-up work. The chain actors go through these activities sequentially. The exploratory meetings and the Quick Scan end with a decision-making point.

Figure 10.6 provides an overview of the set of activities in the exploratory phase. The figure is consistent with our advice to always model processes and underlying activities using the BPMN standard. Chapter 6 provides more details on this standard.

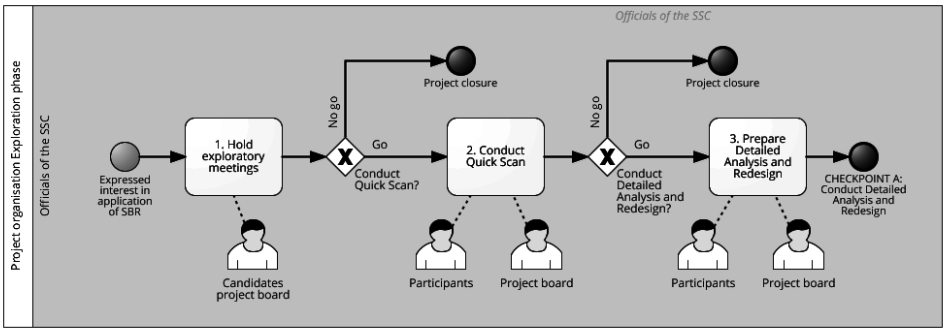


Figure 10.6 – Three set of activities and two decision points during the exploration phase

The following subsections elaborate on the three sets of activities.

10.4.1 *Exploratory meetings*

Actors in the candidate reporting chain (typically the candidates for the project board) engage in exploratory meetings with representatives of the SSC (e.g., managers) or members of the overarching SBR governance board (e.g., the SBR commissioner). These meetings can be triggered by SSC representatives (business development experts) or by candidate reporting chain representatives. During the exploratory meetings, the interested actors gain awareness on the capabilities and limitations of SBR. Together with the interested actors, the SSC can use the meetings plus desk study to sketch out an initial picture of the reporting chain.

The SSC official should mention to the interested actors the option of conducting a Quick Scan. The Quick Scan allows the chain actors to further explore the possibilities of SBR for the candidate reporting chain in a structured manner. If the chain actors agree on conducting the Quick Scan, they can assign this task to the SSC. The goals and deliverables of the Quick Scan are provided by the methodology. However, together with representatives of the SSC, the candidate members of the project board determine the scope, proposed project organisation (including how the various chain parties will be involved) and planning of the Quick Scan, and assess the chain-specific risks and/or attention points for the process.

Table 10.7 – Overview of the deliverable of the exploratory meetings

Action plan for the Quick Scan	A document providing a description of the following: 1) Background, project goals, deliverables, scope, assumptions 2) Outline of the approach, phases and decision-making, activities, project planning, project organisation 3) Quality management and risk management

10.4.2 *SBR Quick Scan*

The SBR Quick Scan offers chain actors substantiated insights into the way the current reporting chain works and what it would mean to apply SBR in that

chain. Based on the findings of the Quick Scan, the SSC officials draw up a recommendation about whether or not to continue on to Phase 2, in which an in-depth analysis is carried out. The SSC should also consider the high-level business case, at least addressing the intentions behind the use of SBR.

The Quick Scan generally starts with a kick-off meeting with the participants proposed during the exploratory meetings. During the Quick Scan, the SSC officials explain SBR and the approach to be used for the Quick Scan. The aim of the kick-off is to finalise the scope and bring in the participants. It is important to record the names of the participants on the team sheet so that the further appointments and meetings can be scheduled.

After the kick-off, representatives of the involved actors and the SSC officials conduct various interviews and workshops. The number of workshops, their exact content and the profiles of the participants depend on the characteristics of the candidate reporting chain. At least two workshops will likely be needed, whereas more than six would be excessive for the purposes of the Quick Scan. In these workshops, the actors describe the A and B situations according to the substantive guide. The possibility of applying SBR is appraised, as are the need for change and the magnitude of the undertaking. There are also plenty of opportunities to think about the change strategy.

The information gathered is put down on paper by SSC officials. This provides 'closure,' in which the content of the deliverables is determined together with the actors. Along with providing a recommendation, the document also gives the interested actors a picture of the possibilities that SBR offers for the candidate reporting chain. The expected deliverables from the Quick Scan step are shown in Table 10.8.

The Quick Scan concludes with a go/no-go decision as to whether or not to continue to the detailed analysis and redesign phase. It might also be possible that the candidate reporting chain is well suited for SBR, but needs to delay the start of the subsequent phase. If a decision is made to start Phase 2, the last part of the exploration phase is to prepare for the following phase.

Table 10.8 – Overview of the Quick Scan deliverables

Quick Scan	A document produced by the Quick Scan participants providing, at a minimum, a detailed description of the following elements: 1) background, goals, scope, readers' guide 2) the public function of the business reporting 3) chain actors 4) chain governance 5) processes 6) data 7) technology 8) cost-effectiveness of the chain 9) the need for change 10) an overview of Situation B for all components 11) an overview of the change undertaking 12) an overview of the change strategy 13) a recommendation regarding the go/no go decision to proceed to Phase 2 14) points for attention for the detailed analysis and redesign phase 15) management summary 16) list of abbreviations and glossary
Business case (outline)	An estimate in broad lines, covering the following: 1) the intentions for Situation B – the role that SBR is going to play in the business reporting domain 2) the current costs – administrative and operational costs 3) the future costs – administrative and operational costs (and benefits, including opportunities) of applying SB 4) investment costs and investment risks 5) alternatives

10.4.3 *Preparing for Phase 2*

Ideally, Phase 1 has laid the groundwork for the planning of Phase 2. Phase 2 requires more time from the actors than Phase 1. The main reason for this is that the anticipated deliverables of Phase 2 are more substantive and detailed than those of the first phase. In order to assure a successful start for Phase 2, actors should have already made available the necessary human and financial resources during Phase 1. The action plan should provide a precise picture of the activities needed and how they should be planned in to achieve the desired results.

In addition, a programme organisation should be set up. The redesign of the reporting chain consists of an integrated whole that includes the processes, data, technology and chain governance, as well as the corresponding support for the transition and operations. For each area, specific design questions will arise that require the knowledge of various experts. Moreover, the design should fully comply with legislation and standards. Due to the complex nature of the design phase and subsequent phases, the methodology should be executed via a programme for effectuating change. As was discussed in Chapter 4, something as comprehensive and sophisticated as the design and implementation of SBR in a candidate reporting chain with its own legacy can only be realised through a prudently designed programme. Figure 10.7 illustrates a programme organisation, to serve as a reference.

The reference programme organisation depicted in Figure 10.7 consists of a steering committee (strategic level) and project teams. Note that the actors in the programme organisation should preferably reflect the governance of the chain to be set up (see Chapter 4). Given that it is a programme, steering from higher levels will be required to a greater extent than will need to be the case once the chain is actually operational. The structure of the reference programme organisation has been deliberately kept 'flat.' Communication lines should be short. A relatively small number of committed individuals are preferred to a large group of people whose potential contributions are too dependent on other activities.

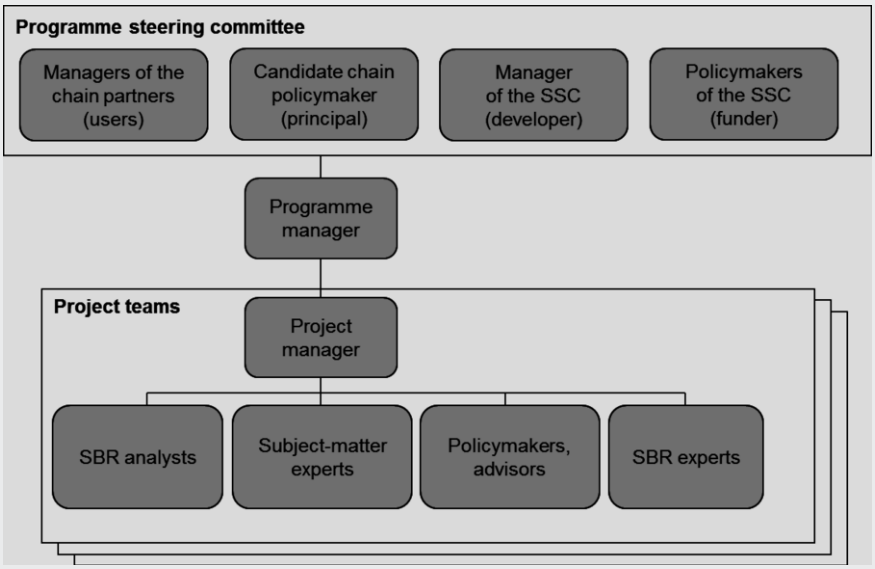


Figure 10.7 – Reference programme organisation

The lead policymaker in the candidate reporting chain acts as the principal of the reengineering programme. Representatives of the involved chain actors (including, at a minimum, reporting parties and any service providers) play the role of users. A SSC manager takes the developer's role. If applicable, representatives of the funder are included. It is the responsibility of the steering committee to manage the various projects in order to guarantee an integral (planned and controlled) approach. The representatives in the steering committee aim to meet the goals of the programme. The steering committee's role comprises steering the design; testing, acceptance and commissioning of the technology; and the realisation of the chain governance. The primary tasks of the steering committee include periodic assessment of the progress (budget and timelines) of the overall chain reengineering programme and ensuring that the business case remains viable. The key authorisations of the steering committee are the go/no-go decisions regarding continuing to the following phase, accepting proposed adjustments or discontinuing projects early. The steering committee's decisions should be reflected in the programme plan.

Since the later phases will require time and resources from all the chain actors involved, the steering committee can choose to sign programme-specific agreements with specific actors. The project teams include representatives from various organisations and backgrounds, resulting in multi-disciplinary project teams. Typical roles within the project teams are shown in Table 10.9. A role consists of a coherent set of tasks, responsibilities and authorisations that can be assigned to one or more persons.

Table 10.9 also shows which actors may provide persons to fulfil a specific role. It should be noted, however, that the list of roles is not exhaustive.

Table 10.9 – Summary of roles in the project teams

Role	Description	Can be fulfilled by:
Project manager	The project manager is responsible for the day-to-day leadership of the projects assigned to him. The project manager is the 'working foreman,' i.e. he has work tasks as well as management tasks. Next to the programme manager, the project manager plays a pioneering role in understanding and resolving complex questions that can arise throughout the course of the programme.	SSC
SBR Analysts	The analysts in fields such as data, process, technology and chain governance are responsible for the analysis and redesign of the as-is and to-be SBR chain.	SSC
Subject-matter experts	Subject-matter experts provide input throughout the analysis and design of the reporting chain. In the later phases, they act as a sounding board for the on-going checks on the results achieved. It is also possible to obtain the involvement of 'outsiders' (e.g., notorious critics).	Private, semi-public and public actors, 'outsiders'
Policymakers, advisors	The policymakers and policy advisors are responsible for the fit between policymaking and SBR, both in shaping the chain reengineering programme to fit the policy context and adjusting the policy context to fit SBR.	Public actors
SBR experts	The SSC provides SBR experts to supervise and contribute in terms of content throughout the implementation programme (separate from the analysts mentioned above). For instance, legal specialists, accountants and market experts.	SSC

The deliverables of the preparation for Phase 2 are listed in Table 10.10 below.

Table 10.10 – Overview of the Phase 2 preparation deliverables

Programme plan	A document providing a description of: 1) background, programme goals, scope, assumptions 2) estimated costs, project times and matrix of dependencies between the projects 3) overall timelines and integral deadlines for the deliverables 4) representation and explanation of the roadmap 5) quality management and risk management
Action plan for the detailed analysis and redesign phase (per project)	A document providing a description of: 1) background, project goals, deliverables, scope, and assumptions 2) outline of the approach, phases, decision-making, activities, services to be used, project planning, and project organisation 3) quality management and risk management
Start-up memo	A start up memo backed by the Quick Scan participants comprising two A4 pages that include, at a minimum, a clear description of the following elements: 1) the public function of business reporting 2) the results of the substantive analysis of business reporting in the candidate reporting chain 3) a sketch of the SBR chain 4) the need for change 5) the proposed strategy in terms of possible points of action and a roadmap

In the preparations for Phase 2, the involved chain actors make sure the required capacity is available, in accordance with the action plan and the programme plan.

10.4.4 *Services provided by the SSC*

In principle, the proposed methodology assumes that the SSC will supervise the chain actors when conducting the Quick Scan. However, other chain actors can also take the lead and specify which input/support they would like from the SSC. Of course, in the latter situation, lead actors should be confident that they can meet the requirements imposed by Checkpoint A for starting the subsequent phase. In this case, the SSC acts as 'intake agent' of the separate components of the preparation conducted by the candidate reporting chain actors.

10.4.5 *Cost types*

The investment of chain actors involves making time available for the exploratory meetings and conducting the Quick Scan. The SSC (or the party that takes the lead in the Quick Scan) should have the resources available to organise meetings and to realise the deliverables of this phase.

10.4.6 *Do's and don'ts in the exploration phase*

Experience with SBR has provided some do's and don'ts for the exploration phase:

- Decision making regarding the reengineering of reporting chains is strategic in nature. It is therefore desirable to get high-level and authorised officials involved in the exploratory meetings as early as possible.
- Communication should be modified depending on the chain party and should answer the following question for each type of chain party: "What's in it for me?" Benefits and costs should be made explicit, especially at the beginning of the project, in order to gain the involvement of all parties in the process. During the course of the project, 'the bigger picture' of SBR can be increasingly communicated.
- The legal framework around the reporting chain can present a barrier to the implementation of SBR (and its business case). Many chains find it attractive to switch to SBR fully over the long term, but would prefer a legal basis for this in order to justify the investment. Sufficient attention should be paid to this issue.
- Especially when parties are confronted with a large number of reporting chains (>10) within a reporting field, it is recommended to first construct an overview of all information chains ("telescoping"). Subsequently, the Quick Scan can be performed for a selected number of reporting chains, based on a set of criteria ("microscoping").
- Reporting chains generally consist of large numbers of actors—mostly organisations that are required by law to report—and there may be overlap in the reported information across chains. SBR can reveal interesting overlaps of reported information between two or more reporting chains. That is why it may be fruitful to talk to requesting agencies in other

chains during the exploration phase. The SBR forums can be used for cross-chain discussions.

- The SSC may be performing several Quick Scans at any given point in time. It is therefore important to find synergy when executing the different scans, particularly when similar chain parties are involved or similar challenges exist.
- Most of the questions from the Quick Scan can be answered through desk study and a small number of workshops with the persons involved. Experience teaches us that subject-matter experts with different backgrounds (e.g., legal, business studies, technical, etc.) can complement each other's views when addressing the questions. To obtain a rich picture, experts from various disciplines that are able to assimilate various results should therefore be consulted.
- The number of participants in the Quick Scan depends on the extent to which information about the reporting chain is already available and the considerations of the project board regarding the need to involve specific chain actors. The number will vary among Quick Scans in different fields of reporting.
- For participants that first encountering SBR, gaining a proper understanding of SBR may prove challenging. Therefore, SSC representatives should allow sufficient time to answer questions and provide resources in order to share knowledge.
- During the exploration phase, representatives of the SSC should deepen their knowledge about previous IT implementations and the corresponding lessons learned for the reporting field in question.
- The representatives of the project board or the participants could insist on not analysing the as-is situation. Perhaps they are motivated to start directly with the redesign phase for SBR. However, from the perspective of the SSC, it is highly desirable to analyse the as-is in sufficient detail. This is needed in order to 1) make tacit knowledge of different chain parties explicit and to ensure that all participants have the same point of reference; 2) guarantee that all relevant information for the redesign phase is available in a standard format; and 3) establish the change desire, change undertaking and change strategy in order to minimise potential risks when implementing SBR.
- Use quality management. Here, the term 'quality' should be taken to mean fitness for use, or able to meet the agreements, demands and expectations of the actors involved. Suitability for the purposes of the chain is the essential criterion for acceptance of the results.

10.5 The detailed analysis and redesign phase

The second phase of the methodology is the detailed analysis and redesign phase. Here, the term 'redesign' is used because there is usually a pre-existing reporting chain and the SBR building blocks are already available. The chain actors have already gone through the exploration phase. The analysis and redesign phase can commence once the following criteria are met (as part of Checkpoint A):

- The body responsible for policy, or the requesting party, has given instructions for the detailed analysis and redesign to be carried out for one or more reporting chains.
- There is a business case showing a clear intention to go through the change process being embarked upon, in which clear goals have been set that are achievable within the foreseeable timeframe.
- There is a recommendation from the SSC in favour of carrying out the detailed analysis and redesign.
- The public function, the current situation (Situation A) and the need for change have all been explored and this is reflected in a document that is supported by the actors involved.
- There is an overview of the desired chain (Situation B), the change undertaking and the change strategy. This overview is reflected in a document that is supported by the actors concerned.
- The programme organisation and the associated forums have been set up.
- The action plan for the detailed analysis and redesign phase has been drawn up and the steering committee has deemed it sufficient.
- The chain actors can make the resources available.

The detailed analysis and redesign phase should have achieved the following end points:

- The public function, Situation A and the need for change have been plotted out in detail and this has been agreed upon by the actors concerned.
- The desired chain (Situation B) has been designed in detail by the actors.
- The market lobby plan has been drawn up.
- The steering committee has a detailed justification of the costs and benefits of applying SBR in the reporting chain.
- The steering committee has been advised as to whether or not the experiment should be carried out.
- The experiment has been prepared.

The detailed analysis and redesign phase consists of five sets of activities. An overview of the activities is presented in figure 10.8.

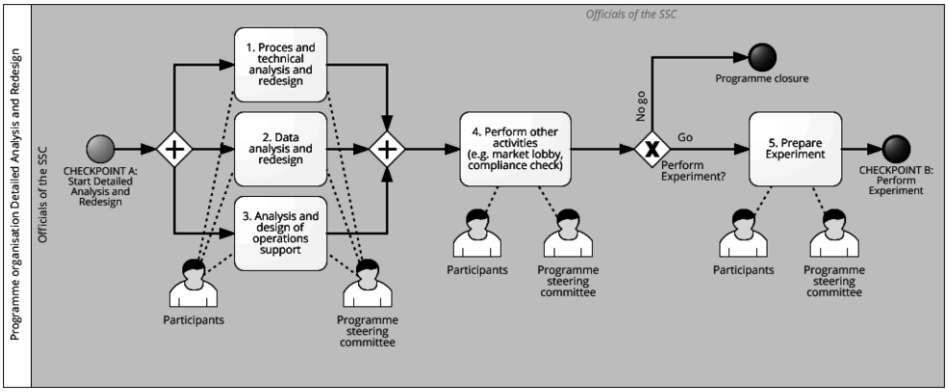


Figure 10.8 – Activity sets and the decision point in the detailed analysis and redesign phase

The first three sets of activities are the detailed analysis and redesign of 1) processes and technology, 2) data and 3) operations support performed by three corresponding project teams. Each project team also investigates necessary changes to the chain governance resulting from the redesign. The teams operate in parallel, with the project managers keeping a close eye on the cohesion between all aspects during the redesign. The programme leader also has an important task to ensure cohesion between all aspects of the redesign. Once the project teams have completed the redesign, several other activities are performed by the officials of the SSC, such as preparing the market lobby and the compliance check. The fifth set of activities involves preparation for the experiment. The following subsections elaborate on the illustrated sets of activities.

10.5.1 *Process and technical analysis and redesign*

The first set of activities is focused on the processes and technology of the candidate reporting chain. Here, experts on the project team conduct a detailed examination of the current business reporting processes and design their future equivalents. The process experts come from both the reporting chain and SBR. They use the process descriptions in BPMN to produce a picture of the current business reporting processes from registration of data elements through to processing and return flows. The analysis is thorough. Because the information exchange processes vary by chain and type of actor, the process experts usually work with archetypes. Each archetype focuses on a specific type of business reporting configuration found in practice. For instance, consider a small neighbourhood hair salon that employs an intermediary for its business reporting obligations vs. the multinational with its own business reporting staff and systems that can be used for S2S information exchange.

By modelling Situation A, potential points for improvement generally appear. The actors start on a redesign project based on Situation A and the building

blocks. Generic services and the I-processes (including corresponding process descriptions) are already available from previous implementations of SBR. In addition, those involved are able to call on the methods, the toolbox and the knowledge already available at the SSC. The SSC process expert analyses the design's impact on the SSC's services and keeps the impact to a minimum (see Section 10.2.3). The design yields a complete description of the I-processes in BPMN that could be implemented, including narrative explanation. The scope of the design extends from the IT systems of the reporting parties to the back office of the requesting party.

Table 10.11 – Overview of the deliverables from the process analysis and design

Process analysis	A description of the current business reporting processes in BPMN, with attention paid to unusual elements. The 'happy flow,' as well as deviations in the process and the corresponding causes, is determined.
Design memos	An overview of the choices to be made during the process design and their corresponding pros and cons, as well as the final design choices.
Process design	A complete description in BPMN of the I-processes that could be implemented and narrative explanation. The design is in line with the agreed-upon frameworks and there is alignment with the data standards and technology services. The scope of the design extends from the IT systems of the reporting parties to the back office of the requesting party.
Impact analysis (Part I: I-processes and technology)	The impact of the transition from A to B for I-processes and technology. The impact is both technological and organisational in nature and involves human resources and out-of-pocket costs. Emphasis is placed on tailor-made solutions within the design (for example, the specific use of an authorisation mechanism).
Compliance file (Part I: I-processes and technology)	Explanation of which design standards and legislation are adhered to and how in the I-process and technology design, in order to allow for the compliance check.

For the technical analysis and design, technical experts examine the consequences of the processes in Situation B on the technical infrastructures. The experts draw up the technical specifications for the new services. They use the analysis and the redesign to determine the impact of the technical implementation of SBR for the various actors.

Table 10.12 – Overview of the deliverables for the technical analysis and design

Business and technology files	A description of functional and technical specifications for the utilisation of generic services and the generic infrastructure. Emphasis is placed on tailor-made solutions within the design (for example, the specific use of an authorisation mechanism).

Lastly, experts on the project team analyse the current chain governance and design its future governance with respect to relevant aspects of the I-processes and technology. At the start, they examine which chain actors are controlling the current aspects of the I-processes and technology (both formally and informally) and whether they are able to govern these aspects satisfactorily under the existing agreements. The experts then examine the dependencies that arise (or change) as a result of horizontal integration, vertical integration and network integration. For the horizontal integration, the chain actors use the pre-existing governance of the chain as far as possible. If governance is present and functioning as it should, it can, in principle, be taken across virtually as-is. Naturally, any new actors joining the chain (which will at the very least include the SSC) should be given a position in the chain governance. If there is no current chain governance (e.g., because the reporting chain is not yet integrated) or the governance is not functioning satisfactorily, the experts then jointly produce a redesign. If actors who are currently not involved in governing the chain reengineering programme have been included in the Situation B chain governance, it follows from Chapter 4 that it is advisable to involve these actors in the change as quickly as possible.

Indicators of a non-functioning governance:

- No available resources for the implementation of changes that are agreed upon
- No process control over changes that are agreed upon
- Uncertainty regarding the development direction for objects in the reporting chain
- Parties that want to be involved are not involved and/or parties that are involved show little interest in being involved
- Parties have disproportionate influence compared to their financial contributions

Additionally, because of vertical integration and network integration, dependencies arise with the other requesting actors. In Section 10.2.3, we elaborated on this matter and argued that the impact on generic services and infrastructure should be minimised. During the redesign, SBR experts will pay close attention to upholding this principle. Therefore, during the reporting chain reengineering, a *laissez-faire* attitude can be adopted toward the chain governance with regard to vertical integration and network integration.

Table 10.13 – Overview of the deliverables for the chain governance analysis and design

Change proposal for chain governance (Part I: I-processes and technology)	A change proposal for the SBR chain governance, dealing with formal accession of the chain actors' representatives to the SBR forums. The change proposal is based on the analysis of current chain governance with respect to aspects of I-processes and technology and on the analysis of the future chain governance with respect to the I-processes and technology along the horizontal, vertical and network integration aspects

10.5.2 *Data analysis and data design*

In the second set of activities, the data experts conduct a detailed examination of the current requested dataset (elements and their definitions) and the data sources. The detailed analysis can trigger policymakers to take a close, critical

look at the datasets being requested through an information requirements analysis. Note that while the information requirements analysis is beyond the scope of the methodology, it can be fruitful when parties are going through both procedures at once.

In the detailed examination, the data experts investigate the relationships between the various data elements. They also look to see what similar or identical data has already been included in the Netherlands Taxonomy and its Extensions. They then use their analysis as the basis for determining what elements need to be added to the Netherlands Taxonomy as an extension taxonomy and what the reports should look like (see Chapter 6). The actors involved can use the methods and tools that are already available in SBR for the analysis and redesign. The SSC data expert analyses the impact of the design on the services offered by the SSC.

Table 10.14 – Overview of the deliverables from the data analysis and data design

Current data model	A representation of the requested elements, the associated definitions and the relationships between the elements.
Design memos	An overview of choices to be made during the data design and their corresponding pros and cons, as well as the final design decisions.
Extension taxonomy and reports	The design of an extension taxonomy in XBRL containing all the requested elements and associated definitions. The design of the reports for the reporting parties and requesters, containing the relevant links to the Netherlands Taxonomy and associated extensions.
Impact analysis (Part II: data)	The impact of the transition from A to B on the data, such as the impact on the Netherlands Taxonomy Architecture and the organisational impact in terms of time, human resources, and out-of-pocket costs.
Compliance file (Part II: data)	A file explaining which design standards (such as the Netherlands Taxonomy Architecture) are adhered to and how in the data design, in order to allow for the compliance check.

Concerning the chain governance, experts in the project team analyse the current chain governance and design its future governance with respect to the relevant aspects of data. Their approach is similar to the approach described for the processes and technology experts (see Section 10.5.2).

Table 10.15 – Overview of the deliverables for the chain governance analysis and design

Change proposal chain governance (Part II: data)	A change proposal for the SBR chain governance, for formal accession of the chain actors' representatives to the SBR forums. The change proposal is based on the analysis of current chain governance with respect to aspects of data (including cost-effectiveness) and the analysis of the future chain governance with respect to data along the horizontal, vertical and network integration aspects.

10.5.3 *Analysis and design of operations support*

In an operational SBR chain, the actors should be up to date concerning the specifications of the chain. In addition, they should know where incidents can be reported and should be kept aware of possible disruptions (for example, due to

maintenance). Operations support provides services in order to arrange these matters. The SSC plays a central role in operations support, especially for the support that applies to SBR directly. However, the requesting party has overall responsibility for the support of the entire reporting chain. Thus, the SSC's role depends on what position the requesting party wants to adopt in terms of operations support. In the activities in this part of the phase, the existing operations support and the SSC services available in that area are used by the chain partners to redesign the operations support. The SSC is keen on differentiating between different type of users, for example, based on the size of the intermediary and the number of businesses it works for, in order to be able to prioritise incident handling.

Table 10.16 – Overview of the deliverables for the operations support analysis and design

Operations support analysis and design	An analysis of Situation A's operations support as well as the design of the operations support for the business reporting in Situation B, describing which type of users can solve problems during the operations. Special attention is paid to differentiating between different types of users.
Design memos	An overview of the choices to be made during the operations support design and their corresponding pros and cons, as well as the final design decisions.
Impact analysis (Part III: operations support)	The impact of the transition from A to B for operations support. Emphasis is placed on the impact to the organisation and human resources.

Concerning the chain governance, experts in the project team analyse the current chain governance and design its future governance with respect to relevant aspects of operations support. Their approach is similar to the approach described for the processes and technology experts (see Section 10.5.2).

Table 10.17 – Overview of the deliverables for the chain governance analysis and design

Change proposal chain governance (part III: operations support)	A change proposal for the SBR chain governance, for formal accession of the chain actors' representatives to the SBR forums. The change proposal is based on the analysis of current chain governance with respect to aspects of operations support and the analysis of the future chain governance with respect to I-processes and technology along the horizontal, vertical and network integration aspects

10.5.4 *Other activities*

Once the project teams have completed the redesign, several other activities are performed by SSC officials. These include activities such as preparing the market lobby, the compliance check and updating the business case.

10.5.4.1 Preparing the market lobby

Once a detailed design is available, the market analyst is able to obtain a picture of the consequences of applying SBR for the various chain partners. At this point, the steering committee will have to make clear who the intended SBR users are. This might include specifying the numbers (e.g., 80% of reporting parties will be

submitting via SBR by 2016) and a target group (e.g., SBR is targeting the larger reporting parties). Preparing the market lobby includes a determination of what support will be available to users as they apply the reporting chain. This is always done in close consultation with the principal and the public bodies participating in the reporting chain. The SSC offers a large number of services that focus on helping market actors to connect to SBR. These include the following:

- Connection suite (test decks)
- Connection packages
- Group information sessions
- Individual support

Table 10.18 – Overview of the market lobby deliverables

Market lobby plan	A document containing a description of the intended users and the corresponding transition support, based on connection packages, individual support and/or group information sessions.

10.5.4.2 Compliance check

The redesign of the reporting chain consists of an integrated whole that includes processes, data, technology and chain governance, as well as the corresponding support during the transition and operations. The processes, data and technical aspects are designed together. The compliance check is the final check of the integral design against the applicable legislation and regulations. A test is also performed to check whether the individual design aspects comply with all the requirements and standards imposed (e.g. the principles of the Netherlands Taxonomy Architecture, process standards and technical standard, plus any additional contexts and requirements from the SSC). Special attention is paid to information security (see also Chapter 8).

Table 10.19 – Overview of the deliverables from the chain governance analysis and design

Compliance files I, II, III and compliance check	The combined compliance files (Parts I, II and III) as well as a structured assessment of the integral chain design against applicable legislation and regulations, including any recommendations.

10.5.4.3 Drawing up the recommendations and the business case

To assist in decision making, the detailed analysis of the current situation and the design are used to further specify the business case and draw up the associated recommendations. The steering committee receives the recommendations and the underlying business case to help in its decision making.

Table 10.20 – Overview of the decision support deliverables

Recommendations and roadmap	A recommendation of whether or not to implement SBR in the candidate reporting chain within the next 1-3 years. This recommendation should reflect the previously stated goals for the implementation of SBR, the anticipated benefits and the necessary investments from the various actors. In addition, a roadmap should be provided that contains clear directions for proceeding with the implementation and realising the benefits.
Business case	A quantified estimate (as good as possible) of: 1) the current costs – administrative and operational costs 2) the future costs – administrative and operational costs (and benefits, including opportunities) of the SBR-chain 3) investment costs and investment risks 4) alternatives

10.5.5 *Decision making*

The decision-making point at the end of the detailed analysis and redesign phase (as part of Checkpoint B) is the most crucial one in the chain reengineering programme. At this point, an overall, feasible design will have been produced that meets the guidelines and requirements imposed. The chain actors are therefore ready to test the design. Recommendations have been given to the steering committee. That advice is supported by the detailed analysis and the business case. This means that the information required for proper decision making has been gathered. Making the vision of SBR known within the reporting chain is now of crucial importance.

The activities that have taken place mean that market actors will now be keeping a close eye on the policy lines chosen. Carrying out the experiment will ramp up the market actors' expectations. The actors who will be using SBR will demand increased clarity regarding future policy so that they can justify the investment. In order to manage expectations properly, the principle when the experiment commences should be the following: *if there are no significant issues with the experiment, the application of SBR within the reporting chain shall be continued in the years that follow, with the aim of fully implementing SBR according to the goals set for the chains*. This effectively means that there needs to be sufficient backing among the key chain actors for the application of SBR within the reporting chain. The key chain actors include, at a minimum, the managers for the requesting actors, plus a number of leading reporting parties and service providers. If there is sufficient backing, the actors selected for the experiment will put SBR to actual use. Note that this makes the experiment fundamentally different from a pilot: a pilot might serve as a way to increase acceptance, whereas for the experiment, acceptance is considered to be the starting point. Please refer to Chapters 3 and 4 for a more detailed treatment of the theme of 'acceptance' and the way in which acceptance can be influenced.

10.5.6 *Preparing for the experiment*

At the end of the detailed analysis and redesign phase, the preparations for the experiment are begun. These activities comprise drawing up the action plan, set-

ting up the experimental environment and making capacity and resources available. In the preparations for the experiment phase, it is important that the chain actors involved are able to free up the capacity and resources required. This means that the action plan should give a precise picture of the activities needed and how they should be planned (including the capacity required for the IT environment and its facilities) in order to achieve the desired results. To clarify where funding will come from, a budget should be drawn up for the experiment, with the costs broken down for the various actors.

Table 10.21 – Overview of the deliverables from the experiment preparations

Action plan for the experiment	A document giving a description of the following: 1) background, project goals, deliverables, scope, assumptions; 2) outline of the approach, phases, decision making, activities, project planning, services to be used, capacity planning for IT services and infrastructure, plus the associated service levels, and project organisation; 3) costs and financing; 4) quality management and risk management.

The SSC offers a service to carry out the experiment. To guarantee the availability of the IT services and infrastructure needed, the requisite preparatory steps must be taken before the experiment starts and the experimental environment must be set up. In the preparation for the experiment phase, the chain actors involved make the required capacity available according to the action plan. Substantial resources are needed to carry out the experiment, and these need to be reserved ahead of time.

10.5.7 *Services provided by the SSC*

Chapter 9 explained how the services of the SSC provide four basic functions, namely, I-process management, data management, transition support and operations support. For each basic function, there are services that deal with the design, the transition and the production situation. The services offered by the SSC during the detailed analysis and redesign phase deal with the design in particular. The SSC provides a single service that handles the coordination between the various services, from design to experiment to production. The SSC can also provide expertise for decision support, such as process supervision or guidance along the substantive guide on the strategic level.

10.5.8 *Cost types*

The detailed analysis and the redesign demand a substantial investment in time from the chain actors concerned. Out-of-pocket costs are very limited. The resources required for the analysis and redesign should be provided by the SSC or the parties taking the lead in elements of the analysis and design.

10.5.9 *Do's and don'ts in the detailed analysis and redesign phase*

Experience with SBR has provided some do's and don'ts for the detailed analysis and redesign phase, which can be taken in addition to most of the do's and don'ts for the exploration phase.

- Involve the policymaking ministries in drawing up the finalised goals for SBR and determine together whether modifications are needed in the legal frameworks that apply to business reporting.
- Make sure that SBR is not seen exclusively as a technical or an ICT project. The temptation to see SBR as an ICT project can be large for the chain actors, given that much of SBR demands a change in the technology. Experience teaches us, however, that projects viewed as solely technical often do not generate sufficient involvement at the higher levels. Such projects disappear quickly from the executive level radar, which primarily scans for solutions to business issues. Emphasise that SBR can potentially serve as a solution for business issues. Furthermore, keep a close eye on the organisational governance.
- Make sure that there is a clear and common view among the chain actors regarding the change objects for the transition (see Chapter 4). Once again, it should be emphasised that it is highly desirable to analyse the as-is situation in full detail.
- Organise the experiment as a cooperation between public and private actors. The Dutch way of implementing SBR is typified by the large say that market actors have in the process. From the very start, the SBR Programme has been a public-private cooperative programme aimed at encouraging acceptance and adoption of SBR by the market actors.
- Design operations support not only 'on paper' but also ensuring that the design includes proper handling of exceptions that can occur in practice.
- Ensure that all the relevant chain actors are involved in the design and governance (see Chapter 4).
- The analysis and redesign includes the I-processes, data, technology and operations support, all having relevant aspects of chain governance to be taken into account. The design should comply with the legislation, standards and agreements. In addition, it needs to be determined what transition support is required. Since the design consists of many aspects, the SSC offers multiple services. Therefore, it is appropriate to make use of a programme rather than a project.
- The project teams should be authorised to make decisions. The project organisation structure is flat, so the project team members assume a great deal of responsibility. The authorisations should go hand in hand with these responsibilities.
- Use the roadmap as a 'pressure release valve.' Do not make any concessions in terms of the final picture, but aim to control the speed of the transition. Hard deadlines can encourage the actors to take the project seriously. Shifts in the timelines can also reduce resistance.
- The scope, functionality and quality should be actively managed using time-boxing. This concept comes from the literature regarding 'agile development' and ensures closure (Richards, 2007). Time-boxing attempts to find a balance between delivering products or partial products on time and being able to implement requirements or preconditions that fall into the category of 'new insights.' Time-boxing divides the entire project pe-

riod into a number of shorter periods known as the 'time boxes' or 'iterations.' An evaluation is produced at the end of each time box to see whether the correct product is being produced in the correct way. This allows the project to be steered as necessary. Whatever the result, the development team should take a fresh look at the end of each iteration to see what the project's priorities are.

10.6 The experiment phase

The experiment is the third phase of the methodology. Chain actors have completed the detailed analysis and redesign phase. The experiment phase can commence once the following criteria are met (as part of Checkpoint B):

- A roadmap has been produced by the key chain actors with appropriate backing, for the implementation of SBR in the reporting chain within one to three years, in line with the stated goals.
- There is a positive recommendation from the SSC regarding the application of SBR within one to three years.
- The design of the SBR chain has been drawn up. It satisfies the requirements and the actors concerned believe that the design is such that there will be no major issues during the experiment.
- The action plan for the experiment has been drawn up.
- The experimental IT environment has been set up.
- The chain actors can make the needed capacity available, and there is funding for the experiment to be carried out.
- The ways in which the actors can participate usefully in the various governance forums is clear.

The experiment aims to achieve the following end points:

- The design has been tested technically and any last 'teething problems' have been resolved.
- The advice and the underlying business case have been updated.
- The plan for scaling up has been produced.

The experiment consists of three sets of activities. The first set comprises the technical test of the design, i.e. controlled implementation of the I-processes, data and technology for Situation B in a limited and safe experimental environment. The second set consists of updating the advice and the business case. The third set comprises the preparations for the following phase (scale-up).

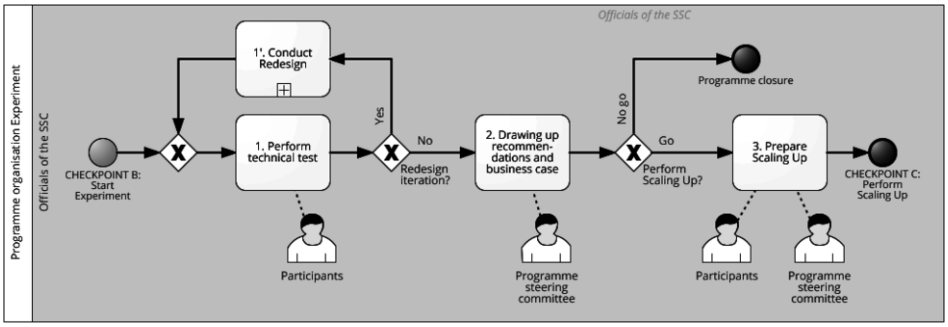


Figure 10.9 – Activity sets and the decision point for the experiment phase

10.6.1 *Technical test*

The technical test of the design takes place in the experimental IT environment provided by the SSC. The experimental IT environment is a flexible facility that assumes the same architecture as the platform used in the production situation for the I-processes and data. However, alternative configurations can also be tested in the experimental environment and workarounds can allow specific functionality or interactions to be simulated. This means that any remaining 'teething problems' in the new application of the building blocks can be resolved. The tests allow the experts at the SSC to determine whether the I-processes, the taxonomy, the IT services and the infrastructure meet the stated requirements. If they do, the technology will be accepted for production. It not, experts produce the final design by altering the initial design where needed. In the rare event that major changes are required, an iteration of the redesign phase takes place (denoted as activity 1' in figure 10.9). This activity can be seen as a 'light' version of the redesign conducted in Phase 2 (Detailed Analysis and Redesign), meaning that, in principle, similar activities are performed as described in Section 10.5, but at much faster pace and with fewer resources required.

Table 10.22 – Overview of the technical test deliverables

Final design	The final design of the I-processes, the extension taxonomy and the reports and operations support for the SBR chain in Situation B, including all technical specifications. Typically, the documentation of the final design includes relevant elements from the Quick Scan such as the public function of the business reporting chains and chain actors.
Functioning SBR chain	A functioning SBR chain in the experimental environment, in which companies and service providers make use of SBR to fulfil their reporting obligations.
Impact analysis (I, II, III)	The combined and updated impact analyses Parts I, II and III.

10.6.2 *Updating the recommendations and the business case*

To assist in decision making, the final design is used to update the business case and draw up the associated recommendations. The steering committee receives the recommendations and the underlying business case to help with its decision making.

Table 10.23 – Overview of the deliverables for the advice and business case

Recommendations and roadmap (updated)	An update to the recommendation of whether or not to apply SBR on a larger scale in the reporting chain within one to three years.
Business case (updated)	An update of the business case.

10.6.3 *Decision making*

If no significant issues arise during the experiment, it is expected that the steering committee will decide to continue with the application of SBR in the reporting chain. The steering committee determines what transition support will be offered and lays down the final change strategy. The steering committee members only face a genuine decision if substantial problems arise during the experiment—for example, if the technical test was not successful and the redesign iteration indicated there would be a major impact on the business case. The updated recommendations and roadmap will help the steering committee in such a decision. The advice will also take into account of any effects of the decision that could extend beyond the chain, as the decision to solve a technical problem in the reporting chain could also benefit other reporting chains.

10.6.4 *Preparations for the next phase*

During the experiment, the chain actors can finalise the design and the plan for scaling up is thereby determined. Note that the experiment will allow the chain actors to formulate answers to the questions from the substantive guide. They then determine the strategy for the next stage using the insights obtained (particularly with regard to the change undertaking). Crucial elements of the preparation will always include the following considerations:

- The reporting chain's transition into the production situation
- The implementation of operations support

The actors make the needed capacity and resources available, in accordance with the plan for scaling up.

Table 10.24 – Overview of the deliverables from the preparations for the scale-up phase

Action plan for scaling-up	A document providing a description of the following: 1) background, project goals, deliverables, scope, and assumptions; 2) detail of the change undertaking per actor and the associated change strategy (believed by the involved actors to be sufficient to achieve that change); 3) services to be used and the corresponding service levels; 4) costs and financing; and 5) quality management and risk management.

10.6.5 *Services provided by the SSC*

The SSC offers a number of services in the experiment phase of the methodology. These services deal with, in particular, the transition of the four basic functions from design to production. The SSC provides the experimental environment and the supervision to go with it.

10.6.6 *Cost types*

Depending on the initial positions of the chain partners, the experiment demands a substantial investment by those actors, in terms of both time and resources. The requesting party is the actor that is the consumer of the SSC's services.

10.6.7 *Do's and don'ts in the experiment phase*

For the experimental phase, the following do's and don'ts should be taken into account:

- Make sure that sufficient time is allotted for working with the experimental environment and that the planning has allowed time for some overrun. Testing the technology can take longer than actors tend to think (or want) beforehand (Brooks, 2006).
- Make sure that there is sufficient transition support to guide the actors. Since it is the first time SBR is being implemented in the reporting chain, guidance will likely come in handy.
- Plan the utilisation of the experimental environment together with the environment's manager (the SSC), taking into account the capacity required.

10.7 The scaling up phase

Scaling up is the fourth phase of the methodology. The chain actors have completed the experiment. Scaling up is possible if the following criteria have been met (as part of Checkpoint C):

- The technical test has produced a functioning SBR chain within the experimental environment.
- Representatives of the chain actors are formally taking part in the SBR governance structures and forums.
- The plan for scaling up has been produced and the programme steering committee has deemed it sufficient.
- The chain actors can make the needed capacity and resources available. The technology has been accepted for production by the SSC (after the design and transition).
- Operations support has been implemented.

The goals of this phase are the following:

- Connection of the community of users according to the target group to the implemented SBR building blocks.
- Completion of the programme.

There are two sets of activities in the scale-up phase. The first set includes the step-by-step connection of the target group users to the generic infrastructure. The SSC's transition support and operations support are essential for connecting the entire community of users. Once the intended users have been connected to the generic infrastructure and information exchange via SBR is possible, the SBR chain is in production. This is the trigger to begin closing the programme (the second set of activities).

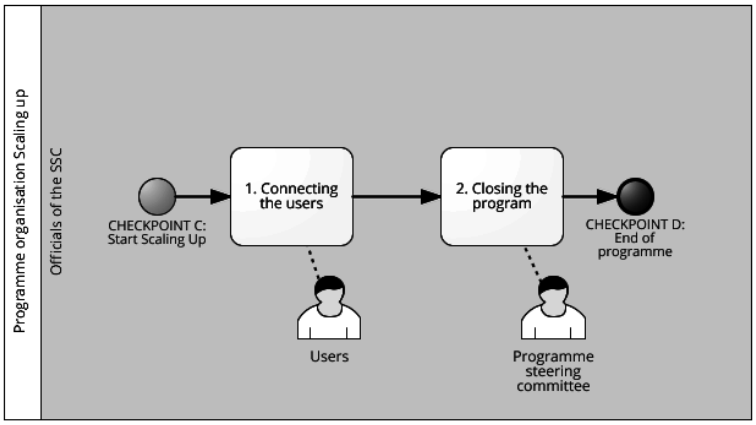


Figure 10.10 – Activity sets in the scaling up phase

10.7.1 *Connecting the users*

The purpose of scaling up is to connect, in a step-by-step manner, the users to SBR. At this point, all the actors involved in the reporting chain are ready to progress to the implementation of SBR. If the experiment yields a chain that is already functioning, this plays a key role in demonstrating that SBR can be applied. It is just as important for the SSC to provide support for the connections to SBR building blocks. Here, investments in the earlier phases of the methodology are starting to pay off: the chain actors have already started the preparations for scaling up by discussing the change undertaking and the change strategy during the exploration phase. The change strategy has also been closely watched throughout the detailed analysis and redesign phase. The experiment allowed the consequences of implementing SBR to be determined definitively and the change strategy was thereby determined. Therefore, all involved actors should have a solid understanding about the obstacles that might arise and how to tackle them. Typically, connecting the users to SBR in the last phase of the methodology implies that the legacy solution will now be discharged. The main obstacle to this process comes in the form of non-acceptance.

Scaling up is, in principle, done according to the scale-up action plan. The chain actors can only decide to adjust things if exceptions appear or unexpected events occur. A number of production services offered by the SSC are being used by this point in the process. The deliverables for the scaling-up phase consist of the outputs provided by the production services. Actors should consider making all relevant specifications available here (such as FAQs) as well as the production and monitoring reports. Depending on the type of connection support chosen, the SSC can also provide elements such as a connection suite or connection packages. Further descriptions of the deliverables used within the SSC for internal assignments are outside of scope of this chapter (see instead Chapter 9).

10.7.2 *Closing the programme*

During the course of the chain reengineering programme, the intended users are connected to SBR. The chain actors have successfully passed through the checkpoints along the way and have resolved any issues (which may have been complex). The SSC services that were initially offered by the temporary project teams (as part of the SBR implementation programme) now become the responsibility of the permanent SSC department that is offering the services. Because the programme has gradually progressed to become incorporated in the structures and services of the SSC, the temporary programme-oriented governance can be incorporated in the more permanent SBR chain governance.

The steering committee completes the programme, transfers the results and the lessons learned (e.g., solutions found for the technical roadblocks) to the SSC and finally dissolves the steering committee and the project teams. If all goes well, the actors concerned will be able to look back with satisfaction on the road they have travelled together and the results that it has yielded.

Table 10.25 – Overview of the programme closedown deliverables

Lessons learned	A description of the lessons learned during the course of the programme, adding best practices to the methodology itself.

10.7.3 *Services provided by the SSC*

A large number of services are used during scale-up. In addition to the services that may be used during the experiment, these include services relating to transition support (e.g., delivering a connection suite, training courses, support, and information, as necessary) and production services (e.g., the production I-processes, the taxonomy production, the associated management information systems, and front desk, back office and operations support).

10.7.4 *Cost types*

In the scale-up phase, the requesting party—as the client of the SSC—generally pays for the services required for the delivery of SBR, according to the agreements made. The extent to which the requesting party wants to support its chain partners in connecting to SBR partly determines the costs. The vertical chain partners will find it important that the chain ambitions are met. They will probably insist that the requesting party in the candidate reporting chain does not neglect this part. Depending on the extent to which the chain partners are already using SBR, scaling up will demand a greater or lesser amount of initial investment by reporting parties and software developers.

10.7.5 *Do's and don'ts during scaling-up*

Experience in SBR has provided some do's and don'ts for the scale-up phase:

- It is understandable that some actors may resist applying the new reporting chain during the scale-up. Chapters 3 and 4 have already discussed acceptance in some detail. It is important that there is always a clear picture of the change requirements for the actors concerned and to

use the support offered in order to lower the hurdles that must be cleared during SBR implementation.
- Scaling-up in phases—allowing different users to connect at different points in time—might be recommended in the light of capacity management for the SSC in the cases where a large number of potential users are expected to connect.

10.8 Chapter conclusion

Chapter 1 highlighted the benefits gained by widespread application of SBR in business reporting. As such, many reporting chains are potentially able to benefit from the implementation of SBR. At the same time, a number of challenges can arise when implementing SBR in a candidate reporting chain (see Chapters 1 through 4). The current chapter has presented a methodology by which to systematically approach the reengineering of reporting chains for SBR. Chain actors might find the methodology a valuable tool that brings awareness to the following aspects of such a course: the relationship between change desire, change undertaking and change strategy; the importance of managing the expectations of reporting parties and software providers; the expected acceptance hurdles and particular do's and don'ts. As such, it can serve as a useful guideline when attempting to realise the full potential of SBR in candidate reporting chains. We present this methodology with much confidence. Our confidence is rooted in the experiences that led to the development of the methodology. At the same time, we acknowledge that chain actors that make use of the methodology might have some concerns. On one hand, chain actors that are confronted with complex problems in their reporting chain during SBR implementation might feel that concrete instructions for specific, less promising situations are missing from the method. On the other hand, chain actors that experience a relatively simple implementation of SBR in their chain might feel that such an extensive methodology and corresponding lists of deliverables are rather exaggerated. As such, many features could have been incorporated into or left out of the methodology. More experience with the methodology's application within different settings should provide a better indication over time of which features are the most crucial for success, and which features might have less relevance.

Finally, even if the methodology becomes a best practice over time, we must be aware of the general limitations of any methodology. No methodology can be seen as a complete and failsafe recipe for success. As such, the methodology should be applied with a sense of professional judgement by those who are knowledgeable and who show a sense of ownership, creativity and, if required, stamina. Those who cannot shake the feeling of SBR implementation as an immense undertaking may find some comfort in the fact that the SSC in the Netherlands is currently well equipped and staffed to assist chain partners along the entire implementation pathway.

11 Final Conclusions

This book has described SBR both as a challenge and as a solution for information chains. In order to provide an in-depth account of the challenge, three chapters were devoted to various issues that surface when information chains are transformed (part A). The six chapters in part B provide a detailed description of the building blocks that constitute the SBR solution. The detailed description of components – whether it's about XBRL or a phased methodology for applying SBR in an information chain – strive to help the reader to comprehend what is needed for automated, system-to-system, information exchange and processing. Please note that a synthesis step is required to get a working solution: an operational SBR chain will only be created if the building blocks are put together in the right way. The applicability – both the pros and the cons – and capabilities of a working solution are however difficult to describe by looking at its constituent parts. A review of a vacuum cleaner for instance will generally not discuss the kind of plastic it is made of. Whether it uses 'wind tunnel technology' or not, is an internal aspect you probably do not want to know. The review will most likely look at how well the vacuum sucks up dust, for which target groups it is useful (hotels or at home), and so forth.

In this final chapter, we want to have a look at SBR as a solution from a similar angle. What is the strength of SBR as a solution for system-to-system business reporting? What barriers do we still see for that solution? What perspectives can

we look forward to, and what threats need to be recognised? This final review assumes a timeframe of about five years.

The strengths of the SBR solution

Considering the application of SBR in the fiscal domain, we can ascertain that SBR in its current state offers a working solution for business reporting. The information delivery chain for corporate income tax is up and running on a large scale. The fact is that the Dutch Tax and Customs Administration has received over 3 ½ million reports via SBR in 2013. Over 7 ½ million reports are expected for 2014. Consequently, this government agency has enough trust in SBR to start heading towards a future in which SBR is the only remaining system-to-system modality for fiscal business reporting. This level of trust is essential for SBR as a solution. In the first place, this is because the Dutch Tax and Customs Administration imposes high demands on a solution. If a solution is good enough for filing taxes, then you can safely assume that its foundation is sound. Secondly, because almost every organisation has to deal with the Tax and Customs Administration, many organisations are already using SBR components (e.g., digital certificates and software with the required interface specifications). This creates potential for other business reporting chains. At the data level, the same applies for the Chamber of Commerce's schedule for mandatory filing via SBR. Many of the requesting parties are interested in the financial statements that are relevant for their sector. The implementation of SBR in other reporting chains is also made considerably easier when it is mandatory for the financial statements domain. The expandability of the concept is one of SBR's key strengths. Basic functions are implemented in a standard way, allowing the business reporting chain to focus its attention on precisely those elements that are important for that particular chain. Information exchange is fully computerised in SBR using internationally accepted standards.

SBR is also interesting in the political arena. It can make business reporting to governmental agencies cheaper and more reliable. A government that chooses to set up information chains in a standard way ensures that both it and the reporting parties will reap the benefits, sooner or later. In areas where the business reporting chain still includes many manual operations (human data entry), or assumes that the information will be delivered in unstructured formats, SBR will also be able to improve business reporting. In such a case, the transition that will be required is substantial and should not be taken lightly by the actors in that chain. In the Netherlands, the Shared Service Centre (SSC) can support actors in candidate chains throughout the entire lifecycle of chain reengineering using a clearly outlined catalogue of services. The SSC can help with the initial analysis, design and connection and can arrange (further) scaling up when actors in the candidate chain are satisfied. Working with a SSC fosters specialisation and economies of scale, promotes reuse of components across information chains and public agencies and provides transparency in the cost of generic components for system-to-system information exchange and processing.

The completeness of the service catalogue and the idea of a 'one stop shop' can be a comforting idea for requesting parties, both public and private. In practice, there are however still a number of barriers regarding the widespread adoption of the SBR solution in other information chains.

Barriers to application

The adoption of SBR implies that a requesting party is giving up some autonomy, although primarily in aspects that from a transactions cost perspective ought to be outside its core business. We already discussed this in Chapter 1. However, there are still some obstinate misunderstandings regarding the SBR concept, producing significant barriers for broader adoption. These misunderstandings are partly kept alive by a general resistance to change, but also sometimes by utter clumsiness. Let us address some of the most common misconceptions:

- SBR is not only useful for processing financial data. All sorts of data can be exchanged and processed using SBR. In the food industry for example, actors use an XBRL taxonomy for microbiological criteria.
- 'Store once, report many' should be seen as setting up your data administration once and then filing based on it multiple times to multiple parties – not sending data in just the once, so that several requesting parties can use whatever they want. The SBR concept therefore does not involve some humungous database that companies with reporting obligations dump all their information into and that is then queried by various requesting parties.
- SBR is not only useful when multiple requesting parties want the same data or similar data. The reuse of concepts is not the biggest and certainly not the only benefit of SBR. There are numerous facets to the standardisation within SBR, such as using the same interface, digital certificate and a SSC. Furthermore, SBR can also generate gains due to the further automation (computerisation) of the information chain (both upstream and downstream).
- SBR does not only result in benefits for government agencies. The expectations of benefits for the private sector were perhaps set too high when SBR was first launched in the Netherlands and the actual benefits (see Chapter 1) are difficult to quantify. That does not mean they do not exist. It is easy to see that large-scale standardisation through widespread use of SBR means more efficient business reporting for "The Netherlands, Ltd."
- No, SBR does not contain roughly as many calories as a pack of butter![36]

[36] An illustration meant to explain that misunderstandings could be damaging and need to be taken seriously. A well-known ice cream manufacturer had a serious problem with an urban myth that an ice cream contained as many calories as a pack of butter. The facts: the ice cream of 80g had 283 kcal. What most people think of as a 'pack of butter' (half a pound or 250g) had 1838 kcal. The statement was incorrect, both at the unit level and per 100g.

Misunderstandings can be fuelled by a lack of knowledge. This may well be the biggest barrier that SBR has to overcome. The SBR community will have to keep investing in knowledge dissemination if it wants to eliminate these incorrect perceptions. To make a fair estimate of the pros and cons of employing SBR, the business reporting chain has to be considered as a system, as a coherent whole. This book shows just how many aspects there are to that. Business reporting chains are generally set up reactively, in other words built up layer by layer in response to issues and political agendas, rather than designed using an integrated architecture. Often, individuals in a chain are specialists in a specific aspect and weigh SBR from that perspective. A metaphor for this is the blind men trying to describe an elephant together.[37] Those at the executive level who are wondering whether SBR can be useful for them will consult other parties who are involved in the business reporting chain, and rightly so. Everyone concentrates on their own piece of the business reporting chain and then use that to form a judgement about SBR. A bit of bad luck can then mean that the overall solution and the added value as a whole are not part of the picture. When viewed as a whole, people will see the potential of SBR correctly, but they will also face a dilemma because SBR is based on an integral design. This generally implies a fundamental transition in which the issue that could be a bit painful for some chain parties is not the adoption of SBR, but letting go of the legacy of the previously used components for information exchange and processing. Despite the positive business case for applying SBR in the candidate chain, it can be difficult to generate internal support for the transformation. That support or commitment is often easier to obtain when chains are already facing a major transition. Consider this: the already planned renovation of your home may be the right moment to put in a modern heating system.

Future prospects

For SBR, the fact that many information chains in the Netherlands are currently being considered for renovation marks a promising era. The recent turmoil in the financial sector, but also in the public and non-profit arenas has strengthened the call for more (corporate) accountability and transparency. Schools, medical institutions and housing corporations all have to account for substantial sums of public funds by reporting to the government. Nevertheless, the authorities were unable to exercise sufficient control over these sectors. Systematic redesigns of the reporting chains in these sectors are being considered and SBR can contribute. Managing public funds is one of the focal points in policy-making, and it begins with getting an accurate account of the expenditures. In the Netherlands, the transfer of some public functions from the federal to the municipal government will further complicate the numerous business reporting chains. That transition will undoubtedly present opportunities for SBR.

---

[37] Each blind man takes a piece of the elephant and tries to describe the whole thing, based on that piece. The blind man with the trunk thinks it is a snake. The others think it is a rope (the tail), or a tree trunk (a leg), a wall (the flank) or a fan (the ear).

The financial supervision domain is also in a state of flux. Since XBRL is rapidly becoming the international standard for digital business reporting, this will certainly boost interest in the SBR approach. It is imperative that actors steer towards the complementary rather than concurrent application of XBRL. Robust agreements, tight steering and central coordination are needed to ensure alignment with the international developments: one of the challenges that SBR is now facing.

Challenges

Widespread application of SBR will go hand in hand with new governance issues. As we have discussed in Chapter 4, setting up the chain governance in some cases can be more challenging than setting up the technology. Implementing an encompassing electronic identity management (e-ID) system within the SBR domain is one concrete challenge that is already at the doorstep. The way SBR is positioned within e-Government will ultimately determine the business case for SBR within the public domain. We have already seen that legislative amendments are sometimes needed in order to force reporting chains to be more efficient. The legislators have to make the next move. Developments may be rapid if there is political support for a government that wants highly automated business reporting chains and sees SBR as the solution.

There are risks of SBR misfiring as well, if no such decision is made and no clear integrated vision of business reporting appears. Business reporting chains will then continue to rely upon different modalities for the same types of business reports and neither SBR nor any alternatives to it will in that case yield the benefits that are potentially there. This will also happen if the parties start 'cherry picking', or just use particular parts of the SBR solution. Standardising just a little bit is like being just a little bit pregnant...

Conclusion

It seems that SBR has proved its worth as a useful solution, particularly in the fiscal domain and for the dissemination of annual financial statements. This strengthens our opinion that SBR is a valuable development. Whether our opinion is objective enough remains to be seen. The authors and editors have done everything they could to provide a fair and encompassing picture SBR, so that readers will be able to judge its value for themselves. No matter how the SBR story unfolds, its scope is now substantial and business reporting domains are still very much subject to change. It is therefore going to be extremely interesting, from a range of viewpoints, to see how this case progresses. The key question that remains is what the title will be for the next version of a book about SBR: SBR, from challenge to solution to.....?

Appendices

Appendix A – A brief history of SBR in the Netherlands

The players and the playing field

The purpose of this section is to provide some background information on the various developments that have led to the inception of SBR in the Netherlands. We start by briefly describing the players and the playing field. Obviously, the main players are the businesses – with reporting obligations – and the parties that request information. A business can refer to a range of organisations that are required to disclose information, ranging from an entrepreneur to a multinational enterprise. The group of requesting agencies consist of both public and private organisations. Two often-neglected groups of players in this context are the intermediaries and the software providers. The intermediaries are the accountants, bookkeepers, financial advisers, tax consultants and fiscal advisers that are hired by businesses. Generally, intermediaries submit business reports to public and private organisations (e.g., banks) and on behalf of a business. Please note that even when the tasks of preparing and disclosing business reports is outsourced to intermediaries, from a legal perspective, the head of the reporting organisation is always responsible for the contents of the disclosed report. While SBR is also applicable for government-to-government and business-to-business reporting, this book mainly focusses on business-to-government reporting.

The software developers provide the administrative software packages for businesses. Businesses and intermediaries use such packages for keeping track of their business administration or bookkeeping, often with different packages or separate functionalities for fiscal matters (compiling declarations) and for generating annual reports.

Having considered the players, let us proceed with an examination of the playing field. The tax domain includes multiple reporting chains that have adopted SBR. Various (national) tax laws compel companies to pay their taxes. This involves filing to the Tax and Customs Administration. This practice might be repeated several times per year. The frequency and timeframe for which a business should disclose information depends on the type of tax declaration. For instance, a business has to submit a (corporate) income tax declaration annually. Many businesses submit a VAT declaration quarterly, but this may also be monthly or yearly, depending on the turnover for that period. The intra-community goods and services declaration (ICP, formerly ICL) is also disclosed monthly, quarterly

or annually. In the Netherlands, companies are obligated to submit these declarations and statements electronically since 1 January 2005.[38]

Businesses may submit these declarations themselves, but the majority of (smaller) businesses use an intermediary. The bookkeeping is one of the areas where businesses have already been using computers for a considerable time (Jans, 1991). Many intermediaries use accounting software from which they can generate the income tax and VAT declarations, plus specific software for drawing up the corporate income tax declarations. The declaration can then be submitted via a system-to-system linkage using this software. This means that the software and receiving systems communicate using an interface, in principle without human interaction. An alternative is to file the report using a digital form on the website of the Tax and Customs Administration. This is mostly done by a small group of businesses who send in their own declarations. The Tax and Customs Administration receives millions of electronic declarations from businesses every year.

In addition to tax declarations, businesses have to disclose their annual report as well. Businesses that are established in the Netherlands are legally obligated to draw up a financial statement each year and submit it to the Chamber of Commerce. Failure to comply with this obligation can result in a (criminal) penalty and directors' liability.[39] The annual financial statement provides an overview of the financial situation of a business. The financial statement consists of a balance sheet, the profit and loss account and the notes to the financial statement.[40] Medium-sized and large companies are obligated to publish an auditor's report along with the financial statement.[41] Smaller companies only have to submit (simplified) financial statements. Since 2005, developments in Europe have allowed businesses – and the intermediaries on their behalf – to submit their financial statement electronically, for example in PDF format.[42] The intermediary can use a 'report generator' to generate the financial statement from the accounting system. However, it is still possible to submit the report in paper.

A third form of business reporting is requested by Statistics Netherlands. Statistics Netherlands is responsible for collecting and processing data in order to publish statistics to be used in practice, by policymakers and for scientific research. In addition to its responsibility for (official) national statistics, Statistics Netherlands also has the task of producing European (community) statistics. In order to fulfil their tasks, Statistics Netherlands submits various requests at

[38]Article 8 Awr, as amended by the 'Belastingplan 2004, Staatsblad 526', dated 29 December 2003.
[39] Articles 2:394 and 2:248 BW; Articles 1 to 4 of the 'Wet economische delicten'.
[40] Article 2:361 BW and Directive 78/660/EEC, Article 2 paragraph 1.
[41] Article 2:392 BW and Directive 78/660/EEC, Article 47.
[42] Article 3 paragraph 2 of Directive 68/151/EEC; Article 3 paragraph 3 Handelsregisterbesluit. Introduced with the 'Besluit tot wijziging Handelsregisterbesluit 1996' and 'Besluit modellen jaarrekening of 22 December 2005', Stb. 2005, 729.

various moments to random samples of businesses. For instance, every month Statistics Netherlands selects random businesses to provide short-term statistics and annual investment and production statistics. The selected businesses receive a letter from Statistics Netherlands. Businesses that do not respond within the given period risk a fine.[43] Businesses are allowed to submit the requested information in written or electronic form. However, Statistics Netherlands only supplies paper questionnaires on demand, encouraging electronic disclosure using the login information provided in the letter. Besides these questionnaires, Statistics Netherlands also retrieves data from other institutions such as the Tax and Customs Administration.

One of the factors that define the domain of business-to-government reporting is government policy. Since the nineties, the Dutch government pays increasing attention to reduction of the administrative burden for businesses and encourages public agencies to embrace the possibilities of using ICT. The Ministry of Economic Affairs (EZ) is responsible for the business domain and is looking for ICT solutions to reduce the administrative burden. In 2002, EZ started a cooperative venture with the commercial sector resulting in the programme 'ICT and Administratieve Lastenverlichting' (ICTAL). Its instructions were to use ICT solutions to reduce the administrative red tape for the commercial sector.[44]

A range of different solutions was launched within ICTAL, with varying success. One example of a concept that did not work was the IDEA concept (Interchange of Data between Enterprises and Administrations). IDEA was an experiment that aimed to find out whether it was possible for the government to retrieve a standardised set of business data directly from the companies' administrative systems. It turned out this was not the right way to reorganise the chain. It was technically possible, but there were legal barriers: according to the State Secretary for Economic Affairs, it could have resulted in an "*undesirable and unnecessary shift of responsibilities between the administrative authorities and the commercial sector*".[45]

One of the more successful solutions developed within ICTAL was the 'Overheidstransactiepoort' or OTP (2004), a single address for the administrative authorities to which a business can file its data electronically. Often described as a 'government transaction gateway', OTP ensures that this information reaches various administrative authorities 'intelligently and securely'. The Ministry of

[43]Statistics Netherlands Act.
[44] www.e-overheid.nl
[45]Letter from the State Secretary for Economic Affairs to ACTAL about the ACTAL recommendations on ICT policy for the reduction of administrative burdens, dated 30 August 2004.

Economic Affairs (EZ) compares the gateway to a post office for electronic messages.[46] In addition to the technical solutions, EZ starts paying more attention to the options for gradually harmonising the information that the various governmental agencies request from businesses.[47] Chain reengineering studies have concluded that requests for information should be in line with or 'fit' the core business operations. Moreover, widely accepted standards need to be used.[48] The first steps towards standardisation of business reporting have been taken.

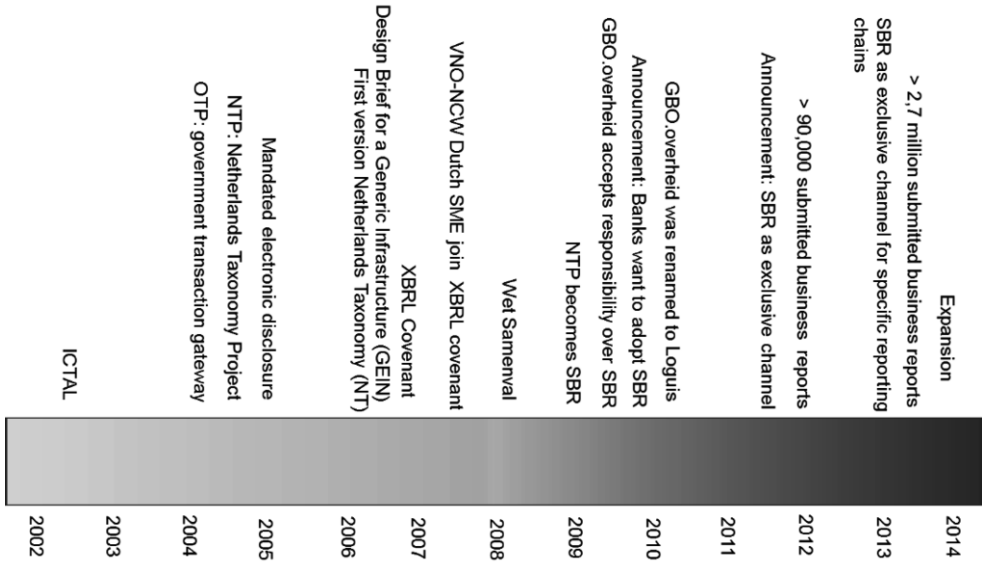


Figure A1 - The SBR timeline

The timeline illustrates the various developments that were relevant for SBR. The first part of the timeline, ICTAL and the government transaction gateway was outlined earlier. The remainder of this chapter will discuss the second part, including the 'Netherlands Taxonomy Project' (NTP), the transitions regarding the governance and the commencement of the SBR program.

[46]Letter from the Minister of Economic Affairs to the Dutch parliament on 27 May 2004; letter from the State Secretary for Economic Affairs to the Dutch parliament on 9 June 2005; both were about the Cabinet plans for tackling administrative burdens (29 515).
[47]Letter from the Minister of Economic Affairs to the Dutch parliament on 27 May 2004 about the Cabinet plans for tackling administrative burdens (29 515).
[48]Letter from the Secretary of State for Economic Affairs to ACTAL about the ACTAL recommendations on ICT policy for the reduction of administrative burdens, dated 30 August 2004.

XBRL and the Netherlands Taxonomy Project (NTP)

The pioneers' vision

The period from 2004 to 2007 featured a relatively small group of pioneers who had a shared vision for the future: making business reporting cheaper and better for companies and government agencies by using:

1. a shared (national) taxonomy,
2. a shared generic infrastructure and
3. a shared service centre that manages all the shared building blocks.

Technical aspects: a shared taxonomy and a generic infrastructure

The ministries of Justice and Finance started the NTP in 2004. The project aimed to create a single XBRL taxonomy for financial statements and fiscal declarations disclosed by businesses. An initial test version of the Dutch Taxonomy was ready by June 2005. A small group of actors started experiments with test configurations. The NTP thus fulfilled the first element of the vision: a shared taxonomy.[49]

In 2005, the State Secretary for Economic Affairs announced the implementation of a new interface in the OTP. This would later enable the use web services that allow for more modularity and flexibility in the execution of information processes, consequently satisfying an important precondition for the electronic exchange and (pre)processing of financial business reports. The State Secretary for Economic Affairs announced that for the implementation, the Ministry of Economic Affairs would develop a design brief for a generic infrastructure (GEIN programme). This design brief would describe all the requirements for the implementation of a generic infrastructure that would be used by several government agencies. Moreover, the design brief was expected to provide a preliminary sketch for a shared business reporting solution. NTP proceeded to use this design brief.

In May 2006, Minister Donner submitted the first financial statements using XBRL. In June 2006, the first version of the Netherlands Taxonomy (NT) was published. The design brief for the generic infrastructure was also completed. The idea was to develop a generic infrastructure, with the NTP project as the launching customer. This would make it easier for businesses to fulfil their reporting obligations to some government agencies (the requesting parties). The generic infrastructure is based on a service-oriented architecture (SOA). Using and reusing individual services provides the requisite flexibility allowing the infrastructure to be used generically for various processes. This will allow busi-

[49] The taxonomy is a dictionary of terms drawn up by involved government parties. The terms are derived from legislation and regulations. Reporting parties use the taxonomy to generate business reports based on their own business administration.

nesses to use a single interface, as opposed to separate ones for the Tax and Customs Administration, Statistics Netherlands, municipalities, etc. GEIN meant that the second element of the vision, the generic infrastructure, was realised.

Organisational aspects: covenant and shared service centre

On the 9th of June 2006, an initial group of organisations signed a public-private covenant. They agreed to reduce the administrative burden for businesses by applying the Dutch XBRL Taxonomy. The adoption of this taxonomy would simplify the collection, definition, exchange, validation and automated processing of data elements in relation to financial statements, fiscal declarations and statistical reports.[50] The covenant was signed on behalf of the government by the ministers of Economic Affairs, Justice, and the Interior and Kingdom relations. The minister of the Interior and Kingdom relations signed the covenant because he is accountable for GBO.Overheid. The covenant describes GBO.Overheid as the managing party for the building blocks (the taxonomy and the generic infrastructure), a first step towards the installation of a shared service centre in line with the pioneers' vision. Including the generic infrastructure in the covenant was the *de facto* start of the expansion of the scope of the NTP. The NTP was no longer solely focussed on data standardisation, it started to play a key role in the standardisation of business reporting processes and the realisation of shared building blocks. The project itself developed an initial version of the generic process infrastructure and continued to develop and maintain the new versions of the Netherlands Taxonomy (NT).

The covenant was also signed by a number of intermediaries and software suppliers involved in the development. Their task was to develop the necessary 'XBRL-ready' software packages for the market, as well as offering their customers related services (and passing on the efficiency benefits). The sector associations for accountants and fiscal advisers signed the covenant as well. The policy-making agencies and the administrative authorities (i.e. Tax and Customs Administration, Chamber of Commerce) managed the NT, the process standards and the building blocks. The covenant formalised the first form of cooperation and organisation in the context of SBR. The numerous parties involved did seem to present a challenge for the creation of a clear direction and priorities within the SBR initiative.

Implementation lagging behind – new initiatives

In the spring of 2007, the Confederation of Netherlands Industry and Employers (VNO-NCW) and the Dutch Small and medium enterprises (SMEs) association (MKB Nederland) joined the covenant. State Secretary De Jager stated at that point that he expected it to be possible for all tax declarations by businesses to be done using XBRL by 2008. Although expectations were high at the time, the

[50]Covenant on cooperation between the government and the market on using the Netherlands XBRL Taxonomy, The Hague, 9 June 2006.

uptake of solutions provided by NTP was disappointing. The project sought solutions in the form of new initiatives. For example, an amendment to Book 2 of the Dutch Civil Code (BW) was thought to provide a major impulse for use of the taxonomy. This alteration help converge the profit declarations and the financial statements for SME's.[51] The same applies for the condensed profit declaration. A small group of about eight intermediaries and the Tax and Customs Administration signed covenants at the end of 2008 for the condensed corporate profit tax return declaration and horizontal supervision.[52] On behalf of the Tax and Customs Administration, State Secretary De Jager signed the covenants, which had a two-year pilot period and which made it possible for the intermediaries to provide a significantly condensed profit tax return declaration in XBRL.

The SBR Programme

Transition in adoption and in governance

From 2009 onwards, there was a period of transition to a more focused task and its execution, which aimed to achieve credible usage of SBR by a number of frontrunners in the business reporting domain.

At the beginning of 2009, NTP became Standard Business Reporting (SBR). Budget was allocated to the SBR Programme from the Government Renewal Programme. The name change brought the SBR programme in line with international nomenclature. Inspired by the Dutch approach to SBR, Australia started a similar project and made good use of the ideas that had been realised so far.

A clear objective was defined for the SBR Programme in the Netherlands: realising a generic government solution for the system-to-system (S2S) exchange and processing of business reporting information.

At the time, the adoption of XBRL (i.e. the NT) for business reporting was still beneath expectations. Less than ten thousand messages were delivered in XBRL, whereas several hundred thousand messages per year were needed to get anywhere close to the anticipated reduction in the administrative burden. The parties involved recognised an excessive focus on all kinds of new initiatives as the main cause for delayed growth. The ministries involved decided to shift the focus of SBR to broader usage of the NT and linking the private sector to the generic infrastructure for the exchange of messages with the Chamber of Commerce, Tax and Customs Administration and Statistics Netherlands.

---

[51] Article 2:396 paragraph 6BW ('Wet Samenval'), as implemented by the Fiscal and Commercial Financial Statements (Alignment) Act (Staatsblad 217, 2008). This made it possible for small legal entities to draw up financial statements in accordance with fiscal principles, i.e. using the accounting principles as applied for the corporate income tax declaration.

[52] Covenant on a pilot for the abbreviated profit declaration for corporate income tax, based on the Netherlands Taxonomy and using process definitions, 11 December 2008.

The implementation of the SBR Programme, including management of the NT, was transferred to GBO.Overheid. Consequently, this organisation also became responsible for the coordination of the generic infrastructure besides the taxonomy that it was already managing. In the autumn of 2009, a governmental steering committee was set up for the governance, in which both the requesting parties and the ministries in question were represented at the highest departmental level. The committee's role was to monitor the progress. The Secretary-General of the Ministry of Economic Affairs was initially the chair of this steering committee. Within the SBR Council, agreements were made with market parties. The requesting parties and GBO.Overheid drew up a joint implementation plan in order to realise both the substantial utilisation of SBR in financial areas and to set up the framework for sensible expansion of SBR (application in other information chains). The board of project leaders was given instructions to realise the 'substantial utilisation', starting with the market parties already involved (the pioneers). Gradually, it became apparent that the governance structure was not yet properly equipped for a scaling up and substantial utilisation. Agreements that are more detailed were required, for instance about web services, service levels, etc. In addition, the new SBR Programme immediately had to address a pressing governance question. State Secretary Heemskerk announced in November 2009 that three major banks were going to adopt SBR for their credit reporting. These banks collaborate in the Financial Reporting Partnership. They would be using their own technical infrastructure and their own extension taxonomy. The banks stated that they would conform to the governmental standards and would aim to use the same interfaces as the government. However, there was no detailed plan available on how this would be realised in practice.

Towards large-scale use

In 2010, GBO.overheid was renamed to Logius. The objective of the SBR programme for 2010-2011 was to realise large-scale adoption of SBR (i.e. a large volume of XBRL messages within the financial domain) alongside stable performance and management of the building blocks. Intensive cooperation, public-private agreements and lobbying allowed the SBR parties to achieve a considerable increase in scale.

In 2011, the number of VAT declarations grew to about 87,000 and the number of financial statements grew to about 3500. The organisation at Logius changed during this period. The upscaling demanded a mature management organisation, a focus on shared services and renewed attention had to be paid to the governance, particularly where it interfaced with the market.[53] Within the programme, it was important to provide enough operational support for companies

[53] Alignment with the market was achieved for example by involving reporting parties in the taxonomy-testing phase, before proceeding towards administrative approval and publication. This gives the taxonomy a certain formal status, a quality level that users could rely upon. The arrival of the taxonomy did not alter the fact that a user (often accountants or intermediaries) remained responsible for proper business reporting.

working on the implementation and implementation support for new companies joining in. Logius and the requesting parties made sure that their service desks were in contact with one another, that the external communication was coordinated and all aspects would be discussed at public (open) briefings. The project management board had a key role in giving instructions to the shared service centre: Logius. Answers were sought to questions regarding the outsourcing of specific activities and the long-term funding. During this process, the spotlight moved to organisational and legal preconditions. During the NTP, an appendix on legal considerations in the GEIN design brief was deemed sufficient. However, in the SBR programme, a dedicated compliance working-group was installed and tasked with the alignment of compliance efforts across jurisdictions.

SBR as an exclusive channel
The solution for realising 'the vision' (i.e. better and cheaper business reporting thanks to a shared taxonomy, a generic infrastructure and a shared service centre) was now in place. It is managed in a way that allowed the SBR programme to take the next step. The government agencies understood that complete adoption by the market and the step to proper service management could not be realised if SBR remained a voluntary solution for business reporting. Market parties acknowledged this as well.

In June 2011, the ministers of Economic Affairs, Agriculture and Innovation and the State Secretary for Finance agreed to turn SBR into the exclusive information delivery channel for the corporation tax and income tax declarations as of 1 January 2013. VAT declarations were to follow in 2014. That signalled the start of an era in which the existing channels were phased out and which required intensive preparation of the market and preparation within the Tax and Customs Administration and Logius.

The use of SBR would only be mandatory for declarations that reporting parties (businesses or their intermediaries) sent in directly from software packages, thus system-to-system. For that reason, this step is referred to as 'mandating' the use of SBR. Alternatives, such as submitting reports via a portal on the Tax and Customs Administration website, will nevertheless continue to exist. For the market, the consequence of the mandatory use of SBR is that the same interfaces will be used to communicate throughout the domain. However, this also means that the government agencies will not be able to implement major changes in the short term. Changes in the public domain require a lengthy preparation and consultation; those affected are no longer a well-defined group, as was the case in the initial years of SBR. Greater attention has to be paid to continuity during maintenance and incidents occur more often.

Another aspect that required immediate attention was an I-process for e-Notification and identification resources (in particular for authorisations). Solutions were operational mid-2012. In addition, the SBR parties took action to prevent

that the distribution of Public Key Infrastructure (PKI) certificates[54] became a bottleneck because just a few suppliers were issuing certificates that were in accordance with the PKI-government framework. This period signalled a number of changes for the governance. In order to comply with the preconditions for mandating SBR, such as e-Notification and certificate distribution, the project management board kept a close eye on the various projects. Moreover, the impact of the mandatory use of SBR in specific chains on the services provided by Logius had to be specified, alongside the requirements it imposed. To be successful a detailed description was needed of Logius' services relating to the taxonomy, the generic infrastructure and the agreements associated with it. This was realised using an extended service portfolio that enables both the customers (requesting agencies) and the SSC to know what to expect and not expect from a service. Clearly defined services enable parties to understand service offerings, including what each service does and does not include, eligibility, service limitations, cost, how to request services, and how to get help. A well-defined service also identifies internal processes necessary to provide and support the service.

The Tax and Customs Administration and the Ministry of Economic Affairs took on the role of the policy-making principal, with the requesting parties as the customers for SBR chains. The financial aspects were examined in depth as well. A pricing model was developed for allocating the costs of using the services as a ratio of the number of messages and/or users of a SBR chain.

Intensive efforts were made with various sector associations to inform the private sector. They actively disseminated information about the progress of SBR, the status of the software packages and the correct application of the SBR elements such as the taxonomy, the interfaces and the information processes. The SBR team of Logius supported the already connected parties, as well as parties in 'candidate chains' that were to be connected in the future. The government agencies understood that transparency on the SBR Programme and the accessibility of relevant rules and regulations was crucial for getting parties on the bandwagon. Moreover, it is a prerequisite for good governance. All this meant that the implementation of organisational and legal preconditions keeps on evolving. Efforts were undertaken in various fields in order to construct a legislative and regulatory basis for applying SBR and formalising the role of the shared service centre (Logius).

Meanwhile the financial accounting domain had already started the process of making SBR mandatory for disclosing financial statements. At the end of 2012, the Chamber of Commerce started to prepare the necessary changes. They began

[54] The SBR parties obligate the use of a PKI-government certificate for the system-to-system disclosure of business reports. These certificates are issued by a limited number of parties who complied with the specific requirements for the PKI-government (the PKI-government Design Brief). This is the most reliable authentication mechanism.

with a decision to facilitate the use of SBR and to discourage the disclosure of business reports in the PDF format.[55] For smaller companies who did not prefer to use SBR, the Chamber of Commerce developed a self-service online portal for the manual (non-system-to-system) disclosure of financial statements. The portal converts the financial statements as supplied into XBRL and forwards that data to the Trade Registry.

Banks expected positive effects from the mandatory use of SBR in their own chains. They anticipated an increase in the number of delivered credit reports.[56] However, they did not make SBR mandatory (yet). Nevertheless, the banks seized the momentum of the governmental mandate to encourage the use of SBR for credit reports. Banks developed a portal for manual submission as an alternative for entrepreneurs that do not have software for system-to-system submission.

Software and intermediary services
The majority of businesses (especially entrepreneurs and small enterprises) will not deal with SBR directly. The exceptions being those who submit their own business reports or develop their own software. For intermediaries and software providers who have made investments for applying SBR or plan to do so, SBR will change their service offering to their customers. More and more intermediaries will use online bookkeeping software and portals for exchanging data with their customers. There are also intermediaries – accountants, bookkeepers, tax consultants – and sector associations who are frontrunners with regard to SBR. They have already been working with SBR, have been involved with the development and are encouraging further application. Besides these frontrunners, there have been intermediaries that have held off implementation of SBR until it became mandatory. Sector associations played an important role in educating and involving the diverse groups of intermediaries.

Software providers were preparing their packages for SBR. This group also included frontrunners, who were quick to make preparations and software providers that were mobilised to take action via the SBR programme. Both fiscal soft-

[55] One question that was also studied during the preparations was the responsibility for the financial statements section of the taxonomy. The taxonomy is based on legislation. In contrast to the Tax and Customs Administration, The Chamber of Commerce receives the financial statements; however, it has no direct relationship with the legislator on financial statements: the Ministry of Justice. Given the legislative situation, the Ministry of Justice would have been the obvious owner of the financial statements taxonomy. However, the ministry was – by choice – not as closely involved in SBR as the Chamber of Commerce, despite the fact that the Minister of Justice signed the covenant in 2006. In 2013, the Council for Annual Reporting was asked to give their stamp of approval on the financial statements taxonomy from that point on.
[56] Financial Reporting Partnership, press release issued on 31 May 2011, on www.rapportageportaal.nl.

ware providers and the intermediaries' sector associations stated their intention[57] not to charge their customers for the investments costs made in the transition to SBR.

Expansion: introducing SBR in other reporting chains
The following period, 2012-2013 and after, was all about expanding SBR to other domains. Expansion refers to the use of SBR services in other information chains. The core of the services provided by the SSC was already well structured from 2012 onwards. In 2013, the governance and the procedures surrounding SBR were worked out in more detail. The strategy for expansion was included as well. In practice, the information processes turned out to be very similar in various domains: the same legislative and regulatory context applies everywhere for submitting business information and sending notifications. This made it possible to apply SBR as a solution in other reporting chains. Moreover, getting more requesting parties to apply SBR surges the benefits of system-to-system information exchange and processing using shared services. Against this backdrop, actors set out to explore the options for expanding SBR to other domains. One domain where this was successfully done was the agricultural domain, referring to the business economics reporting by the intermediaries of agricultural enterprises to the Agricultural Economics Research Institute (known as LEI). LEI in turn submitted this data to the European Commission. The SBR expansion strategy focuses on financial and social business reporting in the public and semi-public sectors. The options explored or described as part of the programme also involved domains such as education, healthcare and housing corporations. Newcomers (requesting parties) have to go through an 'accession' procedure to check whether they comply with the agreements that apply for SBR.

Key features of SBR
We want to conclude this background description with a brief overview of the key features of SBR. Knowing these features contributes to the understanding of what SBR is and is not.

- SBR focuses on optimising the benefits of system-to-system information processing. 'System-to-system' means automated communication between computers, initiated and handled without human intervention.
- SBR is initially designed for information exchange with professional businesses (ranging from entrepreneurs to multi-nationals).
- Businesses can employ SBR for disclosing information to requesting parties in the public sector (such as Statistics Netherlands) and to private institutions such as banks.
- In both cases, the focus is on business reports: financial data about the business derived from its own business administration.
- 'Unequivocal business reporting' within SBR is based on generic activities that have to be performed for each of the various business reporting

[57] Letter of intent from the SBR Council, 27 May 2011

chains, such as receiving, validating, routing and confirming. This can also be considered as the pre-processing of information. The actual processing of the content for analysis and decision-making, including the associated legal consequences, are beyond the scope of SBR. Jurisdictions differ in respect of their policy and legislative environment and their administrative practices and culture. Efforts are being made to standardise and harmonise the definitions of terms, but their interpretation still depends on the relevant legislation and regulations in a specific domain.

- The business 'brings' the data. Submitting business information via SBR is often obligatory, but businesses do so on their own initiative. There is no central database or data pool, to which businesses have uploaded their information and requesting agencies can obtain whatever they need whenever they want. Thus, single information delivery for all reporting purposes is out of the question. In accordance with the law, each business uploads a specific set of data tailored to a specific request (e.g., 2011 tax declaration, 2010 financial statements, and so on). However this does not change the fact that requesting parties may share certain information amongst one another (e.g., between Statistics Netherlands and the Tax and Customs Administration).
- The principle '*store once, report to many'* applies to SBR. After the data has been properly stored in the business administration, reporting parties can send their business reports via one channel (interface) to various requesting parties.

Consulted sources
In addition to the internal sources of the SBR Programme, this background description used the following sources:

Press releases

- *SBR in 2010-2011, Cooperation for large-scale use and stable management*, SBR Programme, 2010, (in Dutch) www.sbr-nl.nl
- *Banks positive about the administrative authorities' decision to use SBR as the exclusive reporting channel*, Financial Reporting Partnership, 31 May 2011 (in Dutch), www.rapportageportaal.nl

Documents

- Letter from the Minister of Economic Affairs to the Second Chamber of the Dutch parliament about Cabinet plans for tackling administrative burdens (29 515), 27 May 2004.
- Letter from the State Secretary for Economic Affairs to ACTAL about the ACTAL Recommendations on ICT policy for the reduction of administrative burdens, 30 August 2004.
- Letter from the State Secretary for Economic Affairs to the Second Chamber of the Dutch parliament about Cabinet plans for tackling administrative burdens (29 515), 9 June 2005.
- Finalised design brief for the generic infrastructure, Ministry of Economic Affairs, March 2006.
- Covenant on cooperation between the government and the market on using the Netherlands XBRL Taxonomy, 9 June 2006.
- Covenant on a pilot for the abbreviated profit declaration for corporate income tax, based on the Netherlands Taxonomy and using process definitions, 11 December 2008.
- Letter of intent from the SBR Council, 27 May 2011.

Appendix B – Writing process

The SBR knowledge retention project aimed to capture the knowledge developed in the SBR Programme and make it available to everyone. More specifically, Logius asked the editors to describe the key aspects of SBR as a challenge and as a solution for information chains, using the relevant concepts and theories in literature for explanation and clarification. In order to achieve this objective, the following steps were taken:

1. Together with the client (Logius), an editorial team was set up that comprised academics and practitioners working on the realisation of SBR.
2. The editors produced a chapter layout and an initial overall setup for the book that was then refined and presented to the client.
3. The editors asked several authors to help with the various chapters. The authors were specialist involved directly in practice in complex themes such as information processes, data specifications, platform technologies, information security and chain governance.

The editorial team – plus the authors – made up the research project team. This team has used a variety of research instruments to produce this book. The figure below provides an overview of the research instruments.

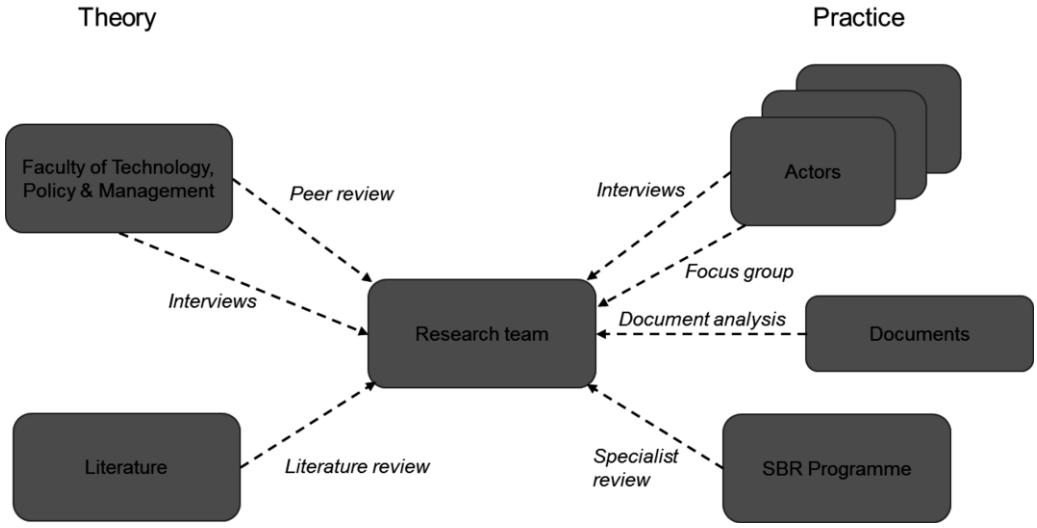


Figure B.1 – Overview of the research tools and methods applied

A comprehensive set of tools was needed because the writing period overlapped with some key developments in the SBR Programme, including the mandatory use of the XBRL and the generic infrastructure in a couple of information chains. The various components in Figure B.1 are explained next.

Interviews. Starting from the knowledge already available in the SBR Programme, in-depth interviews were held as a way of capturing the tacit knowledge

of those working in the SBR Programme. The interviews were semi-structured (half open) of thirty to ninety minutes. Some of the SBR specialists were interviewed more than once. The interviews identified some key themes (i.e., information processes, data specifications, platform technologies, information security and chain governance) surrounding SBR and also revealed some questions that required more in depth literature review and focus groups (e.g., the setup of the taxonomy and the generic infrastructure).

Literature review. Based on the themes and questions that surfaced during the interviews, the research team started with an comprehensive literature review. The available national and international literature on the key SBR themes (i.e., information processes, data specifications, platform technologies, information security and chain governance) was collected and examined from 2011 to 2014.[58]

Document analysis. In addition to the scientific literature, the research team also used official government documents on for instance the SBR Programme and its governance plus – when permissible – minutes of working group meetings.

Peer reviews. Initial ideas and lines of thought for this book were presented as focused articles and then discussed with a broader subset of academic readers, for example in research meetings and international conferences. We gratefully made use of the responses we received in the preparation of this book.

Specialist reviews. The research team presented its interim results (i.e., draft chapters) to specialists for review. The editors selected the reviewers based on their level of expertise on the subject matter and their distance from the SBR Programme. The latter was needed to safeguard that the quality of the chapters could be assessed independent of the SBR Programme and the knowledge retention project. An overview listing the reviewers can be found in the section entitled ' About the contributors'.

Focus groups. Four focus group sessions were held with the actors involved in the SBR Programme. The purpose of each focus group session was to assess intermediate questions and results and refine them further in a collaborative setting. One of the focus group sessions (labelled as the knowledge retention session) used the group decision support facilities at the Faculty Technology, Policy and Management. Using the facilities allowed the editorial team to systematically query 17 practitioners on their current thoughts and concerns regarding various subjects in SBR (e.g., the I-process specifications and the governance).

[58] The digital library at Delft University of Technology allows for systematic searches of the (international) literature. It provides direct access to the databases of IEEE, ACM, SCOPUS and ISI, as well as its own catalogue of publishers (such as Elsevier, Wiley, Springer etc.). See www.library.tudelft.nl.

Appendix C – Glossary and abbreviations

Glossary

A

Approval (permission or access rights)	claim that an intermediary is permitted (authorised) to use a given service, send or obtain a specific message on behalf of a represented party (the client)
Authentication	determining the identity of an reporting party responding to a request, with a predefined level of reliability
Authorisation (process)	checking whether an actor is permitted or approved by a represented party to use a given service, send or obtain a specific message
Automated handling, computerised handling	non-manual execution of tasks with the help of information technology

B

Business information (accountability information)	information about the performance of an organisation or the situation within an organisation that is requested by a third party

D

Data	facts or concepts in a format that is suitable for communication, interpretation and processing into information, either by humans or automated systems, or both
Data specification	the syntactic and semantic requirement for data in an instance, exchanged via the generic process infrastructure.
Digipoort	the Dutch government's generic process infrastructure

E

Expansion	the application of SBR in information chains that have not yet adopted (parts of) this standard
Extensible Business Reporting Language (XBRL)	an open (XML based) machine readable standard for defining structured data as plain text

G

Generic (process) infrastructure	a system of technological components required for automatically handling and (pre)processing messages such as business reports and status notifications. Infrastructure components include interface specifications, I-process specifications and (meta)data specifications.
Generic platform	The term platform refers to services and a generic process infrastructure. Services include both organisational services (e.g., helpdesk support, training sessions for users/software developers) and technical services (i.e., interface services and information pro-cessing services). The adverb generic implies that the platform should be able to service multiple information chains.

I

Independent user	a user (see: user) of one or more i-processes, who does not participate in the public governance. these are typically individual companies and intermediaries
Information chain	a series of at least two organisations that exchange and process information sequentially
Information exchange	electronically sending or receiving data and/or messages from one party to one or more others
Information processing (data processing)	actions related to handling information and/or messages, including recording, saving, modifying, using, forwarding, distributing, linking, securing and destroying information
Information provider	see: reporting party
Information requester	see: requesting party
Instance document	a list of XBRL tags that each has its own specific value and refers to specific concepts in the taxonomy
Interface	the actual implementation of a set of agreements and standards permitting the exchange of data between information systems
Interface service	Interface services are the technical applications that can accept messages (e.g., business reports and notifications) from outside the SSC or deliver messages to another interface service.
Interface specification	a set of agreements and standards permitting the exchange of data between information systems
Intermediary	a service provider that is approved to act on behalf of a beneficiary
Interoperability	the extent to which the various technologies used within an information chain can communicate with each other or can be used together for a given purpose
I-process	an automatized information handling process between different users, composed of web services.

L

Loose coupling	removing the direct links between business functionality and the technical implementation

M

Message	a digital collection of elements with a specific meaning coming from a specific sender (system, organisation or person) addressed to a recipient (system, organisation or person). Messages can include content (i.e., a business report) or contain processing status information (e.g., the message has been received successfully and is accepted for further processing). The generic infrastructure handles messages to and from requesting parties.
Metadata	data that describes the characteristics of other data: data about data

N

Netherlands Taxonomy (NT)	a shared taxonomy used by the requesting parties to prescribe the required semantics and syntax within the SBR context
Netherlands Taxonomy Architecture (NTA)	a set of agreements that determines which elements of the XBRL standard are included in a taxonomy and how
Notification, e-notification	when the requesting party sends a substantive message to a stakeholder / information provider

O

Open standard	a standard that can freely be used by all

P

Participant	a user (see: user) of one or more i-processes, who participates in the public governance
Process	a serial set of tasks with a set objective
Processing services	the various applications that realise automated handling of I-processes. The key processing services include the authentication service, the authorisation service and the validation service.

R

Reporting chain	a chain that has been set up for generating and processing business reports, based upon legislation and regulations
Reporting party	an private, a semi-public or public organisation that submits information using SBR. This can be a legal entity with reporting obligations as well as an authorised professional intermediary (e.g., tax specialist, accountant) that submits information on behalf of its client.
Reporting process	an inter-organisational process focusing on the exchange and processing of business information
Requesting party	a (semi-)public or private party that requests information from other parties and imposes requirements on how it is submitted using SBR

S

SBR framework of agreements	the agreements and standards adopted by the public and private parties involved in SBR
SBR programme	a governmental initiative aimed at realising SBR in business reporting chains, in which governmental parties and market parties collaborate
Service	the provision of a commodity
Solution	a solution is an answer (delivered by Logius) to the need for electronic information exchange within a chain. a solution consists of one or more i-processes, data specifications and technical support
Specifications	a formal definition of requirements which a service, system or application has to meet

Standard Business Reporting (SBR)	a solution for the automated, inter-organisational exchange and processing of information
Submission reference number	a number that tells the reporting party where it can obtain the information it wants regarding its submission
Submission service	an interface service that enables the S2S exchange of messages between reporting party and the generic infrastructure. When tax reports are submitted, we also use the term 'filing'.
System-to-system (S2S) integration	data exchange and processing between the internal information systems of the transacting organisations is fully automated: no human assistance is required.

T

Taxonomy	a collection of controlled dictionary definitions that are organised into a hierarchical structure

U

User	a public or private party (information provider, intermediary, entrepreneurs/business, requesting party) that employ SBR specifications or services

W

Web service	an operationalised application with a specified input, throughput and output of information. a web service is part of an i-proces and can be divided into interface services and processing services

Abbreviations

Abbreviation	Meaning
A	
ACM	Authority for Consumers and Markets
API	Application programming interface
ASCII	American Standard Code for Information Interchange
ASL	Application Services Library
ASx	Applicability Statements, version x
AuSP	Authorisation Service Provider
Awb	General Administrative Law Act
B	
B2B	business-to-business
B2Bi	business-to-business integration
B2G	business-to-government
BAPI	Belastingdienst Advanced Program Integration, a S2S standard used for information exchange with the Tax and Customs Administration
BISL	Business Information Services Library
BPEL	Business Process Execution Language, shortened form of BPEL4WS
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modelling Notation
BPR	Business Process Re-engineering
BSN	Citizen service number
BW	Dutch Civil Code
BZK	Ministry of the Interior and Kingdom Relations
C	
CA	Certificate Authority
CBP	Dutch Data Protection Authority
COBOL	Common Business-Oriented Language
CP	Certificate Policy
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Service Provider
D	
DSR	Digilink Service Register
DTS	Discoverable Taxonomy Set

E

ebMS	Electronic business XML Message Service
ebXML	Electronic business using eXtensible Markup Language
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EDIINT	EDI over the Internet
ESB	Enterprise Service Bus
ETSI	European Telecommunications Standards Institute
EZ	Ministry of Economic Affairs

F

Fi-number	Fiscal number
FRC	Financial Reporting Partnership
FRIS	Financial Reporting Instance Standards
FRTA	Financial Reporting Taxonomy Architecture
FTP	File Transfer Protocol

G

GEIN	Generic Infrastructure Programme

H

H2H	human-to-human
H2S	human-to-system
HRN	Trade Register Number
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol (Secure)

I

IASB	International Accounting Standards Board
IB	income tax
ICT	Information and Communication Technology
ICTAL	IT for the Reduction of Administrative Burdens
IDABC	Interoperable Delivery (of European e-Government Services) to Public Administrations, Businesses and Citizens
IEFT	Internet Engineering Task Force
IFRS	International Financial Reporting Standards
I-process	information processing process
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

J

JIT	Just-in-time

K

KPI	Key Performance Indicators

L

LSS	Lean Six Sigma

M

MIME	Multipurpose Internet Mail Extensions
SMB Netherlands	organisation of small and medium-sized businesses in the Netherlands
MSA	Mail Submission Agent
MSP	Multi-Sided Platform
MTA	Mail Transfer Agent

N

NBA	Netherlands Institute of Chartered Accountants
NIST	National Institute for Standards and Technology
NIVRA (now NBA)	Royal Netherlands Institute of Chartered Accountants, now the Netherlands Institute of Chartered Accountants
NORA	Netherlands Government Reference Architecture
NT	Netherlands Taxonomy
NTA	Netherlands Taxonomy Architecture
NTP	Netherlands Taxonomy Project

O

OASIS	Organization for the Advancement of Structured Information Standards
OBM	Object Management Group
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OIN	Government Identification Number
OSI	Open Systems Interconnection
OSWO	Software Developer Support unit

P

PA	Policy Authority
PDF	Portable Document Format
PI	Process infrastructure
PKI	Public Key Infrastructure
PKIgov	Public Key Infrastructure for the government
PMBoK	Project Management Body of Knowledge

POP3	Post Office Protocol version 3
PRINCE2	PRojects IN Controlled Environments

R

RA	Registration Authority
REST	Representational State Transfer
RSA	public key cryptographic algorithm, developed by Rivest, Shamir and Adleman
RSIN	Legal Entity and Partnership Information Number

S

S2S	system-to-system
SaaS	Software as a Service
SBA	Tax Assessment Service Message
SBR	Standard Business Reporting
SDM	System Development Methodology
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSC	Shared service centre
SSL	Secure Socket Layer
STP	Straight-through processing
SVBR	Semantics of Business Vocabulary and Business Rules
SVR	Simplified Validation Rules

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
ToC	Theory of Constraints
TQM	Total Quality Management
TTP	Trusted Third Party

U

UBL	Universal Business Language
UDDI	Universal Description, Discovery and Integration
UML	Unified Modelling Language
URL	Uniform Resource Locator
US-GAAP	United States Generally Accepted Accounting Principles

V

VNO-NCW	Confederation of Netherlands Industry and Employers

VPB	corporation tax
VPB/IB	corporation tax/income tax
VPN	Virtual Private Network
VSA	Value Stream Analysis

W

W3C	World Wide Web Consortium
Wbp	Netherlands Personal Data Protection Act
WfMC	Workflow Management Coalition
WRR	Scientific Council for Government Policy
WSDL	Web Services Description Language
WUS	acronym for WSDL, UDDI and SOAP

X

XBRL	eXtensible Business Reporting Language
Xlink	XML Linking Language
XML	eXtensible Markup Language
XPDL	XML Process Definition Language

About the Contributors

Bas Avis
Bas Avis has years of experience with data exchange between companies and administrative authorities, working as a business consultant, project manager and account manager. He is currently Delivery Manager Connection Support at Logius. His responsibilities include arranging support for SBR parties during the connection phase. Bas operates from his own company, BA Management Consultancy, and can be contacted via bas@ba-consultancy.nl.

Bas's contribution: general.

Victor den Bak
Victor den Bak MSc works at EBPI as architect and contributes to SBR projects since 2012. His role is to ensure that information technology is correctly embedded in the SBR information processes and that new/modified processes comply with the generic requirements and frameworks imposed for compliance, information security and reuse of standardised components. Victor can be contacted via victor@ebpi.nl.

Victor's contribution: co-author of Chapter 7

Sebastiaan Bal
Sebastiaan Bal LLM, RA leads the data management team at Logius. He contributed to the SBR Program since 2010. During this period, he was responsible for the realisation of the Netherlands XBRL Taxonomy. Sebastiaan is an expert on data standardisation (syntax and semantics), data exchange, processing and analysis. His peers consider him as leading expert on XBRL. He can be contacted via s.bal@thauris.nl.

Sebastiaan's contribution: lead author of Chapter 5, co-author of the revised version of Chapter 2, participation in the knowledge retention session.

Mark Bisschop
Mark Bisschop has a background in accountancy and is affiliated as a consultant to *XBRL voor Accountants* and *DOCCO*. He currently advises accountancy firms on IT and business processes. In addition, he is the co-author of the XBRL Manual for Financial Advisers (in Dutch). During the period from 2010 to 2013, Mark worked on the SBR Programme at Logius. Mark can be contacted via mark@xbrlvooraccountants.nl.

Mark's contribution: general.

Nanko Boerma
Nanko Boerma acted as the Programme Manager for the SBR Programme from 2010 to 2013. He was responsible for formulating the strategic and policy frameworks that allowed for the progression of the SBR Programme. Currently Nanko is the president of the Transactieland.nl-foundation, which strives to position the Netherlands as a world-class knowledge centre on transaction-management. The foundation is a partner for scientific research in this field. Nanko can be via nanko.boerma@transactieland.nl

Nanko's contribution: general.

Ella Broos
Ella Broos acted as the Market Support and Communications Manager the SBR Programme from 2010 to 2013. She is an interim communications manager with expertise in crisis communication and marketing, working largely in the ICT and security domain. She can be contacted via: info@brooscommunicatie.nl.

Ella's contribution: review of the Preface, chapters 2 and 3 and Appendix A (The background to SBR).

Rob Dortland
Rob Dortland PhD has held a variety of management and non-management functions in administrative authorities. His most recent role was that of deputy inspector-general of the Food and Consumer Products Safety Authority. In this role, he engaged in the development of innovative chain monitoring and supervision methods based on Continuous Control Monitoring. He was associated (part-time) with Logius since 2011 as the SBR Agro-domain liaison. Rob currently works as an independent consultant in the areas where government and commerce intersect. Rob can be contacted via rob.dortland@gmail.com.

Rob's contribution: general, participation in the knowledge retention session.

Welmoed Fokkema
Welmoed Fokkema LLM had an active role within the SBR Programme at Logius from 2009 to 2013 as the Compliance consultant, responsible for ensuring compliance and giving advice on legal aspects of SBR. Welmoed specialises in compliance of business processes, data exchange, information security and governance. Since the end of 2013, she has been employed as a Compliance Manager in the pharmaceutical sector. Welmoed can be contacted via welmoed.fokkema@gmail.com.

Welmoed's contribution: co-author of Chapters 4 and 8 and Appendix A.

Bart Hendriksen
Bart Hendriksen has been involved in the SBR Programme as a process analyst and architect at Logius since 2011. In this role, he has contributed actively to the realisation of various components of the generic infrastructure, including e-Notification and e-Authorisation. Bart specialises in service-oriented architecture, information security and I-processes. Bart can be contacted via b.hendriksen@thauris.nl.

Bart's contribution: co-author of Chapters 7 and 8.

Jan Hidders
Dr. Jan Hidders is an assistant professor at the Web Information Systems group of the Delft University of Technology. He conducts research on tools for Ontology Management and the publication of existing data as Linked Open Data. Other research subjects that he works on include the optimisation of big data-processing for graph analytics and more specifically, the development of indexes for data mining databases. Jan can be contacted via a.j.h.hidders@tudelft.nl.

Jan's contribution: review of Chapter 5.

Alexander Hielkema
Alexander Hielkema has been employed at Logius since 2008 in various roles, all which served the development and management of the generic infrastructure. From 2010 to 2013, Alexander's responsibilities included the management and commercial operation of the generic infrastructure. Alexander is an experienced IT manager and an expert in managing the IT resources used in data exchange. Alexander can be contacted via alexander.hielkema@logius.nl.

Alexander's contribution: general, participation in the knowledge retention session.

Frans Hietbrink
Frans Hietbrink RE RA has championed the SBR concept since 2009. He is currently a strategic adviser for SBR/XBRL at the Tax and Customs Administration. He has worked for the Administration for more than 30 years and held various positions during this period, including that of external tax-auditor, internal auditor and manager. Frans is particularly interested in reengineering administrative processes and improving data quality. Frans can be contacted via f_hietbrink@belastingdienst.nl.

Frans's contribution: review of the entire book, participation in the knowledge retention session.

Marc van Hilvoorde
Marc van Hilvoorde was involved in SBR right from the very start and is the spiritual father of the Netherlands Taxonomy. He has written various articles about the XBRL standard and XBRL assurance, as well as contributing to the production of the international edition of 'XBRL for Dummies'. Marc works at Logius and can be contacted via marc.van.hilvoorde@logius.nl.

Marc's contribution: review of Chapter 5.

Roland Hommes
Roland Hommes has been an architect with the SBR Programme since 2009. Before that, he represented the Tax and Customs Administration in the NTP as an XBRL specialist. Roland has worked on various XBRL specifications and is an independent consultant who work on structured digital data exchange. He can be contacted via info@rhocon.nl

Roland's contribution: review of Chapter 5, participation in the knowledge retention session.

Niek van Huizen
Niek van Huizen has been working for Logius since 2011 as a Change Coordinator, more specifically with responsibility for the process of structure implementation of changes via releases on the generic infrastructure for SBR. Niek has a great deal of experience in leading projects, in process implementation, process execution and process evaluation within ICT organisations. Niek is currently working for Logius and he can be contacted via niek.van.huizen@logius.nl.

Niek's contribution: review of Chapter 7.

Jeroen van Hulten
Jeroen van Hulten CSPM currently leads the Chain Information Services department at Logius. In his previous role at the Tax and Customs Administration of the Netherlands, he guided several e-government initiatives such as mandatory electronic tax filing by businesses, the use of DigiD (electronic ID for citizens), the pre-filing of tax declarations and the introduction of SBR. Jeroen has authored a number of articles on business cases and project risk management. He can be contacted via jeroen.van.hulten@logius.nl

Jeroen's contribution: general, participation in the knowledge retention session.

Mark Janssen
Mark Janssen CISSP CISA has been involved with the Logius product PKIgov since 2007. He works for Logius as a Coordinating Special Advisor on Business Operations, for which he also has the role of PKIgov Policy Authority. Mark knows a great deal about information security in general and public key infrastructures (PKIs) in particular. Mark can be contacted via mark.janssen@logius.nl.

Mark's contribution: review of Chapter 8.

Joris Joosten
Joris Joosten was involved as early as 2007 in the design of the interfaces for the generic infrastructure. After a variety of jobs within e-government, Joris is now an architect at Logius, working on authentication and authorisation. Joris can be contacted via joris.joosten@logius.nl.

Joris's contribution: review of Chapter 7.

Bram Klievink
Dr. Bram Klievink is an assistant professor at the Delft University of Technology. He was involved in various projects on e-government research and large-scale ICT innovations in international trade networks. Bram has received an NWO Veni grant enabling him to study governance models for public-private information infrastructures. Bram can be contacted via a.j.klievink@tudelft.nl.

Bram's contribution: review of Chapter 4.

Stephan Kockelkoren
Stephan Kockelkoren has been the Process Coordinator for the SBR Programme at Logius since 2010. He is responsible for aligning the functional requirements of the parties involved at the chain level and for translating them into specifications for process handling in the generic infrastructure. Stephan is an expert in chain orchestration, process modelling (BPNM) and process implementations in the Generic Infrastructure. Stephan works at Cojito and can be contacted via stephan@cojito.nl.

Stephan's contribution: review of Chapter 6, participation in the knowledge retention session.

Sylvia Korpershoek
Ms Sylvia Korpershoek MSc specialises in financial reporting at Thauris. She works on several SBR topics since 2013. Sylvia can be reached at: s.korpershoek@thauris.nl.

Contributions made by Sylvia: co-author of the revised version of Chapter 2 and review of the entire book.

Baldwin de Kruijf
Baldwin de Kruijf is a Transition Manager for the SBR Programme at Logius since 2011, a role that has given him responsibility for the transition of the SBR Programme to the line organisation within Logius. Baldwin specialises in service management. Baldwin is currently working for Logius and he can be contacted via baldwin.de.kruijf@logius.nl.

Baldwin's contribution: general.

Stefan van der Kwaak
S.W. van der Kwaak MMC has been involved in the SBR Programme since 2009. Originally, he was part of the steering team at the Ministry of Economic Affairs. From 2011 onwards, he worked for the SBR team at Logius, where he produced an inventory of the possibilities for wider application of SBR, particularly in the agricultural sector. Stefan freelances as an independent professional and can be contacted via stefanvanderkwaak@inter-esse.nl.

Stefan's contribution: general, participation in the knowledge retention session.

Peter Leijnse
Peter Leijnse holds a master's in Compliance Design and Management and is a senior architect at Logius. He has been actively involved in designing usable, reliable and secure solutions for information exchange in chains, both between businesses and administrative authorities (e.g., generic infrastructure, e-Invoicing), between the authorities and the public (MijnOverheid) and within the government (Digilink). Peter can be contacted via peter.leijnse@logius.nl.

Peter's contribution: co-author of Chapter 7, participation in the knowledge retention session.

René van der Meij
Mr René van der Meij MSc works as a Consultant at Thauris since 2014. As a data analyst René has contributed to the development of SBR, in particular with respect to the semantics in business reporting. René can be reached at: r.vandermeij@thauris.nl.

Contributions made by René: co-author of Chapter 5.

Gabriëlle van Mourik
Gabriëlle van Mourik has worked as a senior project manager for Statistics Netherlands (Statistics Netherlands) since January 2007. From July 2010 to December 2012, she was responsible at the CBS for the implementation of XBRL / SBR in the statistical processes and in that capacity was also involved in the SBR Programme on behalf of the CBS. Gabriëlle has IPMA-B certification and took a master's class in change management. She can be contacted via g.vanmourik@cbs.nl.

Gabriëlle's contribution: review of chapters 2 and 3.

Geert Nederhorst
Geert Nederhorst LLM has been involved in the SBR Programme since January 2013. He actively contributed to the formation of the Chain Information Services department at Logius. Currently, Geert fulfils a dual role at Logius. One the one hand, he heads the solution mangers in the customer (demand) side of the SBR service management triangle (see figure 9.11), meaning that he coordinates service delivery in SBR chains. One the other hand, he leads the implementation of SBR in new domains (SBR expansion). Prior to 2013, Geert was an adviser to the minister and secretary-general at the Ministry of the Interior and Kingdom Relations. Geert can be contacted via geert.nederhorst@logius.nl.

Geert's contribution: general, review of chapters 9 and 10.

Ralf van Oosterhout
Ralf van Oosterhout MSc is an analyst at Thauris. Since 2014, Ralf has contributed to multiple projects in the SBR programme. Ralf can be reached via r.vanoosterhout@thauris.nl

Ralf's contribution: co-author of the revised version of Chapter 3 and the glossary

Jan Pasmooij
Jan Pasmooij RE RA RO has been working for the SBR Programme at Logius since the beginning of 2011 as a Knowledge Development and Sharing Adviser, in which capacity he was directly involved in the communications and information provided for XBRL/SBR, the development on the SBR Online knowledge platform for XBRL/SBR and the SBR Book. Prior to 2011, Jan was actively involved in XBRL/SBR developments in the Netherlands and abroad, as chair of XBRL Nederland /EU and as an employee of NIVRA (now NBA). Since 2011, Jan Pasmooij has been working independently and he can be contacted via jan@pasmooijce.com

Jan's contribution: review of the Preface, chapters 2 and 3 and Appendix A (The background to SBR).

Gertjan Peerenboom
Gertjan Peerenboom is a Strategic Architect at the Tax and Customs Administration Netherlands. He was actively involved in the SBR Programme in 2011. He has principally been involved in the design of the authorisation service and the data submission processes, and connecting them up to the flow of declarations within the Tax and Customs Administration. Gertjan has accumulated a great deal of experience as a business consultant in process architecture and BPM in the public domain. He can be contacted via gj.peereboom@belastingdienst.nl.

Gertjan's contribution: review of Chapter 6.

Erwin Rigter
Erwin Rigter MSc has been involved in SBR since 2012. Erwin co-developed the reporting chain reengineering methodology and has wide experience in the application of the methodology in different reporting fields. In addition, as a process analyst Erwin contributed towards setting up the business line within Logius. Erwin is consultant at Thauris and can be contacted via e.rigter@thauris.nl.

Erwin's contribution: co-author of Chapter 4, lead author of Chapter 10 and review of the entire book.

Marko Roos
Marko Roos works for the methodology department of Statistics Netherlands. He is primarily involved in the development of methods for collecting data digitally. Marko made an active contribution to the initial versions of the Netherlands Taxonomy. Marko can be contacted via m.roos@cbs.nl.

Marko's contribution: review of Chapter 5.

Ian Saturday
Ian Saturday has been involved in SBR since 2013. He is currently architect and program manager for designing and implementing new and modified I-processes and services within the generic infrastructure for payroll tax and pre-filled tax return on behalf of the Tax and Customs Administration. Ian works for Thauris and can be contacted via i.saturday@thauris.nl.

Ian's contribution: co-author of Chapter 7, review of chapters 1, 9 and 10.

John Sloof
John Sloof is a policy adviser for the Chamber of Commerce. He has been involved in the SBR Programme since 2012. John can be contacted via john.sloof@kvk.nl.

John's contribution: review of chapters 2 and 3.

Jacques Urlus
Jacques Urlus RE CISA BBA has worked full-time on XBRL and SBR for 8 years now. He specialises primarily in the user side of XBRL. He is currently advisor ICT & Accountancy at the Netherlands Institute of Chartered Accountants (NBA). Jacques can be contacted via jacques.urlus@nba.nl.

Jacques' contribution: review of Chapter 8, participation in data retention sessions.

Roel Vaessen
Roel Vaessen has been the Market Implementation Manager for the SBR Programme at Logius since the end of 2010. In that capacity, he provides SBR implementation support for market parties such as software suppliers and financial intermediaries. Roel works for Sogeti and he can be contacted via roel.vaessen@sogeti.nl.

Roel's contribution: general.

Haiko van der Voort
Dr. Haiko van der Voort is an assistant professor at the Delft University of Technology. He teaches organisational and decision-making theory to bachelor and masters students as well as to professionals. Haiko conducts research in the area of business/public administration and focuses on decision-making processes regarding supervision, quality management, certification and (self-) regulation. Haiko can be contacted via h.g.vandervoort@tudelft.nl.

Haiko's contribution: co-author of chapters 2 and 3, plus review of Chapter 4. He also participated in the knowledge retention session.

Finally, a special thank-you to **Iris Koetsenruijter**, **Maaike Kaasenbrood, Koen Hoijtink, Han, Frans & Henri {Guillaume}, Eveline Karper, Sjoerd Leferink op Reinink** and **Liselore Bongers** for reviewing the grammar, spelling and checking for inconsistencies. **Annemarie van der Linde** and **Jochem Oosterlee** have contributed to the illustrations. Thank you all!

Literature Overview

A

Ackoff, R. L. (1989). From Data to Wisdom. *Journal of Applied Systems Analysis, 16*, 3-9.

Adams, C., & Lloyd, S. (2002). *Understanding PKI: Concepts, Standards, and Deployment Considerations* (2 ed.): Addison-Wesley Professional.

Agterhorst, J., & Thaens, M. (2000). Veranderkundige aspecten van uitvoeringsketens. Casus uitvoering van de Huursubsidiewet. In H. Duivenboden, van, M. Twist, van, M. Veldhuizen & R. Veld, in 't (Eds.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Algemene Rekenkamer. (2007). *Lessen uit ICT-projecten bij de overheid. Deel A*. Den Haag: Tweede kamer van de Staten Generaal.

Algemene Rekenkamer. (2007). *Lessen uit ICT-projecten bij de overheid - Deel B*. Den Haag: Tweede kamer van de Staten Generaal.

Al-Mashari, M. & Zairi, M. (1999). BPR implementation process: an analysis of key success and failure factors. *Business Process Management Journal,* Vol. 5 No. 1, pp. 87-112.

Andersson, R., Eriksson, H., & Torstensson, H. (2006). Similarities and differences between TQM, six sigma and lean. *The TQM Magazine, 18*(3), 282-296.

Arendsen, R. (2008). *Geen bericht, goed bericht: een onderzoek naar de effecten van de introductie van elektronisch berichtenverkeer met de overheid op de administratieve lasten van bedrijven.* (Doctoral), Amsterdam University Press.

Armistead, C., Pritchard, J.-P., & Machin, S. (1999). Strategic business process management for organizational effectiveness. *Long Range Planning, 32*(1), 96-106.

Arsanjani, A. (2002). Developing and Integrating Enterprise Components and Services. *Communications of the ACM, 45*(10), 31-34.

Ashby, W. R. (1958). Requisite Variety and its implications for the control of complex systems. *Cybernetica (Namur), 1*(2), 83-99.

B

Baldwin, C., & Clark, K. (2000). *Design Rules: The Power of Modularity*. MIT Press: Cambridge, MA.

Ballad, B., Ballad, T., & Banks, E. (2010). *Access Control, Authentication, and Public Key Infrastructure*. Sudbury, MA: Jones & Bartlett Learning.

Bauer, J. M., & Herder, P. M. (2009). Designing Socio-Technical Systems. In A. Meijers, D. M. Gabbay, P. Thagard & J. Woods (Eds.), *Handbook of the Philosophy of Science* (Vol. Volume 9: Philosophy of Technology and Engineering Sciences): Elsevier.

Bekkers, V. (2000). Keteninformatisering en het management van organisatiegrenzen: organisatorische en institutionele implicaties. In H. Duivenboden, van., M. Twist, van., M. Veldhuizen & R. Veld, in 't. (Eds.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Berg, M. (1998). The Politics of Technology: On Bringing Social Theory into Technological Design. *Science, Technology & Human Values, 23*(4), 456-490.
Bergeron, B. (2003). *Essentials of XBRL Financial Reporting in the 21st Century*. New Jersey: John Wiley & Sons.
Berkelaar, T. (2007). Strategieën voor de ontwikkeling van een ICT infrastructuur voor de overheid. In J. Grijpink (Ed.), *Geboeid door ketens*: Platform Keteninformatisering.
Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2010). *Security for Web Services and Service-Oriented Architectures*. Heidelberg: Springer.
Bharosa, N., van der Voort, H., Hulstijn, J., Janssen, M., van Wijk, R., & de Winne, N. (2011). *Impose With Leeway: Combining an Egineering and Learning Approach in the Management of Public-Private Collaboration.* Paper presented at the IFIP EGOV, Delft, The Netherlands.
Bodnik, S. (2013). Top five reasons to use XML. Retrieved 12-8-2014, from http://online-learning.com/blog/top-five-reasons-to-use-xml/
Boehm, B. (2002). Get ready for agile methods, with care. *Computer, 35*(1), 64-69.
Bonaccorsi, A., Carmignani, G., & Zammori, F. (2011). Service Value Stream Management (SVSM): Developing Lean Thinking in the Service Industry. *Journal of Service Science and Management*(4), 428-439.
Bonsón, E., Cortijo, V., & Escobar, T. (2009). Towards the global adoption of XBRL using International Financial Reporting Standards (IFRS) *International Journal of Accounting Information Systems, 10*, 46-60.
Boudreau, K., & Hagiu, A. (2010). Platform Rules: Multi-sided Platforms as Regulators. In A. Gawer (Ed.), *Platforms, Markets en Innovation*. Cheltenham, UK: Edward Elgar Publishing.
Brooks, F. P., Jr. (2006). *The mythical man-month* (Anniversary ed.). Indiana, USA: Addison-Wesly.
Brooks, L. (1997). Structuration Theory and New Technology: Analysing Organisationally Situated Computer-Aided Design (CAD). *Information Systems Journal, 7*, 133-151.
Brookshear, G. (2012). *Computer Science - An overview* (11 ed.). Boston: Addison-Wesley.
Brown, A. E., & Grant, G. G. (2005). Framing the Frameworks: A Review of IT Governance Research. *Communications of the Association for Information Systemsw, 15*, 696-712.
Bruijn, J. A., de. (2011). *Framing*. Amsterdam: Atlas-Contact.
Bruijn, J. A., de, & Herder, P. M. (2009). Systems and Actor Pespectives on Sociotechnical Systems. *IEEE Transactions on Systems, Man and Cybernetics, 39*(5), 981-992.
Bruijn, J. A., de, & Heuvelhof, E. F., ten. (2008). *Management in Networks: On Multi-actor Decision Making*: Taylor & Francis Ltd.
Bruijn, J. A., de, Heuvelhof, E. F., ten, & Veld, R. J., in 't. (2010). *Process Management. Why Project Management Fails in Complex Decision Making Processes* (2 ed.). Dordrecht: Kluwer Academic Publishers.
Buijs, J., Doorn, V. v., & Noordam, P. (2004). *Shared Service Centers: Een kwestie van doen*: Kluwer.
Bürger, G. A. (1929). *Wunderbare Reisen... Freiherrn von Munchausen*. Meersburg Leipzig: Hendel Verlag.

C

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy, 7*(1), 78-81

Cameron, K. S., & Quinn, R. E. (2006). *Diagnosing and changing organizational culture: based on the competing values framework*. San Francisco, CA: Jossey-Bass (Wiley imprint).

Carlston, R. (1996). Syntax and pragmatics. *Keith Brown & Jim Miller: Consise encyclopedia of syntactic theories*, 306-313.

Carr, D., & Johansson, H. (1995). *Best Practices in Re-engineering: What Works & What Doesn't in the Re-engineering Process*. NY: McGraw-Hill.

Carter, S. (2007). *The New Language of Business: SOA & Web 2.0*. Upper Saddle River, NJ: IBM Press.

Chaffy, D. (2004). *E-business en e-commerce: een managementperspectief*. Edinburg, Harlow: Pearson Education.

Chappell, D. (2004). *Enterprise Service Bus*. Sebastopol, CA: O'Reilly Media.

Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. *Computer Standards & Interfaces, 34*, 124-134.

Churchman, C. (1967). Wicked problems. *Management science, 4*(14), 141-142.

Claassens, R. (2007). Semantische interoperabiliteit met behulp van een bedrijfsbrede taxonomie *Via Nova Architectura*.

Clark, C., Cavanaugh, N., Brown, C., & Sambamurthy, V. (1997). Building Change-Readiness Capabilities in the IS Organization: Insights From the Bell Atlantic Experience. *MIS Quarterly, 21*(4), 425-455.

Clegg, C. W. (2000). Sociotechnical principles for system design. *Applied Ergonomics, 31*, 463-477.

Cohen, M. D., March, J. G., & Olsen, J. P. (1972). A Garbage Can Model of Organizational Choice. *Administrative Science Quarterly, 17*(1), 1-25.

Curbera, F., Duftler, M., Khalaf, R., Nagy, W., Mukhi, N., & Weerawarana, S. (2002). Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI *Internet computing, 6*(2), 86 - 93

Cusumano, M. A. (2005). Google: what it is and what it is not. *Communications of the ACM, 48*(2), 15-17.

D

Das, T. K., & Teng, B.-S. (1998). Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances. *The Academy of Management Review, 23*(3), 491–512.

Davenport, T. H. (1993). *Process Innovation: Re-engineering Work through Information Technology*: Harvard Business School Press.

Davenport, T. H., & Short, J. E. (1990). The New Industrial Engineering: Information Technology and Business Process Redesign. *Sloan Management Review, 31*(4), 11-27.

Dervitsiotis, K. N. (1998). The challenge of managing organizational change: Exploring the relationship of re-engineering, developing learning organizations and total quality management. *Total Quality Management, 9*(1), 109-122.

Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654.

Donaldson, L. (2001). *The Contingency theory of organizations*. Thousands Oaks: Sage.

Drejer, A. (2002). *Strategic Management and Core Competencies: Theory and Application*. London.

Duivenboden, H., van, Twist, M., van, & Veldhuizen, M. (2000). Ketenmanagement in de publieke sector: introductie. In H. Duivenboden, van, M. Twist, van, M. Veldhuizen & R. J. Veld, in 't (Eds.), *Ketenmanagement in de publieke sector* (pp. 15-26). Utrecht: Lemma.

Duivenboden, H., van, Veldhuizen, M., & Twist, M., van. (2000). Kantelende ketens: naar publiek ketenmanagement. In H. Duivenboden, van, M. Twist, van, M. Veldhuizen & R. Veld, in 't (Eds.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

E

Earl, M. J. (1994). The New and Old of Business Process Redesign. *Journal of Strategic Information Systems, 3*(1), 5-22.

Eeten, M., van, Bruijn, J. A., de, Voort, H., van der, & Bueren, E., van. (2000). *Koppelen met water*. Delft: Eburon.

Ehrig, M. (2006). *Ontology alignment: bridging the semantic gap* (Vol. 4): Springer.

Erl, T. (2008). *SOA: Principles of Service Design*. Upper Saddle River, NJ: Prentice Hall.

F

Feenstra, R. W. (2011). *Service Composition: A Method for Developing Compositions in a Multi-actor Context*. (PhD), Delft University of Technology, Delft

Feo, J. d., & Bar-El, Z. (2002). Creating strategic change more efficiently with a new design for six sigma process. *Journal of Change Management, 3*(1), 60-80.

Fleck, J., & Howells, J. (2001). Technology, the Technology Complex and the Paradox of Technological Determinism. *Technology Analysis & Strategic Management, 13*(4), 523-531.

Floridi, L. (2011). *Semantic Conceptions of Information* E. N. Zalta (Ed.) Retrieved from http://plato.stanford.edu/archives/spr2011/entries/information-semantic/

G

Galbraith, J. R. (1973). *Designing complex organizations*: Addisson-Wesley Publishing Company.

George, M., Rowlands, D. and Kastle, B. (2003), What is Lean Six Sigma? McGraw-Hill Companies, New York, NY

Goldratt, E. M. (1997). *Critical Chain*. Great Barrington, MA: North River Press.

Goldratt, E. M., & Cox, J. (1984). *The Goal: A Process of Ongoing Improvement*. Great Barrington, MA: North River Press.

Gortmaker, J., Janssen, M., & Wagenaar, R. W. (2004). *The Advantages of Web Service Orchestration in Perspective*. Paper presented at the 6th International Conference of Electronic Commerce, ICEC 2004, Delft, The Netherlands.

Gresov, C. (1989). Exploring Fit and Misfit with Multiple Contingencies. *Administrative Sciences Quarterly, 34*(3), 431-453.

Grijpink, J. (2010). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling*. Den Haag: Boom Lemma uitgevers.

Gruber, T. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition, 5*, 199-220.

Gulati, R., & Singh, H. (1998). The architecture of cooperation: Managing coordination costs and appropriation concerns in strategic alliances. *Administrative Science Quarterly, 43*(4), 781-814.

H

Hagiu, A., & Yoffie, D. B. (2009). What's Your Google Strategy? *Harvard Business Review, 87*(4), 74-81.

Hammer, M., & Champy, J. (1993). *Reengineering the Corporation: A Manifesto for Business Revolution,* : Harper Business

Hansen, J. V., & Hill, N. C. (1989). Control and Audit of Electronic Data Interchange. *MIS Quarterly, 13*(4), 403-414.

Hedeman, B., & Vis van Heemst, G. (2011). *Programmamanagement op basis van MSP* (2 ed.). Zatbommel: Van Haren Publishing.

Heller, J. (1961). *Catch-22*. New York: Simon & Schuster.

Hellsten, U., & Klefsjö, B. (2000). TQM as a management system consisting of values methodologies and tools. *The TQM Magazine, 12*(4), 238-244.

Henderson, J., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organizations. *IBM Systems Journal, 32*(1), 4-16.

Hines, P., Holweg, M., & Rich, N. (2004). Learning to evolve A review of contemporary lean thinking. *International Journal of Operations & Production Management., 24*(10), 994-1011.

Hoffman, C., & Watson, L. (2010). *XBRL for Dummies*. Hoboken, NJ: Wiley Pusblishing Inc.

Hofman, W. (2003). *EDI, webservices & ebXML, interacties in organisatienetwerken*. 's Hertogenbosch: Uitgeverij Tutein Nolthenius.

Hoppe, R. (2010). *The governance of problems. Puzzling, powering, participation*. Bristol: Policy Press.

I

IDABC. (2004). European Interoperability Framework for pan-European eGovernment Services, Interchange of Data between Administrations, Businesses and Citizens. Luxembourg: European Commission, 2004/2094.

J

Janis, I. L. (1972). *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes*. Oxford, England: Houghton Mifflin.

Jans, E. O. (1991). *Grondslagen administratieve organisatie - Deel B: processen en systemen* (19 ed.). Groningen/Houten: Wolters-Noordhoff.

Janssen, M., Gortmaker, J., & Wagenaar, R. W. (2006). Web service orchestration in public administration: Challenges, roles and growth stages. *Information Systems Management, 23*(2), 44-55.

Janssen, M., Veenstra, A. F. v., Groenleer, M., Voort, H. v. d., Bruijn, H. d., & Bastiaansen, C. (2010). Uit het Zicht: Beleidsmaatregelen voor het versnellen van het gebruik van ICT-toepassingen voor administratieve latenverlichting Delft: ACTAL.

Janssen, M. F. W. H. A., & Gortmaker, J. (2005). Orchestreren van ketenprocessen. *Informatie*, 18-22.

Janssen, M. F. W. H. A., & Wagenaar, R. (2004). *An Analysis of a Shared Services Centre in E-government*. Paper presented at the Proceedings of the 37th Hawaii International Conference on System Sciences.

Juran, J. (1992). *Juran on quality by design*. New York: The Free Press.

Juric, M., Mathew, B., & Sarang. (2006). *Business Process Execution Language for Web Services* Birmingham, UK: Packt Publishing.

K

Kauremaa, J., Kärkkäinen, M., & Ala-Risku, T. (2009). Customer initiated interorganizational information systems: The operational impacts and obstacles for small and medium sized suppliers. *International Journal of Production Economics, 119*(2), 228-239.

Kettinger, W. J., Teng, J. T. C., & Guha, S. (1997). Business Process Change: A study of methodologies, techniques, and tools. *MIS Quarterly, 21*(1), 55-79.

Khalaf, R., Keller, A., & Leymann, F. (2006). Business processes for Web Services: Principles and applications. *IBM Systems Journal, 45*(2), 425-446.

Kim, H., Pan, G., & Pan, S. (2007). Managing IT-enabled transformation in the public sector: A case study on e-government in South Korea. *Government Information Quarterly, 24*, 338-352.

Kizza, J. M. (2009). *A Guide to Computer Network Security*. New York: Springer-Verlag.

Kleve, P. (2004). *Juridische iconen in het informatietijdperk*. (Proefschrift), Erasmus Universiteit Rotterdam, Kluwer – Deventer.

Klingenberg, A. M. (2011). *Bestuursrecht, e-mail en internet. Bestuursrechtelijke aspecten voor elektronische overheidscommunicatie.* (Proefschrift), De Rijksuniversiteit Groningen, Groningen.

Kloppmann, M., Koenig, D., Leymann, F., Pfau, G., & Roller, D. (2004). Business process Choreography in WebSphere: Combining the Power of BPEL and J2EE. *IBM Systems Journal, 43*(2), 270-296.

Koffijberg, J. (2005). *Getijden van beleid: omslagpunten in de volkshuisvesting. Over de rol van hiërarchie en netwerken bij grote veranderingen*. (Dissertation), Delft University of Technology.

Kooiman, J. (2003). *Governing as governance*. London: Sage.

Korsten, A. F. A. (1988). *Bestuurskunde als avontuur*. Deventer: Kluwer.

L

Lamb, R., & Kling, R. (2003). Reconceptualizing Users as Social Actors in Information Systems Research. *MIS Quarterly, 27*(2), 197-236.

Laudon, K., & Laudon, J. (2010). *Bedrijfsinformatiesystemen* (11 ed.). Amsterdam: Pearson Education.

Lee, J.-N., Huyn, M., Kwok, R., & Pi, S.-H. (2003). IT outsourcing evolution: past, present, and future. *Communications of the ACM, 46*(5), 84-89.

Lee, M. (2003). *Conceptualizing the New Governance: A New Institution of Social Coordination.* Paper presented at the The Institutional Analysis and Development Mini-Conference, May 3rd and 5th, 2003, Workshop in Political Theory and Policy Analysis, Indiana University, Bloomington, Indiana, USA.

Lee, Y. W., Strong, D., Kahn, B., & Wang, R. (2002). AIMQ: a methodology for information quality assessment. *Information and Management, 40*, 133-146.

Lewin, K. (1951). *Field Theory in Social Science*. New York: Harper & Row.

Linthicum, D. S. (2003). *Next Generation Application Integration: From Simple Information to Web Services*: Addison Wesley.

Logius. (2011). *Programma van Eisen PKIoverheid.*

Longworth, G. (2006). Definitions: Uses and Varieties of. In K. Brown (Ed.), *Encyclopedia of Language & Linguistics (Second Edition)* (pp. 409-412). Oxford: Elsevier.

Looijen, M. (2004). *Beheer van informatiesystemen* (6 ed.). Den Haag: ten Hagen & Stam.

M

Maes, R. (2003). Informatiemanagement in kaart gebracht. *PrimaVera Working Paper Series*.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys (CSUR), 26*(1), 87-119.

Malone, T. W., Yates, J., & Benjamin, R. I. (1987). Electronic Markets and Electronic Hierarchies. *Communications of the ACM, 30*(6), 484-497.

Markus, L., & Bui, Q. (2012). Going Concerns: The Governance of Interorganizational Coordination Hubs. *Journal of Management Information Systems, 28*(4), 163-197.

McComb, D. (2003). *Semantics in Business Systems*: Morgan Kaufmann.

McGilvray, D. (2008). *Executing data quality projects, Ten steps to quality data and trusted information*: Morgan Kaufmann Publishers.

McGovern, J., Sims, O., Jain, A., & Little, M. (2006). *Enterprise service oriented architectures: concepts, challenges, recommendations*. Dordrecht: Springer.

Meijer, S. (2009). *The organisation of transactions; Studying supply networks using gaming simulation*. Wageningen Academic Publishers.

Metselaar, E. E., & Cozijnsen, A. J. (2005). *Van weerstand naar veranderingsbereidheid. Over willen, moeten en kunnen veranderen*. Heemstede: Holland Business Publications.

Mintzberg, H. (1992). *Structure In Fives: Designing Effective Organizations*: Prentice Hall.

Monczka, R. M., Petersen, K. J., Handfield, R. B., & Ragatz, G. L. (1998). Succes Factors in Strategic Supplier Alliances: The Buying Company Perspective. *Decision Sciences, 29*(3), 553–577.

Morgan, T. (2002). *Business Rules and Information Systems: Aligning IT with Business Goals*: Addison Wesley.

N

Nadler, D., & Tushman, M. (1980). A model for diagnosing organizational behavior. *Organizational Dynamics, 9*(2), 35-51.

National Computing Centre. (2005). IT Governance. Developing a successful governance strategy. A Best Practice guide for decision makers in IT. Oxford Road, Manchester: The National Computing Centre.

Newcomer, E., & Lomow, G. (2005). *Understanding SOA with Web services*. NJ: Pearson Education.

Nijsen, A. (2003). *Dansen met de Octopus, Een bestuurskundige visie op informatieverplichtingen van het bedrijfsleven in de sociale rechtsstaat*. Erasmus Universiteit Rotterdam, Uitgeverij Eburon, Delft.

O

O'Neill, P., & Sohal, A. S. (1999). Business Process Reengineering A review of recent literature *Technovation, 19*(9), 571-581

O'Donnell, O., B., R., & Timonen, V. (2003). Transformational aspects of e-Government in Ireland: Issues to be addressed. *Electronic Journal of e-Government, 1*, 23-32.
OECD. (2009). Forum on Tax Administration: Taxpayer services sub-group, Guidance Note on Standard Business Reporting: OECD.
Ohno, T. (1988). *Toyota production system: beyond large-scale production*. New York: Productivity Press.
Oracle. (2014). Programming Weblogic XML. Retrieved 8-12-2014, from http://docs.oracle.com/cd/E13222_01/wls/docs92/xml/intro.html
Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science, 3*(3), 398-427.
Ouksel, A. M., & Sheth, A. (1999). Semantic Interoperability in Global Information Systems. *Special Issue of ACM Sigmod Record, 28*(1), 5-12.

P

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners* (2 ed.). Berlin: Springer.
Papazoglou, M. P., & Georgakopoulos, D. (2003). Service-oriented computing. *Communications of the ACM, 46*(10), 24-25.
Parnas, D. L. (1972). On the Criteria To Be Used in Decomposing Systems into Modules. *Communications of the ACM, 15*(12), 1053-1058.
Pidcock, W. (2002). What are the differences between a vocabulary, a taxonomy, a thesaurus, an ontology, and a meta-model? Retrieved Maart, 2012, from http://infogrid.org/trac/wiki/Reference/PidcockArticle
Piechocki, M., & Felden, C. (2007). *XBRL taxonomy engineering. Definition of XBRL taxonomy development process model.* Paper presented at the Fifteenth European Conference on Information Systems, Technische Universität Bergakademie Freiberg.
Pinsker, R. (2003). XBRL awareness in auditing: a sleeping giant? *Managerial Auditing Journal, 18*(9), 732-736.

Q

Qian, Y., Joshi, J., Tipper, D., & Krishnamurthy, P. (2007). *Information Assurance: Dependability and Security in Networked Systems*: Morgan Kaufmann.
Quinn, R. (1998). *Persoonlijk meesterschap in management; Voorbij rationeel management*. Den Haag: Academic Service.

R

Redman, T. C. (1995). Improve Data Quality for Competitive Advantage. *Sloan Management Review, 36*(2), 99-107.
Reimer, U. (2001). *Tutorial on Organizational Memories for Capturing, Sharing and Utilizing Knowledge*. Paper presented at the International Conference on Enterprise Information Systems, ICEIS 2001, Setubal, Portugal.
Reynolds, G., & Stair, R. (2013). *Fundamentals of Information Systems* (7 ed.): Cengage Learning.
Richards, K. (2007). *Agile Project Management: Running PRINCE2 projects with DSDM*. UK: The Stationery Office.
Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Roebuck, K. (2011). *Public Key Infrastructure: High-Impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*: Emereo Pty Limited.

Rogers, E. M. (2003). *Diffusion Of Innovations* (5 ed.). New York: Free Press.

Royce, W. (1970). *Managing the Development of Large Software Systems.* Paper presented at the IEEE WESCON. Reprinted in Proceedings of the 9th International Conference on Software Engineering (1987).

Rutgers, M. (2011). Het torentje van de overheid. In COAP (Ed.), *Het eigene van de overheid, input voor het debat over de rol van de overheid.*

S

Sambamurthy, V., & Zmud, R. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies *MIS Quarterly, 23*(2), 261-290.

Schekkerman, J. (2000). Ketenintegratie en architecturen. In H. Duivenboden, van, M. Twist, van, M. Veldhuizen & R. Veld, in 't (Eds.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Schellekens, M. H. M. (2004). *Electronic Signatures, Authentication Technology from a Legal Perspective* Den Haag: T.M.C. Asser Press.

Scholl, H. J., & Klischewski, R. (2007). E-Government Integration and Interoperability: Framing the Research Agenda. *International Journal of Public Administration, 30*(8), 889-920.

Simsion, G. C., & Witt, G. C. (2005). *Data Modeling Essentials* (3 ed.): Morgan Kaufmann Publishers.

Stallings, W. (2009). *Business Data Communications*. Upper Saddle River, New Jersey: Prentice Hall.

Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice* (5 ed.). Boston: Pearson Education, Inc.

Swedberg, D., & Douglas, J. (2003). Transformation by Design: An Innovative Approach to Implementation of e-Government. *Electronic Journal of e-Government, 1*(1), 51-56.

T

Teece, D. J. (1998). Capturing value from knowledge assets: the new economy, markets for know-how and intangible assets. *California Management Review, 40*, 55-79.

ten Berge, J. B. J. M., & Michiels, F. C. M. A. (2001). *Besturen door de overheid* (4 ed.). Deventer: W.E.J. Tjeenk Willink.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge; Improving Decisions about Health, Wealth and Hapiness*. New Haven: Yale University Press.

The Royal Academy of Engineering. (2004). The Challenges of Complex IT Projects. London: The Royal Academy of Engineering and The British Computer Society.

Thiadens, T. (2008). *Sturing en organisatie van ICT-voorzieningen* (2 ed.). Zaltbommel: Van Haren Publishing.

Turner, M. (2003). Turning software into a service. *Computer, 36*(10), 38 - 44.

Tuunainen, V. K. (1999). Opportunities of effective integration of EDI for small businesses in the automotive industry. *Information & Management, 34*, 361-375.

Twist, M., van, Edelenbos, J., & Broek, M., van den. (1998). In dilemma's durven denken. *M&O, 5*, 7-23.

U

Uschold, M. (2003). Where Are the Semantics in the Semantic Web? *AI Magazine, 24*(3), 25-36.

Uzzi, B. (1997). Social structure and competition in interfirm networks: The paradox of embededness. *Administrative Science Quarterly, 42*, 35-67.

V

van Oost, E., Alberts, G., van den Ende, J., & Lintsen, H. (1998). *De opkomst van de informatietechnologie in Nederland*. Den Haag: Ten Hagen Stam.

Ven, A., van de, & Walker, G. (1984). The Dynamics of Interorganizational Coordination. *Administrative Science Quarterly, 29*(4), 598-621.

Vidgen, R., Avison, D., Wood, B., & Wood-Harper, T. (2002). *Developing web information systems*. Cornwall, UK: Butterworth-Heinemann.

W

W3C. (2004). Web Services Glossary. from http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211

Wastell, D. G., White, P., & Kawalek, P. (1994). A methodology for business process redesign: experiences and issues. *Journal of Strategic Information Systems, 3*(1), 23-40.

Weerakkody, V., & Dhillon, G. (2008). Moving from E-Government to T-Government: A Study of Process Re-engineering Challenges in a UK Local Authority Perspective. *International Journal of Electronic Government Research, 4*(4), 1-16.

Weerawarana, S., Curbera, F., Leyman, F., Storey, T., & Ferguson, D. (2005). *Web Services Platform Architecture*. Upper Saddle River, NJ: Prentice Hall.

Weill, P. (2004). Don't Just Lead, Govern: How Top-Performing Firms Govern IT. *MIS Quarterly Executive, 3*(1), 1-17.

Weill, P., & Ross, J. W. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review, 46*(2), 26-34.

Weske, M. (2007). *Business Process Management. Concepts, Languages, Architecturees*. Berlin Heidelberg: Springer.

White, S., & Miers, D. (2008). BPMN Modeling and Reference Guide: Understanding and Using BPMN. Lighthouse Point, FL, USA: Future Strategies Inc.

Wit, B., de, Rademakers, M., & Brouwer, M. (2000). Ketenstrategie: van virtuele naar reële ketens. In H. Duivenboden, van, M. Twist, van, M. Veldhuizen & R. Veld, in 't (Eds.), *Ketenmanagement in de publieke sector*. Utrecht: Lemma.

Womack, J., Roos, D., & Jones, D. (1990). *The Machine That Changed the World*. New York, NY: Rawson and Associates.

Womack, J. P., & Jones, D. T. (1996). *Lean Thinking: Banish waste and create wealth in your organization*. New York: Simon & Schuster.

Wortmann, H., & Kremer, D. (2011). Het belang van goed opdrachtgeverschap. *Management Executive*(juli).

WRR. (2006). *Lerende overheid - een pleidooi voor probleemgerichte politiek*. Amsterdam: Amsterdam University Press.

WRR. (2011). *iOverheid*. Amsterdam: Amsterdam University Press.

Z

Zuurmond, A. (1994). *De Infocratie - een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk*. Rotterdam: Erasmus Universiteit.