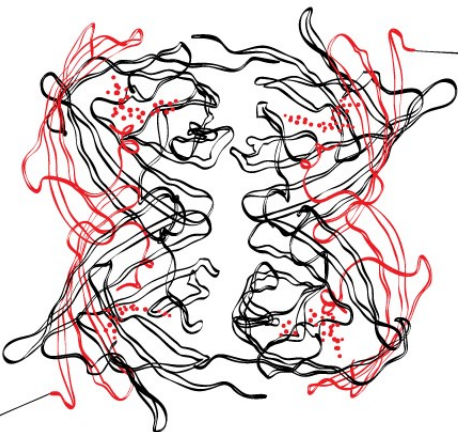
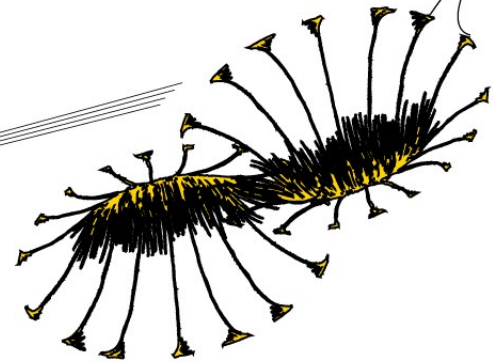




ASSESSING THE IMPACT OF BUSINESS  
PROCESS REDESIGN DECISIONS ON  
INTERNAL CONTROL WITHIN BANKS

A Methodology



UNIVERSITY OF TWENTE.



**Deloitte.**



---

# MASTER THESIS SVEN WIELSTRA

---

## Assessing the Impact of Business Process Redesign Decisions on Internal Control within Banks: A Methodology

Enschede, 16-06-2014

### *Author*

**Sven Wielstra**

Programme MSc Business Information Technology  
Institute University of Twente,  
Faculty of Management and Governance  
Student Number s1008358  
Email [b.a.wielstra@alumnus.utwente.nl](mailto:b.a.wielstra@alumnus.utwente.nl)

### *Graduation Committee*

**Marten van Sinderen**

Department Computer Science  
Email [m.j.vansinderen@utwente.nl](mailto:m.j.vansinderen@utwente.nl)

**UNIVERSITY OF TWENTE.**

**Maria Iacob**

Department Industrial Engineering and Business Information Systems  
Email [m.e.iacob@utwente.nl](mailto:m.e.iacob@utwente.nl)

**UNIVERSITY OF TWENTE.**

**Geert Waardenburg**

Department Deloitte Risk Services B.V.,  
Forensics, Compliance and Analytics  
Email [gewaardenburg@deloitte.nl](mailto:gewaardenburg@deloitte.nl)

**Deloitte.**



“Trust in the LORD with all your heart; do not depend on your own understanding. Seek his will in all you do, and he will show you which path to take.”

Proverbs 3:5-6



# PREFACE

---

This research is the master thesis that concludes my master study 'Business Information Technology' at the University of Twente. Concluding my master study also means the end of my time as a student. During this time I learned a lot, both through the study itself as through other activities within and around the university. Therefore I really enjoyed my time as a student and I hope that I can apply the skills learned within the future, just as I did during this research.

This research was performed in cooperation with Deloitte Risk Services in Amstelveen within the department 'IT Risk'. I also worked together with colleagues from Deloitte Consulting, which provided valuable information. The aim of this research is to provide a methodology that serves as a guideline to assess the impact of business process redesign decisions on internal control within banks.

First, I would like to thank my university supervisors Marten van Sinderen and Maria Iacob for their valuable feedback and support. They provided guidance and helped sharpen my research by sharing their experience and view on it.

Secondly, I would like to thank Deloitte for providing the opportunity to conduct my research. I want to especially thank Geert Waardenburg for being my external supervisor. His experience in practice expressed in the various meetings we had helped me to understand a rather new field of research and therefore he really guided me during the exploration of risk management and internal control. I would also like to thank Ronald van der Wal, Frank de Vocht and Leonne Jongejan for their substantial contribution to my research, both through sharing experience and information. Besides I would like to thank the other colleagues involved in the research.

Finally I would like to thank my girlfriend Daniëlle and my parents Luuk and Jacomijn, who helped and supported me during this research and my years of studying. Their boundless optimism helped me through the difficult stages of this research.

I hope that you will enjoy reading this research and if you have questions, please feel free to contact me.





---

# EXECUTIVE SUMMARY

---

Banks are struggling to successfully implement control requirements into their processes and information systems, while laws and regulations are getting more and more elaborate and require banks to implement controls not only in their processes, but also in the underlying information systems. Financial scandals and the financial crisis led governmental institutions and financial authorities to increase supervision and pose laws and regulations that often tighten requirements for bank processes. Shareholders demand more efficiency and more information, while customers demand better and faster service as well as on-demand high quality information. As a consequence, multiple banks have a mission to increase operation efficiency in order to decrease costs, improve transparency by means of better management information generation and to provide real-time information delivery to customers and other stakeholders in order to improve client servicing. To be able to do this banks are currently redesigning many of their processes and underlying information systems. Automation of controls is a major issue in this transformation, since information systems have a growing part in the processes.

Redesigning bank processes however, has an impact on risks and influences the way in which controls are implemented. It also means that potential areas of risk are shifting. But there is no integrated approach to assess the impact on business process redesign decisions on internal control. The Governance, Risk Management and Compliance research area recognizes the need for a more integrated approach and recommends that business process models should be linked to risks and controls, but little scientific research is done in this area and no concrete guideline for assessing the impact of business process redesign decisions on internal control is developed. Therefore this research focuses on designing a methodology that serves as a guidelines for assessing the impact of business process redesign decisions on internal control. This is done so that a better understanding of business process redesign and the impact on internal control within banks is achieved. Concretely, the following question is answered in this research:

## **How can we assess the impact of business process redesign decisions on internal control within banks?**

A number of concepts play an important role in the design of the methodology, namely: drivers, performance input, process requirements, “as is” situation, process information, “to be” situation, business process redesign/business process management, risk, risk appetite, controls, controls shift and internal control. Using the research model, in which these concepts were linked, a methodology was designed based on five methodology goals.

The most important results of this research are:

- The need for an integrated and structured approach to assess the impact of business process redesign decisions on internal control was identified both through a literature review as through interviewing experts.
- Five methodology goals were formulated. It was argued that a methodology that serves as a guideline based on these goals would serve as the needed approach. The methodology goals were found to be adequate.
- A methodology for assessing the impact of business process redesign decisions on internal control was designed, based on the five methodology goals.
- The methodology was demonstrated using the mortgage provision process of a real world bank and the impact of various business process redesign decisions on internal control was assessed and visualized. The five methodology goals were found to be achieved by experts.
- The methodology serves as an enrichment to the current methodologies used and offered. Therefore the methodology is a valuable addition to the portfolio of Deloitte.
- Through its various steps, the methodology helps constructively working together.
- The methodology serves as a good guideline.
- The methodology is a good starting point for discussion. It offers sufficient basis to develop it further into a concrete approach that can be applied at the clients of Deloitte.



# Table of Contents

<b>Part 1 - Research Introduction</b> .....	<b>1</b>
1 Introduction .....	1
2 Background .....	3
2.1 Business Process Redesign and Internal Control .....	3
2.2 Problem Statement.....	5
3 Research Proposal.....	7
3.1 Theoretical Framework.....	7
3.2 Empirical Framework .....	7
3.3 Scope .....	9
3.4 Research Questions .....	10
3.5 Research Relevance .....	11
3.6 Research Methodology.....	11
3.7 Research Overview .....	13
<b>Part 2 – Information Gathering</b> .....	<b>14</b>
4 Literature Review .....	14
4.1 Literature Review Strategy .....	15
5 Compliance, Internal Control and an Integrated Control Framework .....	16
5.1 Compliance .....	16
5.2 Risk .....	17
5.3 Internal Control .....	19
5.4 Controls and Risk Appetite .....	20
5.5 Control Frameworks .....	24
6 Drivers.....	28
6.1 Financial Authorities .....	28
6.2 Shareholders.....	28
6.3 Customers.....	29
6.4 Competitors .....	29
7 Business Process Redesign.....	30
7.1 Business Process Management and Business Process Redesign .....	30
<b>Part 3 – Design</b> .....	<b>33</b>
8 Research Model .....	33
8.1 Mapping of Literature on Research Model.....	34
9 Formulation of Methodology Goals.....	36
10 Methodology .....	37
10.1 Modeling the “as is” Situation .....	40
10.2 “as is” Situation Risk Analysis .....	44



10.3	“as is” Situation Controls Analysis .....	47
10.4	Process Requirements .....	60
10.5	Modeling the “to be” Situation.....	63
10.6	“to be” Situation Risk Analysis.....	65
10.7	“to be” Situation Controls Analysis.....	66
10.8	Controls Shift Analysis .....	69
11	Demonstration.....	74
11.1	Introduction.....	74
<b>Part 4 – Results and Conclusions.....</b>		<b>75</b>
12	Discussion .....	75
12.1	Research Relevance and Methodology Goals.....	75
12.2	Business Process Redesign.....	76
12.3	Risk Analysis.....	76
12.4	Control Analysis .....	77
12.5	Impact on Internal Control .....	78
12.6	Future Potential .....	79
13	Conclusions .....	80
13.1	Research Questions .....	80
13.2	Limitations and Suggestions for Further Research .....	90
13.3	Contributions.....	91
14	References .....	92
Appendices .....		98
Appendix A. List of Figures .....		98
Appendix B. List of Tables .....		100
Appendix C. Concept Matrix.....		101
Appendix D. Used BPMN Semantics.....		104
Appendix E. Models.....		105
Appendix F. Risks and Controls .....		106
Appendix G. Controls Shift .....		107
Appendix F. Evaluation Interview Overview.....		108

---

# PART 1 - RESEARCH INTRODUCTION

---

In this part an introduction to the research is given, in which the subject of the research is introduced (chapter 1). Chapter 2 provides background information about the subject and in chapter 3 the research proposal is given.

## 1 Introduction

Banks experience an increasing pressure from multiple stakeholders on the way they currently perform. Financial scandals and the financial crisis led governmental institutions and financial authorities to increase supervision and pose laws and regulations (Laeven and Levine, 2009); (Allen et al., 2012), that often tighten requirements for bank processes (Angelini and Clerc, 2011). Shareholders demand more efficiency and more information, while customers demand better and faster service as well as on-demand high quality information. These aspects are drivers for banks to reorganize their processes in order to fulfill the requirements that flow from these drivers. As a consequence, multiple banks have a mission to increase operation efficiency in order to decrease costs, improve transparency by means of better management information generation and to provide real-time information delivery to customers and other stakeholders in order to improve client servicing. Rabobank (2013) for example states that they need to transform their processes in order to make sure that their customer only need to insert the minimal amount of information needed, and therefore make the processes more customer-friendly.

This is why in the past few years, banks decided to redesign their processes in order to meet the requirements flowing from the drivers of stakeholders mentioned above (Küng and Hagen, 2007). This means that parts of existing processes are restructured and new process steps are implemented. Often this goes hand in hand with automation of several process steps. Meanwhile, compliance to applicable laws and regulations is still a must. Aligning controls that stem from laws and regulations with the design of business processes is a major challenge (Sadiq and Governatori, 2009).

Controls that were previously done manually now often will have to be performed in an automated environment. Control automation is therefore becoming increasingly important. The redesign to a more automated process design poses a new challenge to banks and other financial institutions. How do they stay compliant with laws and regulations of multiple stakeholders? What automated controls need to be in place and what control frameworks are usable to analyze these controls for completeness and how can they use these control frameworks together?

To answer these questions, financial institutions ask Deloitte Risk Services to assess if they are in control of their processes. Since IT is playing a prominent role in modern process design, multiple kinds of control frameworks are needed in order to assess the internal control environment as a whole. While frameworks like COSO are used to assess control on a more managerial and strategic level, frameworks like COBIT and ISO 27002 focus more on the underlying information systems and infrastructure.

Control on both aspects is needed in order to be in control of the whole process. Because financial institutions have not enough expertise and insight in the contents and use of the various control frameworks, Deloitte Risk Services is asked to come up with an integrated solution. The reason for this is the fact that simple applying multiple control frameworks and adding up the results is too time expensive. Frameworks tend to have overlapping features and certain aspects of control frameworks are not needed, because laws and regulations only mandate certain aspects to be in control. Therefore a more or less tailor-made solution is needed, which has to be provided by Deloitte Risk Services.

But what exactly will be the impact of various business process redesign decisions on risks and their consecutive controls? What are the risks involved with increased automation? What controls will be needed in order to mitigate these risks? Business process redesign implies a shift in risks and consecutive controls. These questions will shape the integrated control framework, since the shift in risk and therefore control objectives needs to be incorporated in this framework.

This research therefore tries to answer these questions by assessing the impact of different business process redesign decisions on risk and consecutive controls. This will be done by identifying the drivers for business process redesign within banks and analyzing literature regarding compliance, risk, internal control, controls, risk appetite, control frameworks and business process redesign. Based on this research a methodology will be designed that serves as a guideline for identifying the business process redesign decisions banks face, and assessing the impact of these decisions on internal control. This research will therefore provide valuable new insights into business process redesign in relation with risks and controls within banks and it will therefore also provide Deloitte Risks Services with valuable insights on the requirements for the integrated control framework they are developing.

This thesis is structured in four parts. Part 1 gives an overview of the research, including a background and the problem statement. Part 2 includes the literature review. Part 3 is about the justification of the research, the research model and the design of the methodology based on this research model. The design is also evaluated in this part. Part 4 gives the conclusions of this research.

## 2 Background

In this chapter, high-level information is given about the most important topics within this master thesis. This information provides valuable insight into the problem statement that concludes this chapter. It starts with elaborating on the drivers towards business process redesign and Internal Control in section 2.1. In section 2.2 the problem statement is given.

### 2.1 Business Process Redesign and Internal Control

There is an increasing pressure from various stakeholders and market changes on banks and other financial institutions. These various stakeholders are governmental institutions/financial authorities, customers, competitors etc. Financial scandals and the recent financial crisis showed the importance of bank regulation and supervision (Klomp and Haan, 2012) and therefore led financial authorities like DNB and AFM to make new laws and regulations (Demirgüç-Kunt et al., 2008; Demirgüç-Kunt and Detragiache, 2011). For example, scandals in the United States lead to the creation of the Sarbanes-Oxley act (Damianides, 2005). But also other stakeholders like shareholders pose drivers on financial institution's activities. They want more transparency (United States Agency for International Development, 2000) through management information, so that they can make sound decisions based on process information quickly (Earl et al., 1995); (Grover and Jeong, 1995). Customers demand better services and instant access to their data, while the society as a whole demands more transparency in banking processes due to recent financial scandals. Due to globalization margins are shrinking, while digitalization and automation offer incentives for cost reduction and therefore a better competitive position. New computing technologies are recognized as facilitators of fundamental business change (Teng et al., 1998). For example because the transaction volumes of banks are so high that even small improvements through means of information technology may result in substantial cost reductions (Grembergen et al., 2005).

Automation also offers possibilities for management information generation through analytics, better integration of information systems and real-time data to customers. Transformation of processes to meet these drivers is therefore a major topic within the banking world. Banks are therefore more and more engaged in business process redesign (BPR) (Küng and Hagen, 2007). BPR aims to achieve efficiency, transparency and better client servicing through the rethinking and redesign of business processes. Figure 1 gives an overview of the drivers for process redesign within banks.

Banks have become increasingly aware that redesigning processes to meet the drivers of stakeholders (often by means of automation) also means that new risks will occur and controls will have to be restructured in order to mitigate these risks. This not only means that new controls have to be implemented at a process level, but also at an IT system level, since the role of IT in banks is becoming more and more important. Companies like Deloitte recognize that linking process redesign with control activities is one of the major aspects on the agenda of client banks.

*“Given the significance of these directives, and the important role IT has in financial systems, many organizations have proactively enhanced the design, documentation, and consistency of IT controls”. (Fox and Zonneveld, 2003)*

Banks have to stay in control of their processes in order to mitigate risks to an acceptable level. Redesigning the processes by using new technologies and information systems also impacts the way in which controls are implemented. While controls were done manually in the past, redesigning processes to more automated ones will result in controls being done automatically. Banks need assurance that these “new” controls are also sufficient for mitigating risk to an acceptable level. As a result, frameworks like COSO for financial reporting and CobiT for IT governance (Grembergen et al., 2005) have become major topics in the financial world, according to Damianides (2005). These frameworks are applied to assess if the controls in place are sufficient.

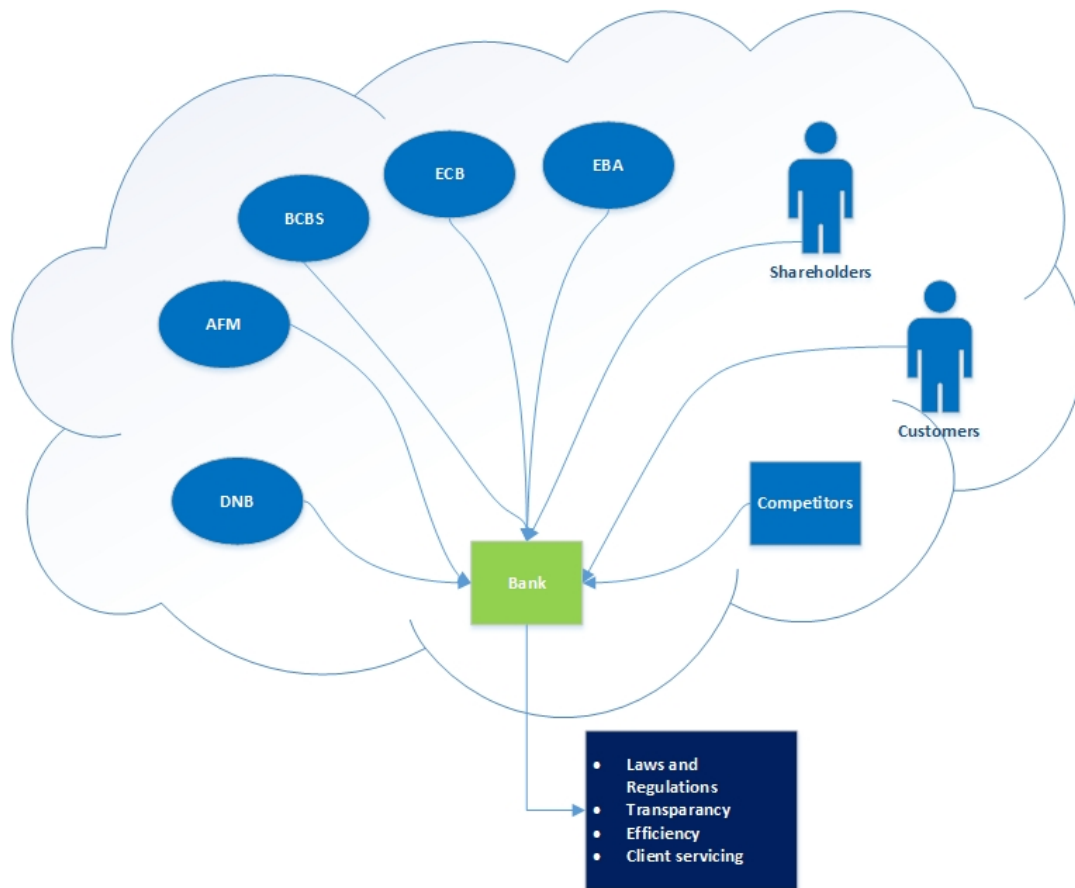


Figure 1. Drivers for Business Process Redesign

Figure 2 illustrates how the controls management (internal control) process interconnects with Business process management. Redesigning business processes by for example using more automated solutions also means that internal control environment has to be changed accordingly. Manual controls will most likely have to be redesigned into automated controls. This is a challenge that banks face in the near future.

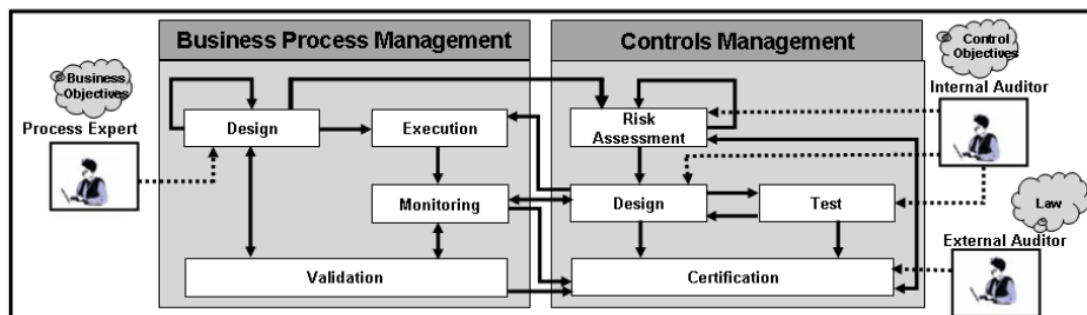


Figure 2. Interconnection of Business Process Management and Controls Management Source: Sadiq and Governatori (2010)

The interest in the topics business process management, compliance, risk and internal control is reflected in Governance, Risk and Compliance (GRC) (Frigo and Anderson, 2009), which is a growing research area. Figure 3 shows the Governance, Risk and Compliance (GRC) model, which shows the interdependence of the three topics. All three topics impact each other and vice versa. Compliance has an impact on both governance and risk management of processes and IT. Also making sure that a proper and well integrated internal control environment is in place, leads to an increased risk management, which in turn has an impact on compliance and governance.

The idea behind GRC is the fact that the three topics described in it are mostly managed and addresses separately within organizations and that efficiency and effectiveness of the three topics can be increased by addressing them in an



integrated approach. Linking process models to risks and consecutive controls is an important aspect in this approach. Some academic research has already been conducted in this area:

- Racz et al. (2010 A) describe that as individual issues, governance, risk management and compliance have always been important topics to organizations, but that the integration of the topics is new. After analyzing 107 sources they state that: *“There is basically no scientific research on GRC as in integrated topic”*. They also say that the information that is provided in current research is limited to a high level. They conclude with encouraging researchers to do more research to the concrete implementation of the topics.
- Sadiq et al. (2007) emphasize that more research is needed in order to link business process modelling with risks and controls. They propose that processes should be modelled in order to link risks and controls to different aspects within the process model. Namiri and Stojanovic (2007) also conduct further research into linking controls to business process by means of business process models. Kharbili and Stein (2008) also link compliance, internal control and business processes in their research towards a compliance management framework, describing that these concepts have direct impact on each other.
- Gericke et al. (2009) try to develop a method that supports the implementation of an integrated GRC solution in which governance, risk management and compliance are linked to each other. This method provides high level steps that should be followed in order to do create strategic awareness about the interrelatedness of the concepts and provides means to implement a GRC strategy. They also state that more research has to be conducted in this area.



Figure 3. The Governance, Risk and Compliance Model Source: Racz et al. (2010)

## 2.2 Problem Statement

Banks are struggling to successfully implement control requirements into their processes and information systems (Barth et al., 2004). Laws and regulations are getting more and more elaborate and require banks to implement controls not only in their processes, but also in the underlying information systems. This trend can be seen in various organizations (Hardy, 2006). Also stakeholders require more transparency within processes by making use of new technologies in order to generate better management information, better service to the customer and efficiency to stay ahead of the competition through cost reduction. The multitude of stakeholders often makes it hard for banks to ensure that they are addressing all drivers for process redesign and the consequent process requirements.

These process requirements have an impact on the way processes are implemented within banks. Currently banks perform much of their controls on processes manually and processes are structured in such a manner that it is often very hard or even impossible to acquire real-time and accurate information. This is also caused by old systems and even legacy systems. These systems cannot meet the requirements made by stakeholders in terms of efficiency, transparency, customer service and internal control.

As a result, banks are currently redesigning many of their processes and underlying information systems. Automation of controls is a major issue in this transformation, since information systems have a growing part in the processes. Controls that were previously done manually can now be performed more efficiently by IT. But banks need to be sure that their renewed internal control environment is still sufficient. There are multiple frameworks developed to categorize controls

into various risk areas in order to assess if there is sufficient internal control. But not all of these frameworks are applicable to specific industries and processes. Also, many of the frameworks have overlapping areas and using them all means that some areas are covered multiple times, which is not efficient. Deloitte Risk Services recognizes that a lot client banks encounter and struggle with this problem. Therefore Deloitte Risk Services tries to develop an integrated approach for auditing clients, by using multiple control frameworks and using parts of them in order to make sure that all areas are covered. Different control frameworks can complement each other (Von Solms, 2005). The next step in this process is the development of an integrated control framework, which consists of multiple general and industry specific frameworks combined. This need for more academic research to this matter as well as practical implications can also be found in the literature:

*“Overall, it can be concluded that intersection between risk management, business process management and compliance is very much in need of more investigation, both academic research (i.e. for the sake of understanding organizational and institutional practice) and practical research to contribute to the development of better solution, guidelines and frameworks for companies.”(Rikhardsson and Best, 2006)*

Redesigning bank processes however, has an impact on risks and influences the way in which controls are implemented. Redesigning bank processes also means that potential areas of risk are shifting. Designing new process steps or changing existing ones means the introduction of new risks, eliminating old risks or a new approach to existing risks. This means that new controls are needed to mitigate these risks. Also, some of the controls that were in the past performed manually are now performed automatically. This has implications on the integrated control framework that has to be developed. This framework has to take in account the shifting risk areas and therefore a shift in controls, in order to assess internal control properly. The need for more research into business process redesign in the financial world, because of its own characteristics, is also expressed in literature:

*“The characteristics of BPR projects in financial institutions differs from those of manufacturing firms because business processes for financial institutions are more information intensive and service oriented.” (Shin and Jellema, 2002)*

The GRC area recognizes the need for a more integrated approach and recommends that business process models should be linked to risks and controls, but little scientific research is done in this area (Racz et al., 2010) and no concrete way for assessing the impact of business process redesign on internal control is developed. Therefore this research focuses on designing a methodology that serves as a guideline for assessing the impact of business process redesign decisions on internal control. This is done so that a better understanding of business process redesign decisions and their impact on internal control within banks is achieved.

## 3 Research Proposal

This chapter describes the research outline, which consists of seven sections. First, an overview of the underlying theoretical framework of this research is given and discussed in section 3.1. Secondly, the empirical framework is given in section 3.2. Thirdly, the scope of the research is given in section 3.3. The main questions and the additional sub questions are given in section 3.4. Then the relevance of the research is discussed (3.5). The research methodology is elaborated in section 3.6 and this chapter ends with the research overview (3.7).

### 3.1 Theoretical Framework

The theoretical framework of this research will be focused around the concepts described in the previous chapter, namely business process management, risk management and compliance. Another important concept within the theoretical model of this research is science research. All these concepts will be further elaborated on in the next sections and in part 2 – Information Gathering, in which a literature review will be done.

### 3.2 Empirical Framework

The empirical framework of this research consist on the background and context described in the previous chapters. This chapters describes the context of the research, as well as the problems banks are struggling with at this very moment. This research will be focused on this empirical framework by applying the theoretical framework described in the previous section.

Based on context research as well as information acquired by having exploratory meetings with experts within the field a conceptual model is created that will serve as a starting point for the research done in part 2 – Information Gathering. This conceptual model is given in figure 4.

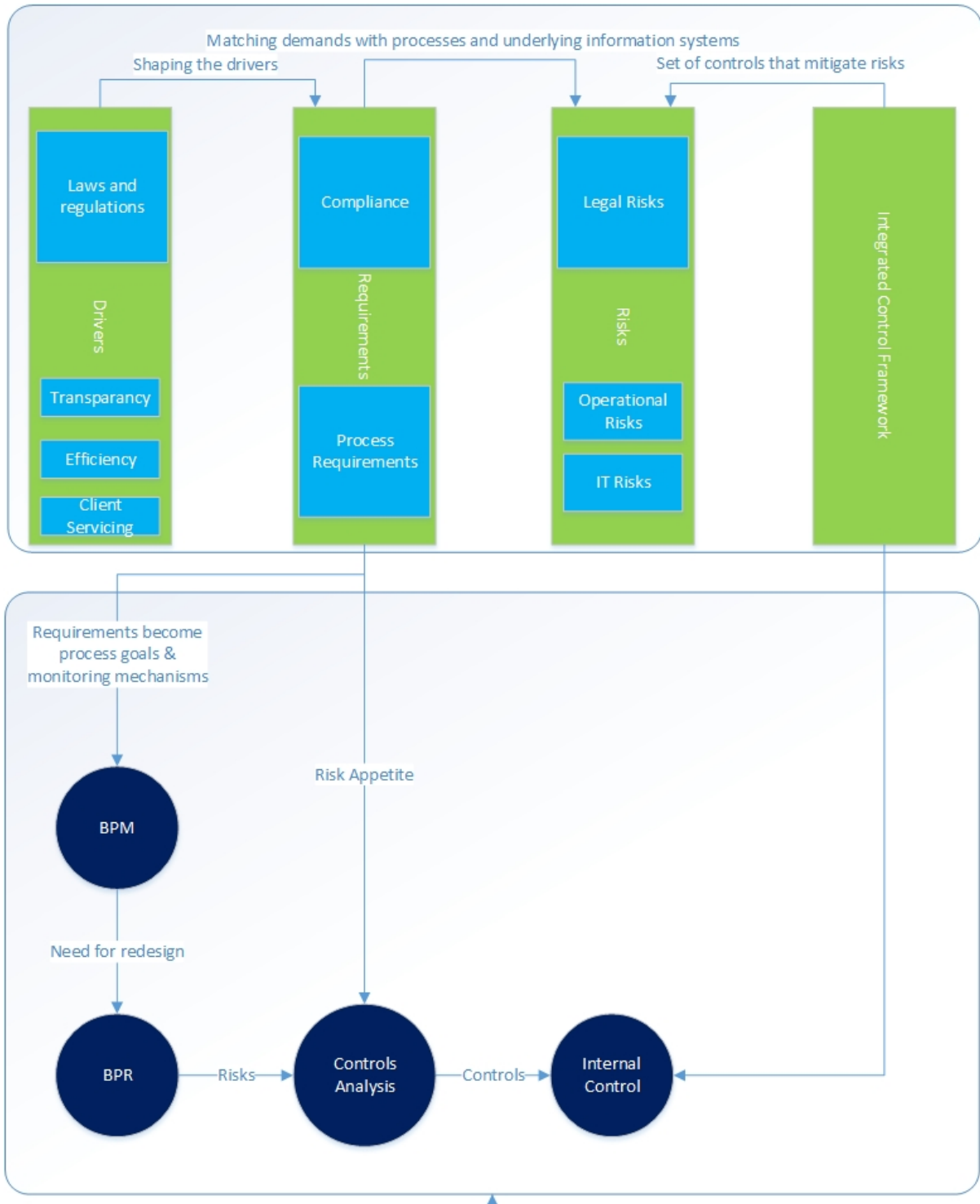


Figure 4. Conceptual Model

### 3.3 Scope

In this section the scoping of this research is given. This scope was agreed on with both the internal and external supervisors. Subsection 3.2.1 describes the different risk categories and in subsection 3.2.2 a number of categories is chosen to scope on. The reason for scoping on these specific categories of risk is given there.

#### 3.3.1 Risk Categories

Figure 5 shows the FIRM risk framework of DNB (De Nederlandsche Bank, 2014), which gives an overview of the different categories of risk. There are two main areas of risk:

- *Financial Risk*: These are risks concerned with economical ratios. Credit risk for example concerns with the credit ratio of a bank.
- *Non-financial Risk*: These are risks not directly concerned with economical ratios. These risks are more about the performance of a bank. The different types of non-financial risk are briefly stated here:
  - *Environmental Risk*: These are risks concerned with the bank status towards the external environment.
  - *Operational Risk*: Risks that flow from the operations process.
  - *Outsourcing Risk*: Risks that flow from outsourcing certain processes or process steps.
  - *IT Risk*: All risks that flow from the usage of IT to support processes.
  - *Integrity Risk*: These risks have to do with the integrity of a bank.
  - *Legal Risk*: These are the risks when looking at compliance to laws and regulations.

#### 3.3.2 Scoping on Categories

Because of limited time and resources a certain scoping is need on categories used within this research. As described in the previous chapters, the main issue faced by banks is the fact that various drivers from stakeholders require banks to redesign their business processes, but they do not know how this will impact risk and the consecutive controls, while they have to make sure that the controls they have in place are sufficient. The main drivers are compliance to laws and regulations in the context of the drivers to increase efficiency, transparency and client servicing, by redesigning processes to make more use of new information systems, technologies and automation.

These drivers will therefore lead to a shift in risks. These risks can be categorized in both areas of risk and therefore the shift in risks impacts both areas of risk. Of course business process redesign has impact on for example the financial risks, because ratios like the credit ratios still have to be enforced in the newly structured processes. And of course compliance to laws and regulations has an impact on Non-financial risks such as Environmental Risk and Integrity Risk, since compliance improves for example the reputation of a bank. Also Outsourcing Risk can be for example influenced by business process redesign, since certain outsourcing steps may change within the process.

But the risk area that is mostly affected by the shift in risks due to the drivers for business process redesign is the Non-financial risk area. Operational Risk as well as IT Risk is greatly affected by a restructuring of the process by making more use of automation and modern technologies and Legal Risk is all about compliance to the laws and regulations in this area. The restructured process still needs to be compliant to various laws and regulations. IT Risk and Operational Risk will be closely related in a process design in which operations are being automated. This is why this research is focusing on these three categories of risk.

Risk Categories	
Financial Risk	Non-Financial Risk
Matching/interest rate risk	Environmental Risk
Market Risk	Operational Risk
Credit Risk	Outsourcing Risk
Insurance Technical Risk	IT Risk
	Integrity Risk
	Legal Risk

Figure 5. FIRM Risk Framework (DNB)

### 3.4 Research Questions

The problem statement as posed in the previous chapter leads to the formulation of the following research question:

**How can we assess the impact of business process redesign decisions on internal control within banks?**

This research question assumes three things:

- Business processes for both the “as is” and the “to be” situation are or can be modeled.
- There is a way to define controls of which the internal control environment consist.
- There has to be a methodology to assess the impact business process redesign decisions on internal control.

In order to answer this main research question, a number of sub questions is formulated. The ordering of these sub questions is based on figure 4. By answering these sub questions, the concepts shown in the theoretical and empirical framework shown above as well as the relation between them will become clear. By analyzing these concepts and the relations between them, a research model to base the methodology to be designed on can be formulated. Also, more expertise in this field of research will be acquired by answering these sub questions, which will help to sharpen the research. The sub questions will be answered in a number of chapters. The sub questions are:

#### Compliance, Risks and Internal Control

1. What is compliance and what is the added value of being compliant?
2. What is risk and how can it be analyzed?
3. What is internal control and how does it contribute to mitigating risks?
4. What are controls and risk appetite and how do these concepts relate to internal control?
5. What are control frameworks and how does an integrated control framework ensure internal control?

#### Business Process Redesign

6. What are the main drivers for banks to redesign their processes?
7. What is business process redesign?
8. What is the relation between business process redesign and risk?

#### Design

9. Can we define a methodology to assess the impact of business process redesign decisions on internal control?
10. What is the impact of various business process redesign decisions on internal control within the mortgage provision process?

### 3.5 Research Relevance

The research is expected to have the following contribution to theory, as well as practice:

1. Extending current theory by identifying the need for more research towards a structured approach for assessing the impact of business process redesign decisions on internal control. This is a contribution to theory.
2. Extending current GRC theory by providing a methodology in which the contents of GRC are specifically linked and operationalized. This is a contribution to theory.
3. Extending current theory by providing valuable insights in how business process redesign impacts risks and consecutive controls within bank. This is a contribution to theory.
4. Also providing Deloitte Risk Services with valuable insights in how business process redesign impacts risks and consecutive controls within banks, and with a methodology as a guideline to assess this impact. This is a contribution to practice.

This research thus has relevance in both theory and practice. Both the literature on control frameworks and their relation to business drivers is extended and Deloitte Risk Services gains more insight in the impact of business process redesign decisions on risks and controls, which enables them to provide a better service to their customers in the future.

### 3.6 Research Methodology

The research is done in several steps. The different steps will be described briefly in this section. Figure 6 gives an overview of the steps. The first step is a literature review, which is needed in order to gain more insight into the concepts described in the conceptual model as well as the linkages between them.

The second step, in synthesis with the literature review, will be gathering information from practice, such as stakeholder information and information about laws and regulations as well as about other drivers. This information cannot be acquired by academic literature only, since for example laws and regulations are domain specific and Deloitte Risk Services itself has a lot of domain specific information about past experiences in the financial world. This specific information cannot (sufficiently) be acquired by analyzing academic literature alone and needs to be gathered from with Deloitte Risk Services as well as other sources. The practice of gathering information has an iterative nature, since exploring new academic knowledge leads to further exploration of the practical impact and vice versa.

The third step consists of formulating methodology goals based on literature, the final research model and expectations of the methodology. The fourth step will be design of the methodology based on these goals and the research model gained through literature study. Notice that the third and fourth steps also have an iterative nature with the first and second step, since additional information from literature may be needed in order to sharpen the methodology goals and the methodology design itself.

The fifth step consist of applying the methodology within a demonstration. During this demonstration the methodology will be applied on a process in a real bank with the goal to demonstrate that the methodology goals can be reached by performing the different steps described within the methodology and that the steps deliver sound results. The sixth step is the evaluation of the demonstration with experts, and finally in the seventh step the conclusions will be written.

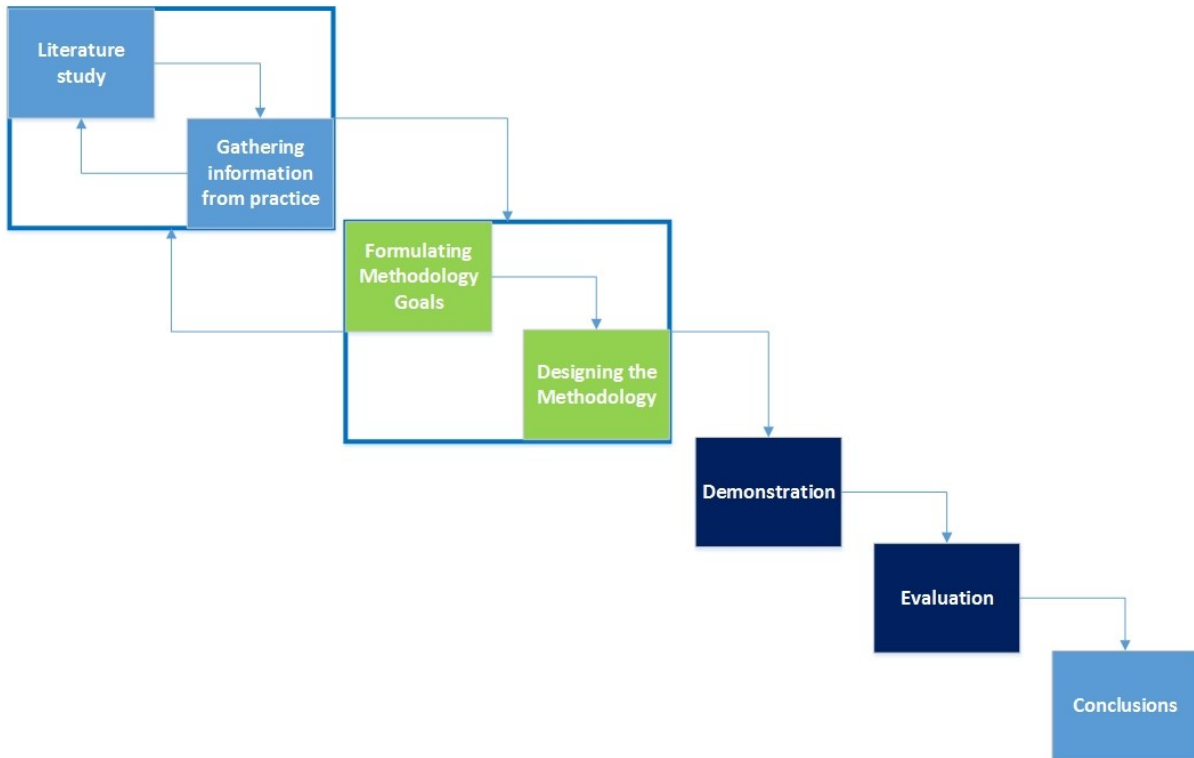


Figure 6. Research Methodology

This approach is based on the research methodology proposed by Peffers et al., (2007). Figure 7 shows this research methodology, which has six steps: Identify problem & motivate, define objectives of a solution, design & development, demonstration, evaluation, and communication. All these aspects will be covered in this research. Table 1 gives a mapping of the six steps of the methodology to steps in this research.

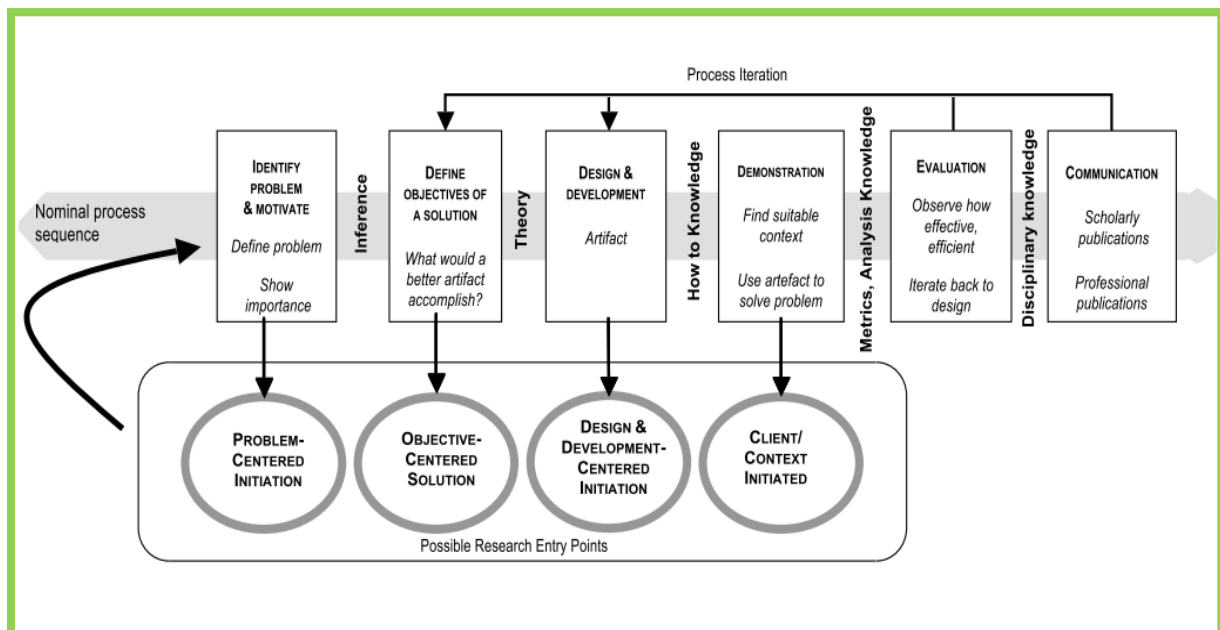


Figure 7. Design Science Research Methodology for Information Systems Source: Peffers et al. (2007)



Table 1. Mapping of DSRM to Research Steps

DSRM	Research steps
Identify problem & motivate	Problem statement and drivers for business process redesign
Define objectives of a solutions	Literature review on compliance, internal control, control frameworks, risk and business process redesign.
Design & development	Setting up goals/ designing the methodology
Demonstration	Demonstration within a real bank with experts.
Evaluation	Evaluation of the methodology with experts.
Communication	Publication of thesis and use within Deloitte.

### 3.7 Research Overview

In order to answer the research question as proposed in section 3.4, a number of sub-questions is formulated. These sub-questions will be answered in different chapters of this thesis. Table 2 gives an overview of the structure of this thesis. It shows in which chapters the sub-questions are answered, by which methodology and what the outcome of the sub-questions is.

This thesis consists of four parts. In this part, part 1 – Research Introduction, the research is introduced. In part 2 – Information Gathering, relevant literature is studied and described. Part 3 – Design is about setting up the methodology based on methodology goals and performing a demonstration. The final part, part 4 – Results and Conclusion, describes the results and conclusions of this research.

Table 2. Research Overview

Research question	Answered in	Methodology	Outcome
<b>Theoretical framework</b>			
What is compliance and what is the added value of being compliant?	Part 2	Literature review	Concept and added value of compliance
What is risk and how can it be analyze?	Part 2	Literature review	Concepts of risk and a way to analyze risk
What is internal controls and how does it contribute to mitigating risks	Part 2	Literature review	Concept of internal control and its contribution to risk mitigation
What are controls and risk appetite and how do these concepts relate to internal control?	Part 2	Literature review	Concepts of controls and risk appetite, their relation with internal control and a way to analyze risk appetite
What are control frameworks and how does an integrated control framework ensure internal control?	Part 2	Literature review	Concept of ICF and its contribution to internal control
<b>Process</b>			
What are the main drivers for banks to redesign their processes?	Part 2	Literature review	Drivers for BPR within banks
What is business process redesign?	Part 2	Literature review	Concept of BPR
What is the relation between business process redesign and risk?	Part 2	Literature review	Relationship between BPR and risk
<b>Design</b>			
Can we define a methodology to assess the impact of business process redesign decisions on internal control?	Part 3, Part 4	Design and evaluation of design	Methodology that serves as a guideline to assess impact
What is the impact of various business process redesign decisions on internal control within the mortgage provisioning process?	Part 3, Part 4	Demonstration and evaluation of demonstration	Impact assessment of various BPR decisions within the demonstration

---

# PART 2 – INFORMATION GATHERING

---

## 4 Literature Review

This chapter gives an overview of how the literature review is conducted. Reviewing literature forms an important part of the information gathering process. It provides further insight into the context and helps explain the theoretical and empirical model as proposed in the previous part. Furthermore literature is used to provide additional insight into the need for business process redesign. Section 4.1 describes the strategy that is used during the literature review in order to find relevant articles and describes how relevant articles are selected.

Figure 8 gives an overview of the literature review steps. First, the concepts of compliance and the added value of compliance will be elaborated on. Secondly, the concept of risk and risk analysis will be further explained. Thirdly, the concept of internal control and its relation to compliance and controls will be discussed. Fourthly, controls and risk appetite will be explained. Fifthly, the concept and use of control frameworks is describes, as well as the concept of the integrated control framework. Finally, business process redesign will be further explained, after the drivers for BPR have been analyzed and described. The findings will serve as input for the research model.

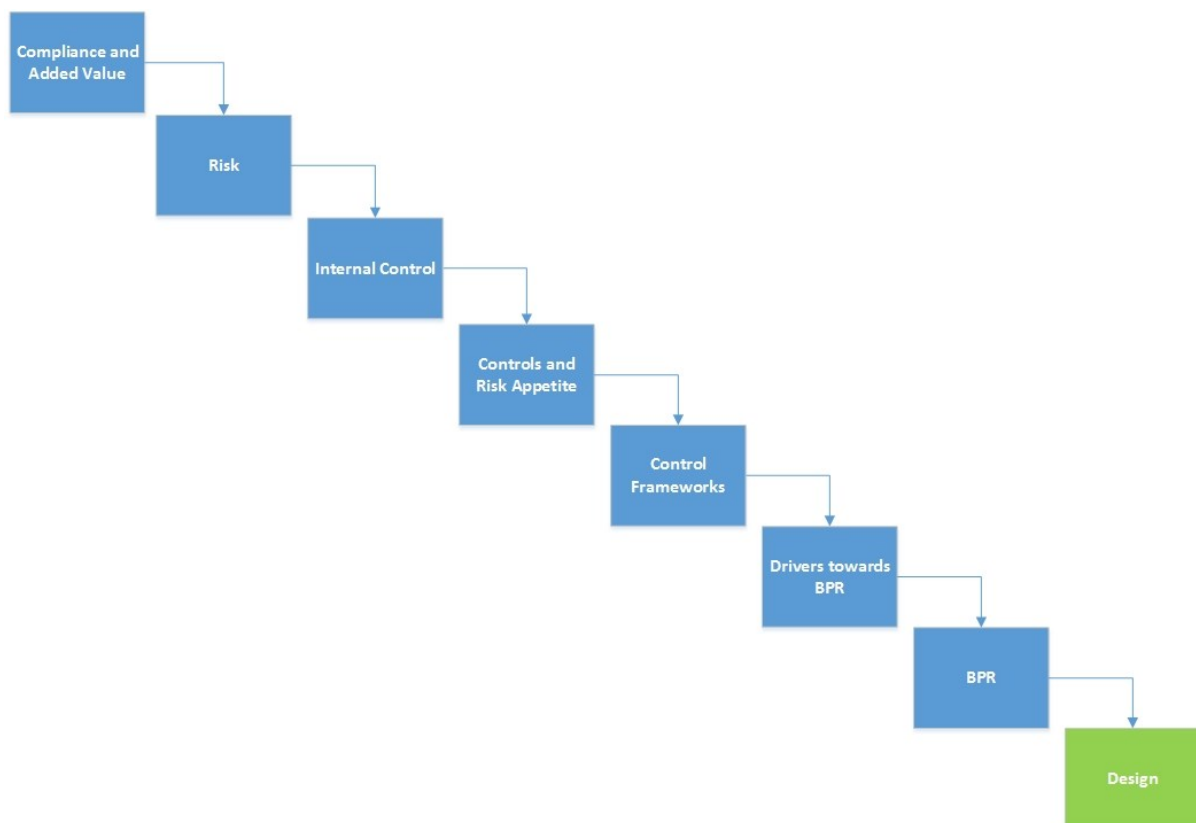


Figure 8. Literature Review Steps

## 4.1 Literature Review Strategy

### 4.1.1 Literature Search

The literature search that has been conducted is done on a semi-structured basis. In order to find relevant papers to answer a number of sub-questions (see table 2), the following search strategy has been used:

- Important keywords are used in the search queries. These keywords were selected by using part 1 – research introduction. The research to the background and context of the problem provided a number of keywords based on concepts related to the topics of this research. Other initial keywords were provided by exploratory meetings with the supervisors. The keywords were used separately as search queries, but also combined in order to find the best articles. While searching for literature new keywords were found, which were often found related to the concepts already used, or being an aspect within the content of the concept further elaborated on in other literature. Using these keywords as well enriched and deepened the literature search and resulted in finding related articles and extending the knowledgebase of our research. Webster and Watson (2002) call this the concept-centric approach.
- Also, a number of authors seemed to be publishing on certain topics more often. Articles were also searched for using the names of these authors as search queries. Webster and Watson (2002) call this the author-centric approach.
- Finally, while reading relevant articles, the references of these articles were checked for relevant literature. Highly relevant articles tend to have a list of references of which the articles are also highly relevant.

The databases used are Google Scholar and Science Direct. Google scholar is very large database and covers most relevant journals and conferences and was therefore chosen for its richness. Science Direct was chosen because of the fact that it is the only accessible database when working at the office of Deloitte Risk Services that can be used to access articles found in Google Scholar. Also Science Direct has a functionality that suggest related articles when an article is selected. This functionality makes it easier to use the concept-centric approach as described above.

### 4.1.2 Selection Criteria

To assess literature for its relevance, a number of criteria was used. These criteria give an indication of the quality of the literature. The criteria used are:

- Sorting on relevance: Google Scholar sorts on relevance. We looked at the first twenty hits to make sure we covered the most relevant literature.
- Scanning the title: By quickly looking at the titles of articles, irrelevant papers are quickly filtered out.
- Looking at the number of citations: The minimal number of citations was set to five, to make sure that possible irrelevant articles did not enter our literature base. We label articles with less citations as “not accepted by the academic world”.
- Year of publication: Because this research is based on developments around compliance, financial scandals and the financial crisis, articles published before 1995 are not used in this research.
- Reading abstracts, introductions and conclusions: By reading these parts of an article, a good impression of the contents of the article is captured.
- Scan articles for author names: If one author happens to be involved in multiple articles around a certain topic, this could indicate that an author is experienced within this research area.
- Another trivial criterion is availability. The University of Twente only has limited access to journals and papers. Some literature may therefore not be available for use.

### 4.1.3 Other literature

Certain literature was also provided by supervisors and colleagues. Literature provided the internal supervisor as well as colleagues is mostly not of an academic nature and will therefore not be found by searching in academic databases. Because of completeness reasons this literature is also included in the literature review. Literature with a more practical nature is a valuable addition to academic literature. Practical information about for example the content of frameworks and banking processes can often be found by searching on Google. This was also stimulated by Deloitte Risk Services

## 5 Compliance, Internal Control and an Integrated Control Framework

### 5.1 Compliance

As described within the previous section, compliance to governmental and institutional regulation is a major topic within the financial world. This development has been triggered by ever evolving processes within financial institutes, that are nowadays being supported more and more by information systems, and by financial scandals and the financial crisis. In this section, the definition and evolution of compliance will be discussed further in detail in order to get a good understanding of the environment financial institutions are working in. This will be done by first looking at the concept of compliance by organizations and then analyzing the added value of being compliant. Besides the fact that being compliant to regulations bring additional costs to financial institutions, like hiring auditors and consultants, redesigning processes to be in line with laws and regulation, communicating to customers in a more transparent way etc., it also brings certain values to organizations. For example, being compliant also contributes to the good name of organizations, making them more attractive to potential investors and customers.

#### 5.1.1 The Concept of Compliance

Sutinen and Kuperan (1999) came up with a model, which is shown in figure 9, which tries to describe all the possible determinants of compliance. Important factors in this model are compliance because of a moral obligation and social influence, possible non-compliance because of illegal gains and compliance because of an expected penalty.

*“Compliance is defined as ensuring that business processes, operations, and practice are in accordance with a prescribed and/or agreed set of norms. Compliance requirements may stem from legislature and regulatory bodies (e.g., Sarbanes-Oxley, Basel II, HIPAA), standards and codes of practice (e.g., SCOR, ISO9000), and also business partner contracts.” (Sadiq and Governatori, 2010)*

Regulatory compliance is the compliance to existing regulations (Damania et al., 2004). This is mainly reflected in the model of Sutinen and Kuperan (1999) in the form of deterrence and enforcement. An institution poses a law or regulation, and when the organization is not compliance to this law or regulation, penalties will follow. Moral obligation and social influence does play a role, but in general this factor is directly subjected to laws and regulations by governing institutions.

Research to compliance within the fishing industry in Denmark showed that compliance tends to work when the penalties of being non-compliant exceed the benefits that can be gained by being non-compliant. If not, fishers are willing to take the risk of receiving a penalty and will not be compliant to laws and regulations (Nielsen and Mathiesen, 2003).

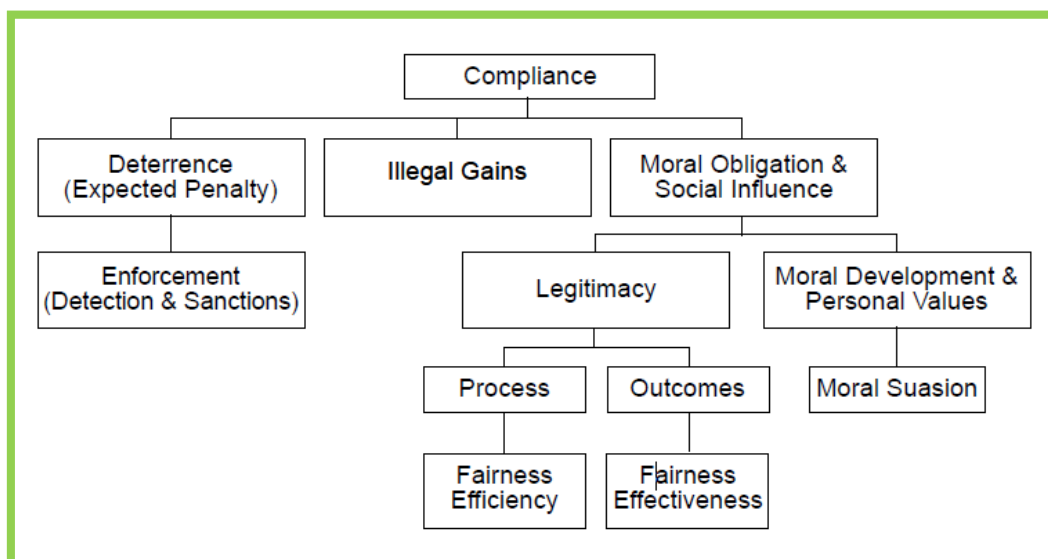


Figure 9. The Determinants of Compliance Source: Sutinen and Kuperan (1999)

### 5.1.2 Added Value of being Compliant

While compliance has been seen as a burden in the past, there are also indications that organizations see the compliance to certain laws and regulations as an opportunity to make their business processes and operation more effective and efficient (Sadiq and Governatori, 2010) and therefore save costs.

This is one of the reasons organizations are looking for new ways to incorporate compliance into their business processes and operations in order to make sure that they stay compliant and also can be compliant to new laws and regulations as soon as they appear. This is called *compliance by design*. It means that organizations start to use frameworks to capture compliance requirements in a generic and standardized way and transform these requirements to control measures in order to make sure their business processes and information systems are aligned to the control objectives that stem from the laws and regulations.

Another reason is the fact that being compliant to regulations ensures that certain risks are analyzed and mitigated. Risk taking is fundamental to business activity (Spira and Page, 2003), but laws and regulations mandated by governing institutions require organizations to look at their business processes in order to determine where the risks are and to mitigate them to an acceptable level. The level of acceptance is determined by the risk appetite of an organization (which will be discussed later) and the maximum amount of risk allowed within the laws and regulations mandated. Reducing risk increases the liability of an organization, which in turn increases the security of potential investors. Risks are managed by a number of accountability mechanisms such as (Spira and Page, 2003):

- Financial reporting
- Internal Control
- Audit

The added value of being compliant is also an incentive for certain organizations strive to be as compliant as possible (Potoski and Prakash, 2005). Compliance can serve as a competitive advantage, since it reflects responsibility and customers and investors are nowadays sensitive to this, because they do not want to be referred to as being irresponsible. This can be seen in need “green initiatives” by organizations, who go a step further than just being compliant to environmental laws and regulations, but also see being green as their main objective (Lubin and Esty, 2010).

Banks are subjected to a laws and regulations of various financial institutions. Compliance to the laws and regulations is therefore a major issue. The cost of being non-compliant is expressed in penalties that banks receive when they are found not compliant. Big amounts of money are connected to these penalties. The fact that a bank does not have to pay these fines, because it is compliant, can also be seen as the added value of being compliant.

## 5.2 Risk

The Project Management Institute defines risk as:

*“an uncertain event or condition that, if it occurs, has a positive or negative effort on a project objective” (Project Management Institute, 2000)*

Risk can be seen as a deviation from how things are expected to go or perform. In the banking world this concretely means that for example a certain process step does not generate the result it is supposed to do or that for example a customer receives a mortgage based on his financial data, while if the data was processed correctly, the customer would never have received a mortgage. Risks can vary in impact. Small deviations in bank account amounts do not have such a big impact as a payment server going down, causing thousands of customers to be unable to do payments.

Lambert et al. (2006) describe that a risk assessment can be done through five steps:

- Risk identification
- Risk measurement
- Risk evaluation
- Risk acceptance and avoidance
- Risk management

The first three steps can be described as risk analysis which will be further elaborated on in this section. The last two steps have to do with the risk appetite, controls and internal control environment of an organization. These concepts will be discussed in the next sections.

Research by Kliem (2000) describes three ways to analyze risks. Quantitative risk analysis, qualitative risk analysis and a combination of both. Quantitative risk analysis uses mathematic calculations while qualitative risk analysis uses judgment as a primary basis to determine the relative importance of one risk to the others and the respective probability of occurrence. To determine the importance of a risk three questions have to be answered (Kaplan, 1997) (Kliem, 2004):

- What can happen?
- How likely is it to happen? (Occurrence)
- If it does happen, what are the consequences? (Impact)

A widely used visualization tool to map this risk importance is the risk matrix, which is also elaborated on in documents of Deloitte (Curtis and Carey, 2012); (Institute of Conflict Management, 2013). It combines the frequency of occurrence on the X-axis with the impact on the Y-axis. Figure 10 gives an impression of a risk matrix. Determining the frequency and the impact is done using one of the three ways for risk analysis. The three blue dots represent three risks. While for example the left one represents a risk with a high impact, the chance of occurrence is very low. By using a visualization tool like this, comparison between and discussion about certain risks is made easier for the people involved.

Qualitative risk analysis is mentioned as a good way to analyze risk by Kliem (2000). This form of risk analysis uses judgment of expert to determine risks. Bass and Robichaux (2001) use a variation on the discussed risk matrix and qualitative risk analysis to determine risks in their research. Remenyi and Heafield (1996) also mention the risk matrix in their research, but they mention an alternative version using structuredness and technical inexperience as axis. Risk analysis benefits greatly from experts involved in the analysis. Solvic et al. (2004) state that almost all risk analysis benefits from experiential guidance. Even risk analyses that are performed in a more prototypical exercise such as proving a mathematical theorem or a move in chess benefit from experiential guidance they say. Experience with risk analysis on processes simply enables experts to target the potential areas of risk, since they are the ones that perform these analysis regularly.

Using experts that know the process well also prevents the fact that people assess bigger risks in areas they do not sufficiently know, because they perceive more uncertainty there (Sjölberg, 2000); (Kunreuther, 2002). Solvic et al. (2004) also state that analysis needs to be more sensitive to the “softer” values that drive people’s concern about risks. These might be important indicators for risks as being identified by people responsible in the process of which the risks are analyzed. These people are the process owners, who feel the impact of the risks and are the ones that should mitigate the risks when needed, which also makes them the risk owners (Coles and Moulton, 2003); (Moulton and Coles, 2003). This vision is supported by Hammer and Stanton (1999), who describe process owners as:

*“Senior managers with end-to-end responsibility for individual processes, process owners are the living embodiment of a company’s commitment to its processes. To succeed, a process owner must have real responsibility for and authority over designing the process, measuring its performance and training the frontline workers who perform it.”*

Drew (2007) states the following about risk analysis, which supports a qualitative risk analysis approach:

*“Typically the level of a risk will be measured by the likelihood of an incident occurring and the financial impact if it does. This is best done by capturing experts’ opinions of loss severities and frequencies (using both internal and external expertise) and discussing with responsible management in each line of business individual loss scenarios and the total losses an enterprise could sustain as a result.”*

Quantitative risk analysis, which focuses more on mathematical calculations, is also posed as a way to determine risks. This is done by for example Kaplan (1997). But because risk is caused by many uncertainties it is hard to frame risk precisely (Muehlen and Ho, 2006). Limited research has been conducted in the area of assessing the risk of BPR efforts, especially on quantitative risk analysis (Crowe et al., 2002). The aim of this thesis is not to conduct more research to this matter. Therefore quantitative risk analysis does not pose a good analysis method for this research.

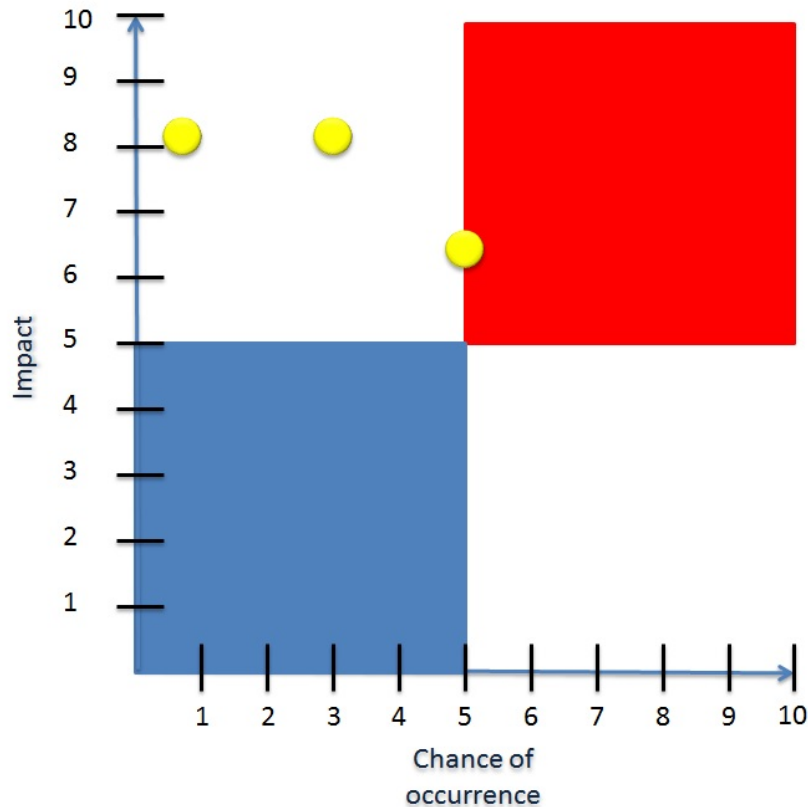


Figure 10. Risk Matrix

### 5.3 Internal Control

Internal control is a system aimed at assessing, minimizing and controlling risk associated with company business processes, business transactions, information technology applications and information dissemination to internal and external decision makers (Neiger et al., 2006); (Rikhardsson and Best, 2006). It is also defined as:

*“a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives”.* (Zhang et al., 2007)

Both definitions are about providing assurance. The focus on internal control has grown quickly in the last years, due to the fact that new laws and regulations require banks to report on their internal control (Hermanson, 2000). The Sarbanes-Oxley Act (SOX) is an example of this. This act mandates internal control (Zhang et al., 2007); (Ashbaugh-Skaife et al., 2008). Assuring that there is enough internal control is done through auditing by external parties (Ashbaugh-Skaife et al., 2007); (Ashbaugh-Skaife et al., 2008).

Because of all the laws and regulations that are posed by different governing institutions, banks need ways to assure that their processes and information systems are conform the requirements mandated by these laws and regulations, which means that the risks within their processes are mitigated to an acceptable level. Breaux et al. (2004) recognize the need for information systems to be compliant to the requirements in highly regulated industries:

*“In highly regulated domains such as healthcare, there is a need for more comprehensive standards that can be used to assure that system requirements conform to regulations.”*

Aligning control objectives that stem from laws and regulations with business processes in order to mitigate risks is a major challenge for organizations (Sadiq and Governatori, 2010) and especially for banks, since they operate in a highly regulated industry. Figure 11 shows this process. Control objectives prescribe that certain risks should be mitigated. This mitigation asks for internal control, which in turn is interrelated with the tasks within business process structure that is in place. Business processes models describe how certain tasks are carried out and how tasks are interrelated. These business processes in turn often need information system support, which also impact internal control the use of information

systems may determine whether controls are being automated or not and internal control also needs to cover the information systems. Internal control can be seen as focused on two aspects (Rikhardsson and Best, 2006):

- Controlling *behavior* such as use and safekeeping of resources and assets so that certain objectives can be reached.
- Controlling *the quality of the information* that for example managers use for decision making or to report to external stakeholders.

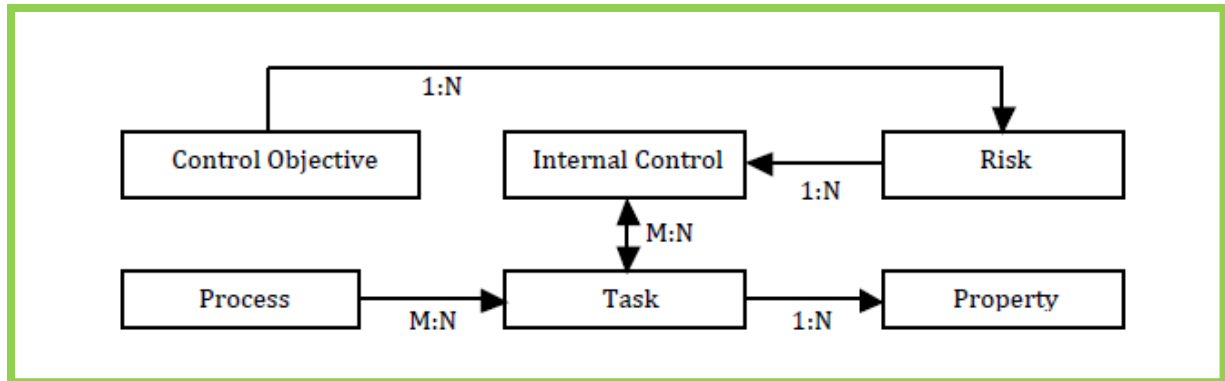


Figure 11. Relationship between Process Modelling and Internal Control Source: Sadiq and Governatori (2010)

Figure 12 shows how a control objective is translated into one or multiple controls, which together with other controls comprises the internal control environment. An objective is translated into specific controls that describe what actions should be taken in order to meet the control objective and therefore mitigate the risks prescribed within the control objective.

Control Objective	Internal Control
Customer due diligence	All new customers must be scanned against provided databases for identity checks.
	Accounts must maintain a positive balance, unless approved by bank manager, or for VIP customers.
Record keeping	Retain history of identity checks performed.

Figure 12. Control Objective and Related Controls Source: Governatori and Sadiq (2009)

## 5.4 Controls and Risk Appetite

The internal control environment is a set of controls (Ge and Mcvay, 2005), stemming from the control objectives. The way these controls are performed (for example manually or automated) therefore impacts the internal control environment. Adequate resources need to be available within the internal control environment in order to make sure that controls function properly (Doyle et al., 2007); (Doyle et al., 2007). This is why it is important to assess the impact of BPR decisions on internal control. By doing this, a bank can sufficiently prepare for a change in the internal control environment. Controls are a product of a company facing certain risks, which it is willing to take or not to take. Risks are identified by control objectives that stem from the laws and regulations.

Figure 13 shows the risk universe, the risk tolerance and the risk appetite. The risk universe contains all the risks within the environment of an organization. The risk tolerance is the amount of risk an organization might just be able to bear. An organization chooses a certain operating area within the environment and the risks within that area become the risks of the organization. Processes also have risk universe, these are all the risks that might be faced within a process. Process also have a specific risk appetite, which has to be established (Deloitte, 2014).



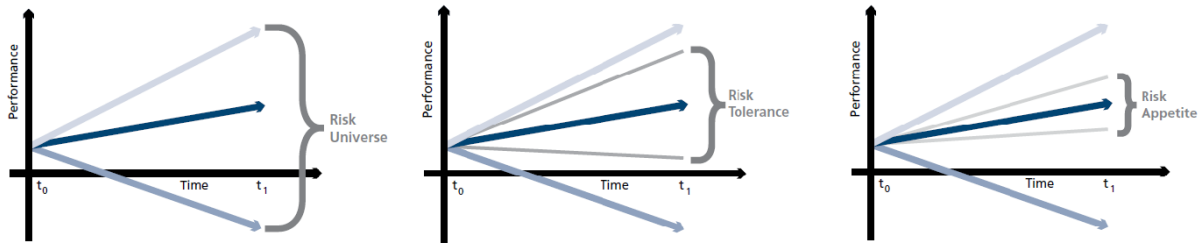


Figure 13. Risk Appetite Source: The Institute of Risk Management (2011)

The risk appetite is the extent in which the organization is willing to take risks (Power, 2009). The risk appetite may shift over time, because of changing uncertainties (Gai and Vause, 2005). It is described in literature as:

*“The amount of risk exposure, or potential adverse impact from an event, that the enterprise is willing to accept or retain. This risk appetite provides a threshold beyond which the enterprise will apply risk treatments and controls to reduce the risk exposure level to within the appetite of the enterprise.” (Drew, 2007)*

The risk appetite depends on a number of factors. Gai and Vause (2005) describe two factors for risk appetite, which are described in figure 14:

- **Risk aversion:** The intrinsic makeup of investors and other people finally responsible. This is unlikely to change markedly, or frequently over time. *“It’s a preference hard-wired into agents’ characteristics”* (Danielsson, 2010). A paper by Dungey et al. (2003) however states that anecdotal evidence suggests that periods of heightened risk aversion often coincide with periods of financial distress. This also shown in research by Adrian et al. (2009).
- **Macroeconomic environment:** Uncertainties within the environment of the organization, such as financial distress. But laws and regulations and other requirements made by stakeholders in the environment may also have implications for risk taking.

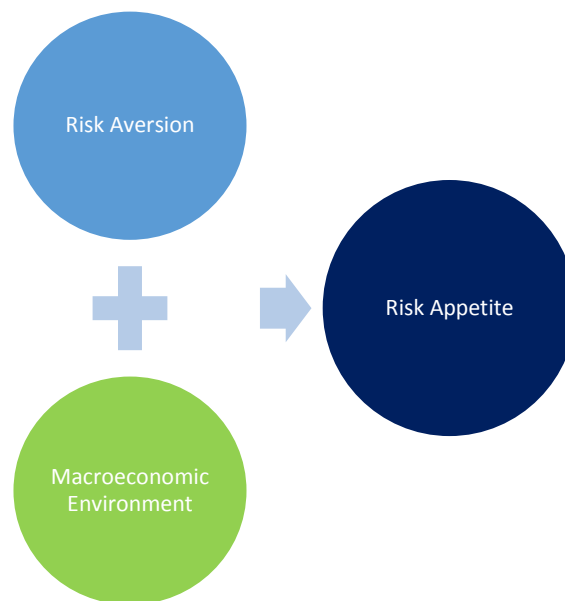


Figure 14. Determinants of Risk Appetite Based on: Gai and Vause (2005)

Although attempts have been made to for example measure Risk aversion (Bekaert et al., 2009), risk appetite analysis is often also done in a qualitative fashion (Kaufmann et al., 2013). Not much empirical literature about risk appetite is available yet (Danielsson, 2010). Since one of the factors, risk aversion, requires deeper insight into the intrinsic makeup of investors and other people involved, it is important to assess this makeup through interaction with them, for example by doing interviews. Risk appetite is not only about capital but also about human behavior (Power, 2009). Because risk aversion is hard to assess or measure, it is important that while doing a risk appetite analysis in a qualitative fashion, the

people responsible are incorporated. By incorporating the people that carry the responsibility for the whole process in the analysis, their aversion is caught.

The amount of risk should be within this risk appetite (Muehlen and Ho, 2006). The risk appetite is normally smaller than the risk tolerance, since organizations always want or have to mitigate a certain amount of risk. Defining the risk appetite for an organization or for certain processes has certain benefits (Drew, 2007):

- It enables making informed business decisions
- It helps focusing on the risks that exceed a defined threshold or appetite for risk
- It strengthens a culture of awareness of risk and openness to report risk
- It helps qualify a range between daring and prudence

The amount of risk a company wants to mitigate can be determined using an equation shown in figure 15. The risk universe consists of risk appetite and the amount of risk to be mitigated. Risk mitigation is done by putting controls in place. Therefore by using this equation, the needed controls can be determined.



Figure 15. Risk Universe Equation

Controls are a way to help a corporation achieve its objectives, such as producing accurate financial reports, despite the presence of threats (Panko, 2006). Controls are put in place as measures to mitigate the risks that are identified and labeled as risks that have to be mitigated, using the equation described above. Having controls in a process helps to identify threats and therefore helps to assure accurate deliverables and mitigate the risks associated to these threats, so that a certain goal can be met. Figure 16 shows how controls fit within a process. It consists of certain process activity and five aspects that are related to that process activity (Lambert et al., 2006):

- *Inputs*: The input for the process activity. Can be an actor, output from another activity etc.
- *Outputs*: The result from the activity.
- *Controls*: Describes a certain constraint on the activity. This is the control measure making sure that the constraint is met and therefore mitigates the risk that the constraint is not met.
- *Mechanism*: Describes how the process activity is completed. This can be for example be done by a human intervention or by means of automation.
- *Sources of risk*: These are the sources of risks that are identified to be involved in a certain process activity.

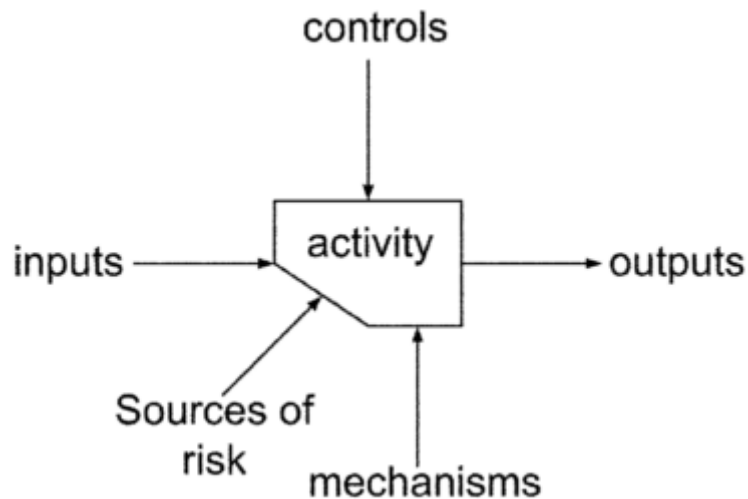


Figure 16. Controls within a Process Source: Lambert et al. (2006)

In practice this means that a bank for example has controls on the process of giving loans. The controls check various data, like the salary of the loan requester in order to assess the ability of the loan requester to pay his loan back in time. Banks need these controls in order to assure financial institutions like AFM and DNB that their process are internally correct and that risks are mitigated sufficiently. Figure 17 shows how controls help to achieve goals by mitigating risk within the process. There are three types of controls according to Bass and Robichaux (2001), Kliem (2000); (2004), Cavusoglu et al. (2004), Kartseva et al. (2004) and Panko (2006):

- *Preventive*: mitigate the impact of a risk or stop it before having impact. Deviations are prevented from occurring.
- *Detective*: Deviations are detected so that action can take place. There are two main approaches in detective controls (Sadiq and Governatori, 2010):
  - *Retrospective reporting*: Risk are detected “after-the-fact” manually.
  - *Automated detection*: Assessment time and correspondingly the time for remediation/mitigation of deficiencies is improved.
- *Corrective*: determine the impact of a risk and establish measures to preclude future impacts. Deviations have occurred and have to be fixed.

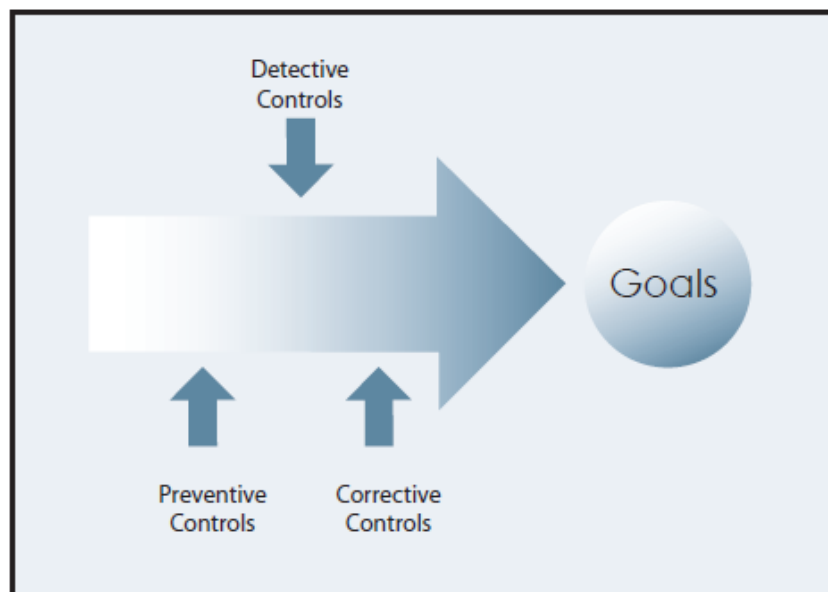


Figure 17. Controls Source: Panko (2006)

## 5.5 Control Frameworks

This section describes the concept of control frameworks, how they help assuring internal control in different areas and how they can be combined into an integrated control framework that helps assuring internal control in multiple areas at the same time by just applying this single integrated control framework. This will be done by illustrating the concept of control frameworks using the most commonly known ones as examples.

### 5.5.1 COSO

COSO is a control framework that is widely used for financial reporting control (Hermanson, 2000); (Rikhardsson and Best, 2006) since the introduction of the Sarbanes-Oxley act, which requires financial institutions to use a control framework to evaluate internal controls. The framework has three categories of objectives (PwC, 2013):

- *Operations Objectives*: These pertain to effectiveness and efficiency of the organization's operations.
- *Reporting Objectives*: These pertain to the reliability of reporting. They include external and internal financial and non-financial reporting.
- *Compliance Objectives*: These pertain to the adherence to laws and regulations to which the organization is subject. This category is especially relevant to this research.

These objectives can be found in the organization as entity-level objectives on a more strategic level and sub-objectives that flow from the strategy-setting process. The entity-level objectives flow down the hierarchy of an organization and are transformed into sub-objectives that relate to the different organizational levels: Divisions, Operating units and Functional activities. For example, sales has different objectives than production and these objectives differ from level to level.

It consists of five components: control environment, risk assessment, control activities, information and communication, and monitoring (Lindow and Race, 2002; Klamm and Watson, 2009).

- *Control environment*: The set of standards, processes and structure that provide the basis for carrying out internal control across the organization. It comprises the integrity and ethical values of the organization and justifies the governance responsibilities. The risk appetite is also determined here.
- *Risk assessment*: This is the practice of identifying and assessing risks that will be encountered while achieving the objectives.
- *Control activities*: These are the actions established through policies and procedures that ensure that the degree of risk mitigation established by the management is carried out.
- *Information and communication*: Information is necessary within the organization to carry out internal control responsibilities. Communication is the continuous process of providing, sharing and obtaining the information that is needed.
- *Monitoring activities*: This is the practice of ongoing evaluations, in order to make sure that all the five components of internal control are present and functioning well. This produces a continuous loop of feedback that is used as input to redesign and improve the functioning of the five components.

It is important to note that this process is an iterative and multidirectional process. The different components influence each other, while information gained within one component serves as input for another component. Figure 18 gives an overview of the components within the framework, as well as the categories and the organizational levels.

In order to assess the presence and functioning of the different components on both entity-level objectives as the sub-objectives, the different components consist of a number of principles. There are seventeen principles in total, which in turn have attributes representing characteristics associated with the principles. Table 3 gives a more detailed overview of the principles per component.

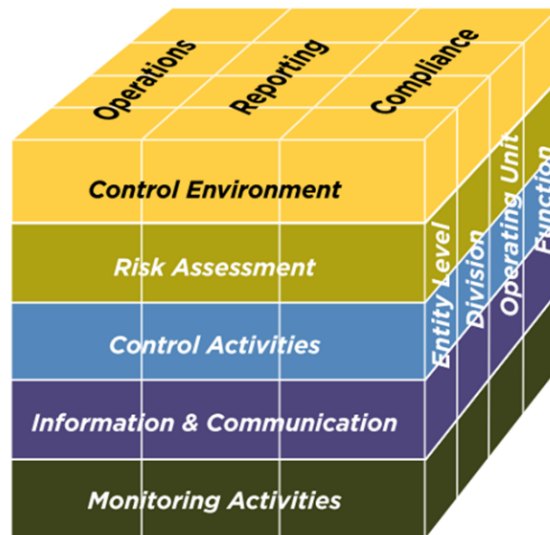


Figure 18. COSO Framework Source: PwC (2013)

Table 3. COSO Principles Source: PwC (2013)

#	Control Environment
1.	The organization demonstrates a commitment to integrity and ethical values.
2.	The board of directors demonstrates independence of management and exercises oversight for the development and performance of internal control.
3.	Management establishes, which board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4.	The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5.	The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	
6.	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7.	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as the basis for determining how the risks should be managed.
8.	The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9.	The organization identifies and assesses the changes that could significantly impact the system of internal control.
Control Activities	
10.	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11.	The organization selects and develops general control activities over technology to support the achievement of objectives.
12.	The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.
Information and Communication	
13.	The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14.	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
15.	The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.
Monitoring Activities	
16.	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17.	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

### 5.5.2 COBIT

Another well-known and frequently used control framework to assure internal control is the CobiT (Control Objectives for Information Related Technology) framework (Tuttle and Vandervelde, 2007), which links risk management practices to business processes as well as to internal control (Pederiva, 2003); (Rikhardsson and Best, 2006). It helps organizations balance their IT risk and investments in control. Because the framework has such a strong control focus, it is widely applied by both external and internal auditors to financial statement audits. The CobiT framework focuses more on what-to-do, instead of how-to-do, so concrete solutions based on the outcome of the framework are still needed.

The CobiT framework consists of a process model that is organized around a system life cycle approach that includes all activities related to IT (Ribeiro and Gomes, 2009), which has four domains (Hardy, 2006):

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Within each domain there is a number of specific processes that an organization should address to achieve detailed and specific IT control objectives. Together there are 34 processes (Pederiva, 2003); (Bouker, 2008) with objectives. All the objectives should then be met in order to assure a high level of control.

All processes within a domain are related to seven information criteria:

1. Effectiveness
2. Efficiency
3. Confidentiality
4. Integrity
5. Availability
6. Compliance
7. Reliability

Every process affects a certain number of the seven information criteria. An auditor can therefore directly assess certain controls for their effect on the quality of information. All the auditor has to do is to map the controls to a certain process to find out what information criteria are influenced by that control.

Table 4 gives an example of the CobiT conceptual model. In the “Deliver and Support” domain there is a certain process “Educate and train users”. This process has a “high” importance and impacts the information criteria “Effectiveness” and “Efficiency”. The process has two control objectives that have to be achieved in order to assure information quality on the two criteria, namely control objective 3.7.1 and 3.7.2. In other words, if both control objectives are found to be met by an auditor, he concludes that process 3.7 is addresses properly and therefore “Effectiveness” and “Efficiency” of information are increased with an importance “high”.

Table 4. CobiT Conceptual Model Example Based on: Tuttle and Vandervelde (2007)

Information criteria	Importance	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
<b>Process</b>								
<b>1 Plan and organize</b>								
1.1 Define a strategic IT plan	H	X	X					
1.2								
<b>2 Acquire and Implement</b>								
2.1 Identify automated solutions	L	X	X					
2.2								
<b>3 Deliver and Support</b>								
3.7. Educate and train users								
3.7.1 IT support training	H	X	X					
3.7.2 Continuity training								
<b>4 Monitor and Evaluate</b>								
1. Monitor and evaluate IT performance	H	X	X	X	X	X	X	X
2.								

### 5.5.3 Integrated Control Framework

As can be seen in the examples, the two control frameworks use a different level of granularity. While COSO focuses more on a more managerial and methodological level, CobiT focuses more concretely on risks and controls within IT. It can be said that CobiT gives some kind of implementation to the COSO framework, while COSO describes the overall methodology. CobiT especially focuses on the risk assessment and the control activities for IT within the COSO framework. Also both control frameworks do describe control objectives, they do not describe concrete controls.

While COSO is very often used within organizations like Deloitte to serve as a structural guide for internal control assessment, CobiT is more or less a control framework that is used to implement some of the steps that are described in COSO. But on its turn, it does not describe how for example decision-making structures should be implemented and controlled (Simonsson and Johnson, 2006). This is how the integrated control framework is built up by Deloitte Risk Services. Different components from various control frameworks are used to build an integrated solution, using the COSO framework as a guidance framework on a higher level.

Efforts to combine multiple frameworks into one, more comprehensive, solution have also been made within the academic world. Sahibudin et al. (2008) tried to combine ITIL, ISO27002 (ISO/IEC, 2005) (other well-known IT control frameworks) with CobiT into a more comprehensive IT Framework. Von Solms (2005) also recognizes that different controls frameworks can be used in a complementary approach and shows this by mapping CobiT and ISO17799 in order to find out if they can complement each other, or one of the control frameworks has to be chosen.

## 6 Drivers

This chapter provides an overview of all the different drivers for business process redesign within banks. The analysis is done using a stakeholder point of view. Different stakeholders are identified and the drivers they generate for banking processes will be discussed. In section 6.1, different financial authorities will be discussed. Because of their power, they play a prominent role in the banking world. Section 6.2 discusses shareholders of banks. Customers (6.3) and competitors (6.4) are also discussed as important drivers for banks to redesign their processes.

### 6.1 Financial Authorities

De Nederlandsche Bank (DNB) is prominent player in the Dutch banking environment. As the central bank authority within the Netherlands, it has a lot of power over the Dutch banks. DNB monitors the Dutch banking environment and serves as a governmental institution that makes laws and regulations based on choices within the Dutch Government. DNB also stimulates progression in the Dutch banking environment, both through laws and regulations as through advice. A report about the tariff structure and infrastructure of the Dutch payment traffic (Werkgroep Tariefstructuren en Infrastructuur in het Betalingsverkeer, 2002) for example evaluates the performance of Dutch banks against banks in other countries and tries to give solutions to increase efficiency.

The Autoriteit Financiële Markten (AFM) is another governmental institution that monitors the Dutch financial market as a whole. It not only monitors banks, but also other financial institutions. AFM also poses laws and regulations on banks.

The European Central Bank (ECB) is the governing authority of all national banks of European members, like DNB. This financial authority monitors the European banking environment and makes laws and regulations based on choices made on a European level.

The Euro Banking Association (EBA) is a group of private banks on a European level working together, making policies, developing best practices etc. (Euro Banking Association, 2007). Since the introduction of the Euro as the universal monetary unit within the European Union, more and more decisions about financial institutions and banks are made on a European level by the ECB, for example SEPA (European Central Bank, 2009). EBA helps member banks implement laws and regulations by providing guidelines and best practices.

The Basel Committee of Banking Supervisors (BCBS) is a committee of banking supervision on an international level. Its members come from countries all over the world. The Basel Committee formulates broad supervisory standards and guidelines and recommends statements of best practice in banking supervision (Bank for International Settlements, & Basel Committee on Banking Supervision, 2006), such as Basel III, which requires banks to revise and restructure their risk management organization by ensuring technical compliance with new rules and ratios (Härle and Lüders, 2010). The committee expects member authorities like DNB and other nations' authorities to take steps to implement these recommendations through their own national systems.

Banks need to show these authorities that they are compliant to all the laws and regulations they pose. This is why banks need more transparency. Transparency enables banks to have better insight into their own processes, but it also enables financial authorities to have a better insight into the banks. By being transparent, banks show that they have nothing to hide and they provide financial authorities with the ability to inspect them thoroughly.

### 6.2 Shareholders

Shareholders play an important role in every organization and therefore also in banks. Eventually they have a personal interest in the bank, since they share in the revenue. Therefore their drivers are closely related to those of the customers. When the customers are happy, revenue will increase and the shareholders will receive their part.

But shareholders demand another aspect: Management Information. Management Information is a term used for information that is needed by management to make sound decisions. Therefore the management needs information about various processes, products and services. Based on this information the management can decide to for example launch a new product, redesign a process or cancel a certain service. Management Information is also closely related to transparency. Processes, products and services become more transparent to shareholders when they receive all the data



needed to base decisions on. New technologies and information systems make the gathering of data and the mining of this data for specific data much easier. Therefore these information systems and technologies have to be incorporated in business processes. This is an important driver from the shareholder and managerial side of banks.

Also efficiency is an important driver for shareholders. Efficiency is expressed in for example cost reduction and faster response times. Reducing costs means that there is more revenue or more money available to support other processes. Cost reduction can also mean that products and services can be offered at a lower price in order to still gain the same revenue. By doing this, a bank becomes more attractive to the customer.

### 6.3 Customers

Due to digitalization and globalization, customers have access to more information about banks and their products and services. Customers have become smarter due to the bulk of information that is available via different channels, for example social media (Constantinides, 2010). And because most of these products and services can nowadays be accessed via the internet or other technologies, switching has become far easier. Therefore customer power has increased (Constantinides, 2013). They for example now have the power to file complaints online on for example forums and other channels. These for a have a very large reach, since everybody with a connection to the internet can access them. Therefore the impact of complaints has grown, since everybody is able to read them and comment on them. One angry customer can lead to a whole flow of angry comments and even protests or legal steps.

This is why banks are increasingly putting effort in customer servicing. Customers for example want their data to be available 24 hours per day and seven days per week (Huang et al., 2006). This data also has to be real-time available, which means that the data has to be correct at that point of time. Therefore transactions and other data needs to be processed continuously. Also connectivity of clients to the services the bank offers needs to be assured. Transparency towards customers is one of the goals of banks (ABN AMRO, 2013). Therefore the whole technical aspect of business processes has become more and more important. Old process structures do not support the flexibility and possibilities to make all these changes happen. Therefore new technologies and innovations have to be incorporated in the business processes.

### 6.4 Competitors

Competitors form an important reason for banks to redesign their business processes. Globalization (Grover and Malhotra, 1997) and digitalization has led banks to not only operate within a certain region or country, but also cross-country and even cross-continental (Zalewska-Kurek, 2013). The network of ABN AMRO for example spans Europe and Asia (ABN AMRO, 2013). This has led to the fact that banks like for example the Royal Bank of Scotland operates in the Dutch market. Besides from the fact that more banks have entered the market, banks are also continuously looking for ways to improve their products and services. Being more efficient is needed in order to stay ahead of the competition. Banks have to be "the best in class". New innovations and technologies enable banks to deliver better products and services and that is why banks need to incorporate these innovations and technologies in their business processes. Efficiency also expresses itself in cost reduction. Banks can perform the same processes more efficient and therefore reduce their operational costs. Lower costs means a better competitive position compared to other banks.

## 7 Business Process Redesign

### 7.1 Business Process Management and Business Process Redesign

Business process redesign (BPR), or business process re-engineering (Larsen and Myers, 1999), is defined as the fundamental rethinking and radical redesign of processes resulting in dramatic performance improvement (Gunasekaran and Nath, 1997); (Al-Mashari and Zairi, 1999); (O'Neill and Sohal, 1999); (Khong and Richardson, 2003). It is about redesigning existing business processes and implementing new ones (Earl et al., 1995) and it requires "out of the box" thinking to explore things outside what has been done before (Grover and Malhotra, 1997). It therefore improves cost efficiency, speed, productivity, competitiveness (Attaran, 2004) and service effectiveness (Abdolvand et al., 2008).

Figure 19 shows the major elements of BPR when using information technology to improve client servicing. Information technology is seen as (one of) the most effective enabling technology for BPR (Grover and Malhotra, 1997); (Gunasekaran and Kobu, 2002); (Teng et al., 2008); (Attaran, 2004). While this case talks about simplification and standardization as major process restructuring aspects, our research focuses more in real-time information accessibility etc., as described in the previous chapters.

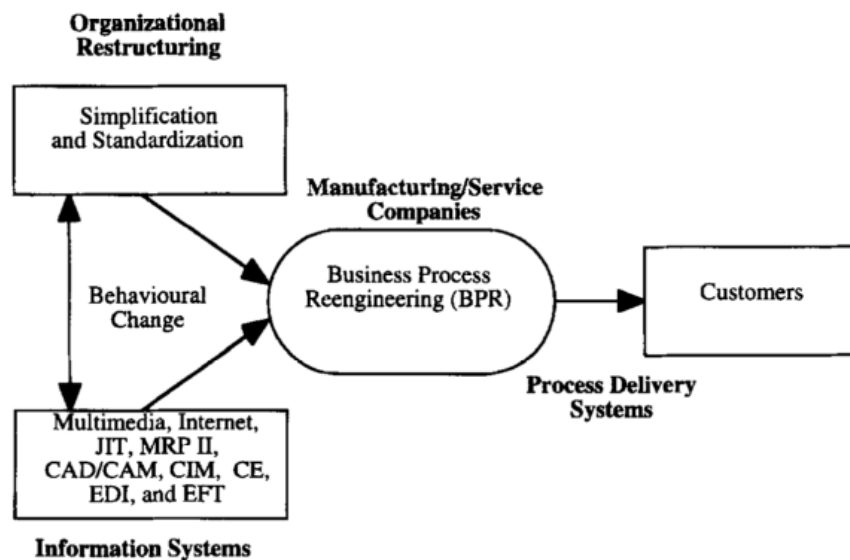


Figure 19. Major BPR Elements when using IT to Improve Client Servicing Source: Gunasekaran and Nath (1997)

BPR is part of a bigger cycle, the Business Process Management (BPM) cycle. Figure 20 shows this cycle. The inner cycle is that of the design, implementation, enactment and evaluation of the process. Goals and process monitoring deliver new input for the process. Aligning controls that stem from regulations with the design of business processes is a big challenge (Sadiq and Governatori, 2009). This research focuses on specific drivers for banks, which serve as goals within this overview. These drivers demand the process to be redesigned. But drivers also serve as process monitoring, since laws and regulations pose certain requirements on the process that have to be monitored.

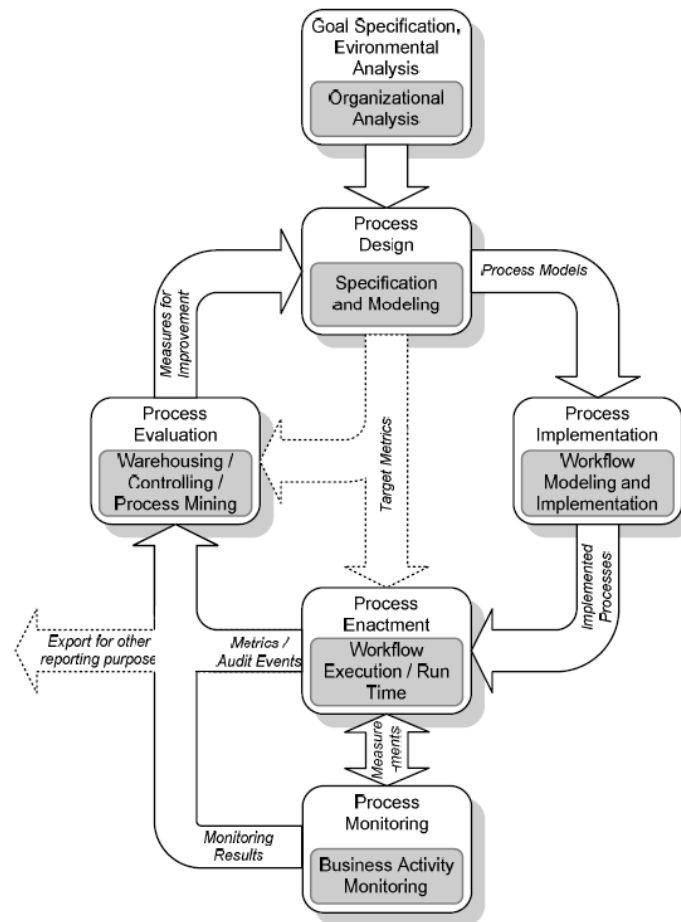


Figure 20. The Business Process Management (BPM) Lifecycle Source: zur Muehlen and Ho (2006)

The research of Khong and Richardson (2003) tells us that while a number of BPR projects fail (Grover and Jeong, 1995), the organizational improvements in cost reduction, better client servicing and increased speed are evident. The idea of BPR is to rethink certain process steps and redesign them in such a manner that they perform better and to make sure that the process as a whole fits better to the stakeholders requirements. An important factor in the process of redesigning processes is the evolution of information technology (Shin and Jemella, 2002). New information technologies enable certain process steps to be done faster and more efficient, or even automatically. Manual steps in the process can now be done automatically by machines and information systems.

Business process redesign consists of four different steps that have to be taken (Shin and Jellema, 2002):

- *Energize*: This step consists of making sure that the whole organization understands why change is needed and to make sure that everybody is committed to the change.
- *Focus*: In this step the current process is analyzed. The as-is situation is analyzed.
- *Invent*: In this step the business process as it should be ("to be" situation) is determined, using the drivers for redesign. Redesign decisions are proposed and evaluated against each other.
- *Launch*: The redesign decisions determined in the previous step are implemented here.

Within the invent step it is important to analyze different design decisions in the context of the requirements (Larsen and Myers, 1999) and to analyze what impact certain redesign decisions will have on risks. Redesigning certain process steps will often result in shifting risks, because risks are coupled to certain process steps. Doing these steps differently or replacing them with new steps, will also mean that risks will change or new risks will occur. Consecutively, the controls to mitigate these risks will also change. New controls will have to be implemented or existing controls will have to be updated.

O'Neill and Sohal (1999) wrote a literature review about BPR, also summarizing a number of techniques that are commonly used in BPR. They state that the focus of a BPR project should be on the outcome and not on the tasks themselves. The required outcome will determine the scope of the BPR process. The techniques they mention in their research are:

- *Process visualization*: Model the end state or vision of the process. It will serve as a goal to work towards.
- *Process mapping/operational method study*: Use tools of operational method studies for reengineering tasks.
- *Change management*: Focus on the human side of reengineering. Managing the change is the largest task.
- *Benchmarking*: Compare your process with processes within other organizations to develop a goal.
- *Process and customer focus*: The primary aim of BPR is to redesign processes with regard to improving performance from the customer perspective.

Combining these techniques results in the fact that it is important to visualize the process as it should look like, while keeping in mind the change needed as well as the client's needs. It is also recommendable to look at other organizations and their processes, because they might provide valuable insights.

Based on these insights it might be concluded that in order to perform BPR it is important to visualize the "to be" situation, in order to determine how to move to this situation with the "as is" situation as a starting point. This is also supported by Lin et al. (2002) who state that visualization through business process modelling serves two important purposes:

- Capture existing processes and structurally representing them
- Represent new processes in order to evaluate them

During the "invention" of the "to be" process, it must therefore be visualized, so that different BPR decisions can be analyzed of their impact on risks. There are multiple techniques to visualize the "to be" situation, of which process modeling (Kueng and Kawalek 1997) is a prominent one. Important other techniques that should be kept in mind are change management, benchmarking and a customer (Motwani et al., 1998) and process focus.

---

# PART 3 – DESIGN

---

## 8 Research Model

After doing the information gathering, a more specific research model was developed. This model is based on the conceptual model given in Part 1 – Introduction, enhanced with the information gained in Part 2 – Information Gathering. It is shown in figure 21.

The model describes the causal relation from drivers to the impact on internal control, by means of a shift in controls. We will briefly elaborate on this causal relation by means of a number of steps:

- Analyzing the drivers results in a number of process requirements that will have to be fulfilled by the process to be designed (the “to be” process). Performance input from the “as is” process also provides input for the analysis of drivers. Certain drivers may stem from performance issues in the current process that need to be improved in the process to be designed.
- Process information from the “as is” situation also serves as input for the “to be” situation. In order to transform the current process to an improved one that is based on the process requirements, information from the old process is needed in order to actually transform this process.
- In both the “as is” and the “to be” process, there is a number of risks. Subsequently the controls to these risks can be determined by means of control frameworks and best practice. Controls can be detective/preventive/corrective and manual/automated according to the literature. The current risk appetite has to be determined in order to assess what risks will actually have to be mitigated by the controls linked to them. For both situations this means that the combination of risks, controls and risk appetite, by using the risk universe equation will result in a number of risks to be mitigated. The controls linked to these risks will be the set of controls selected to achieve the risk mitigation. Risk appetite literature showed that when risk and risk appetite are combined, the risk to be mitigated can be determined by means of an equation.
- Finally, the shift in controls can be determined by following these steps. This is the impact on the internal control environment.

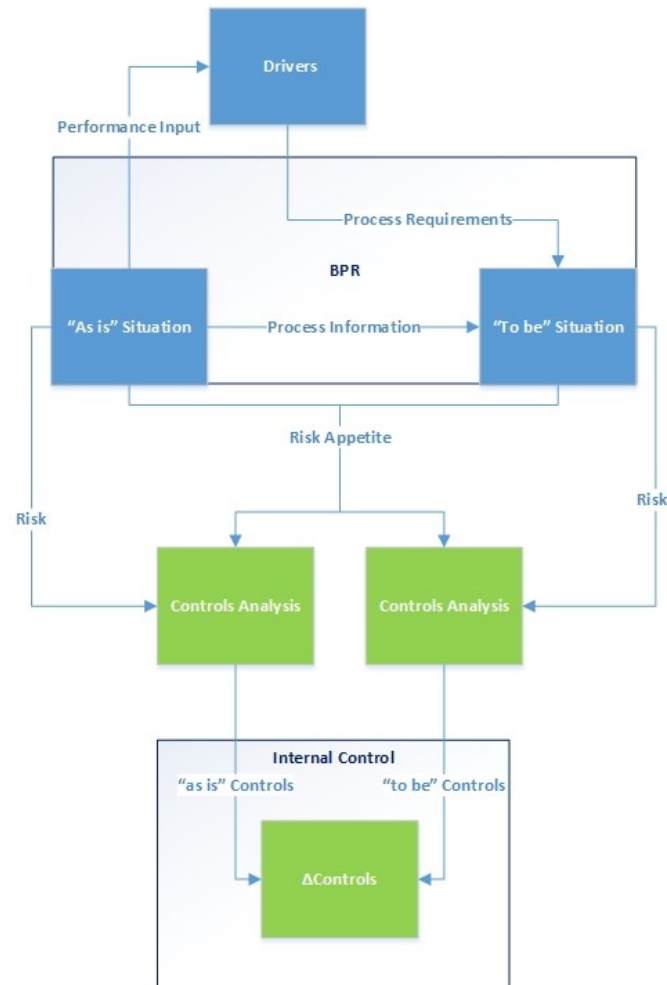


Figure 21. Research Model

## 8.1 Mapping of Literature on Research Model

In order to indicate the importance and added value of this research, as proposed in part 1 – Introduction, a mapping of the read and analyzed literature was done on the concepts forming the research model. The method for doing this is described by Webster and Watson (2002). They propose that a concept matrix should be built, that has the articles on the Y-axis and the concepts discussed within the articles on the X-axis. Then a synthesis of the literature should be made by discussing each identified concept. By comparing the results of this synthesis with the research model described above, some potential research gaps can be found. These research gaps will serve as the justification for this research and the research questions formulated in part 1 – Introduction. The concept matrix build can be found in Appendix C. Concept Matrix.

Identification of the concepts was done by carefully analyzing the articles, by for example looking at the keywords mentioned in the abstract and the list of keywords provided in the article. In order to assess if concepts proposed were indeed discussed on elaborately enough, the contents of the article were analyzed:

- Just mentioning the word “controls” for example, is not enough for the concept “controls” to be mapped to the article within the concept matrix. The contents of the concept have to be discussed.
- Articles not directly mentioning a concept, but discussing relevant aspects within the contents of a concept were also mapped as describing the concept. Hammer and Stanton (1999) do for example describe the concept of “process owners”, which is identified in risk analysis literature as an important aspect in the content of risk analysis. Such literature was used to enrich the knowledge on the concepts within the research model and was found using the concept-centric approach as discussed before.
- Also the articles or papers found in practice are present within the matrix.

Before elaborating on the findings, an important side note has to be made. Some literature is written about the risks involved in performing the BPR itself. Remenyi and Heafield (1996) for example describe the different risks that can occur while performing BPR. These are however not the type of risks we are looking for. We are looking for the risks that stem from various business process redesign decisions, not the risk within the BPR process itself. While we did map the concepts BPR/BPM and Risk/ Risk Analysis for these articles, we are aware that the kind of risk discussed in these articles is not the concept of risk we are looking for. However these articles still provide valuable insight into BPR/ BPM and often into Risk Analysis, since this is a method and it does not depend on what risks are being measured. Based on the concept matrix and, a number of findings can be identified:

- Drivers for business process redesign mentioned in part 1 – Introduction are found abundantly within the studied literature. Many articles however are only limited to mentioning these drivers. Mostly these articles are about developments within the financial world that were used to support the need for business process redesign.
- Compared to the other concepts, relatively much articles are written about the major concepts of BPR/ BPM, Risk/ Risk Analysis, Controls and Internal Control. Mostly this is GRC literature in which the interconnectedness between compliance, governance and risk management is discussed as a trending topic.
- Almost all of the articles that about Controls are also about Internal Control. Most of these articles talk about Internal Control being a set of Controls, or about the impact of Controls on the Internal Controls environment.
- The concepts of BPR/ BPM and Risk/ Risk analysis are also found together often in literature.
- The concepts of Risk/ Risk Analysis and Risk Appetite/ Risk Appetite Analysis are also found together often in literature.
- The concrete aspects of BPR/ BPM are not discussed separately very often. Process requirements are not mentioned and described explicitly, as are the “as is” situation, the process information and the “to be” situation. Some cases delve deeper into the concrete aspects of BPR as identified within the literature, but even when they do aspects are missing. For example, sometimes drivers are transformed into requirements and a “to be” situation is sketched, but the “as is” situation and the process information is not elaborated on. Also, incentives for modeling processes in order to find risks are given within literature, but no concrete modeling case from “as is” to “to be” is given within literature.
- The logical linkage between drivers, the concrete aspects of BPR/BM, BPR/ BPM, Risk, Risk Appetite, Controls and Internal Control described in our research model is never explicitly discussed within the literature. As stated above, different aspects are linked within literature and sometimes references to other concepts within the research model are made, but no article links all the different concepts together explicitly by means of a methodology etc. Twenty articles elaborately discussed four or more concepts. Actually, no real case studies towards the impact of business process redesign decisions on internal control are performed within the literature. Although these impact assessments are made more or less within consulting firms like Deloitte, no methodology for it has been described in literature.
- ΔControls/ Controls Shift Analysis is not elaborated on within the literature. As can be seen, literature does describe the concepts of Risk, Risk Appetite and Controls. Some of these articles also state that the concrete impact of these concepts may change over time, since for example risks may change, but they do not clearly state how different points in time should be mapped against each other in order to find a certain shift in controls. A reason for this may be the fact that, as described in the previous bullet, all prominent concepts within the research model are never linked all together explicitly. Also the concept of Risk Analysis is discussed in literature in a broader context than the context of this paper. The literature provides valuable insight into Risk Analysis, but it gives not direct application on the context of this research.

As can be seen within the analysis, more research towards a comprehensive and complete methodology is needed in order to assess the impact of business process redesign decisions on internal control as posed within part 1 – Introduction. This methodology has to make the explicit linkage between the concepts clear and has to give means to perform the Controls Shift Analysis in or to assess the different in Controls between different situations. It has to describe the implementation of the various steps within this process in order to provide the users of the methodology with concrete handles to perform the impact analysis.

## 9 Formulation of Methodology Goals

As the primary contribution of this research we argue that we can combine the various concepts discussed within the literature research and described within the research model into a sound methodology that serves as a guideline for assessing the impact of business process redesign decisions on internal control. This statement can be split into multiple goals, each describing one or more linkages within the research model:

**G1: Determining the “to be” situation by modelling the process through combining the “as is” process model with the information from the requirements analysis.**

We argue that combining the process model of the “as is” situation with information about process requirements of the “to be” situation will result in a process model for (a possible) “to be” situation.

**G2: Identifying risks for both situations by performing a qualitative risks analysis, in which the process models serve as an input.**

We argue that the process models that will be created can serve as an input for a qualitative risk analysis. The process models serve as process map that displays the process and therefore it can be used as a tool for experts to identify risks within the process.

**G3: Linking controls to the risks by using control frameworks as well as other best practice information and assessing the cost of these controls by means of a qualitative approach.**

We argue that we can use the controls frameworks described in the literature as well as other best practice information to find controls that mitigate the risks that are identified. We also argue that by means of a qualitative approach, in which experts are used, the cost of these controls can be assessed.

**G4: Determining a selection of controls to be implemented by combining the risks with their identified controls, the cost of these controls and the risk appetite, using a qualitative approach.**

We argue that if the concepts described within this goal are combined within the qualitative approach in which experts are used, a selection of controls can be made out of all the controls identified. This selection of controls will be the controls used.

**G5: Assessing and visualizing the impact on internal control by representing the controls of both the “as is” and the “to be” situation into one overview by using their cost and type.**

We argue that if the controls used in both situations are mapped against each other and are described by means of their cost and type within on structured overview, this overview will visualize the controls shift and therefore the impact on internal control.

We argue that a methodology that serves as a guideline based on these goals serves as an answer our main question:

**How can we assess the impact of business process redesign decisions on internal control within banks?**

The design of this methodology and validation of the goals and methodology, based on a demonstration and evaluation interviews, will provide more insight into the fact if this is indeed the case.



## 10 Methodology

The methodology described within the conceptual model will be further elaborated on within this chapter. This methodology will serve as a guideline for assessing the impact of business process redesign decisions on internal control through means of different sequential steps. This chapter will be used to further elaborate on each step within the methodology.

Each step consist of one or multiple tasks. Within each task, various methods, tools and techniques will be used in order to produce the result that is required. These methods, tools and techniques are based on literature, but also on best practice activities within Deloitte. Experts within Deloitte Risk Services were asked for best practice information in order to provide methods, tools and techniques for certain activities.

As stated before in part 2 - Information Gathering, activities like risk analysis and risk appetite analysis are most often done using qualitative methods. One important part of risk management is the fact that the field is highly dependent on qualitative methods such as brainstorm session since experience is very important. Therefore techniques like experts sessions as a qualitative research technique will be commonly used within the methodology proposed in this research.

We also found out that while doing qualitative research within the field through for example expert sessions, it is important to incorporate the owners of processes and risks (Coles and Moulton, 2003); (Moulton and Coles, 2003) within the research. These people are the ones who face the process and the risks every day and they are the ones who are responsible for the fact that process function properly and risks are mitigated adequately. They are the ones that have direct influence over the way a process is structured or how a process is functioning. They are not to be mistaken with the people who perform certain aspects of the process. A call center employee for example may encounter the consequences of a risk, but is not responsible for the fact that the telephone system is hampering.

The personal experience of process owners with certain processes and risks is a very valuable addition to the experience acquired by incorporating external experts from Deloitte Risk Services. Although these people have another kind of expertise, namely the fact that they work within different setting and for different clients, through which they gain knowledge from multiple points of view, they are in the end not responsible for the processes, making them look differently to certain risks.

It is also important to note that while this methodology links business process redesign with risk management by providing means to assess the impact of redesign decisions on internal control, the methodology is executed parallel to the BPR process itself. Deloitte Risk Services does not execute the BPR process, but is asked to assess the risks and the impact on internal control that come with such a project. Therefore multiple steps within the methodology can contribute from information that is already available from the BPR project team. However these steps are still described within the methodology, because they provide the basis for risk assessment.

Another reason is the fact that this methodology requires business process models and process requirements to be of a prescribed granularity, while process models already developed and process requirements already determined in the BPR project often do not provide this granularity. The key here is to make sure that the information gathered is translated into information with this right granularity.

We will now elaborate further on the different steps within the methodology. The structure used to describe this methodology, its steps and the tasks within each step is based on a thesis written by Schepers (2007). An overview of the different steps within the methodology is given in figure 22. The methodology has eight steps:

1. *Modelling the "as is" Situation*: Creating a process model overview of the current situation.
2. *"as is" Situation Risk Analysis*: Identifying the scoped risks within the process.
3. *"as is" Situation Controls Analysis*: Categorizing the risks and determining what controls are needed based on the risk appetite determined.
4. *Process Requirements*: Transforming stakeholder drivers into process requirements for the "to be" situation.
5. *Modelling the "to be" Situation*: Creating a process model overview for a possible future situation.
6. *"to be" Situation Risk Analysis*: Identifying the scoped risks within the future process.

7. *“to be” Situation Controls Analysis*: Categorizing the risks and determining what controls will be needed based on the risk appetite determined
8. *Controls Shift Analysis*: Determining and visualizing the shift in controls between the “as is” and “to be” situation.

The notation used is the Business Process Modeling and Notation (Object Management Group, 2014), a widely used process modelling notation, of which the semantics can be found in Appendix D. Used BPMN Semantics. It clearly describes the different tasks within the different steps of the methodology and also shows clearly what output is generated by certain tasks and what input is needed for certain tasks.

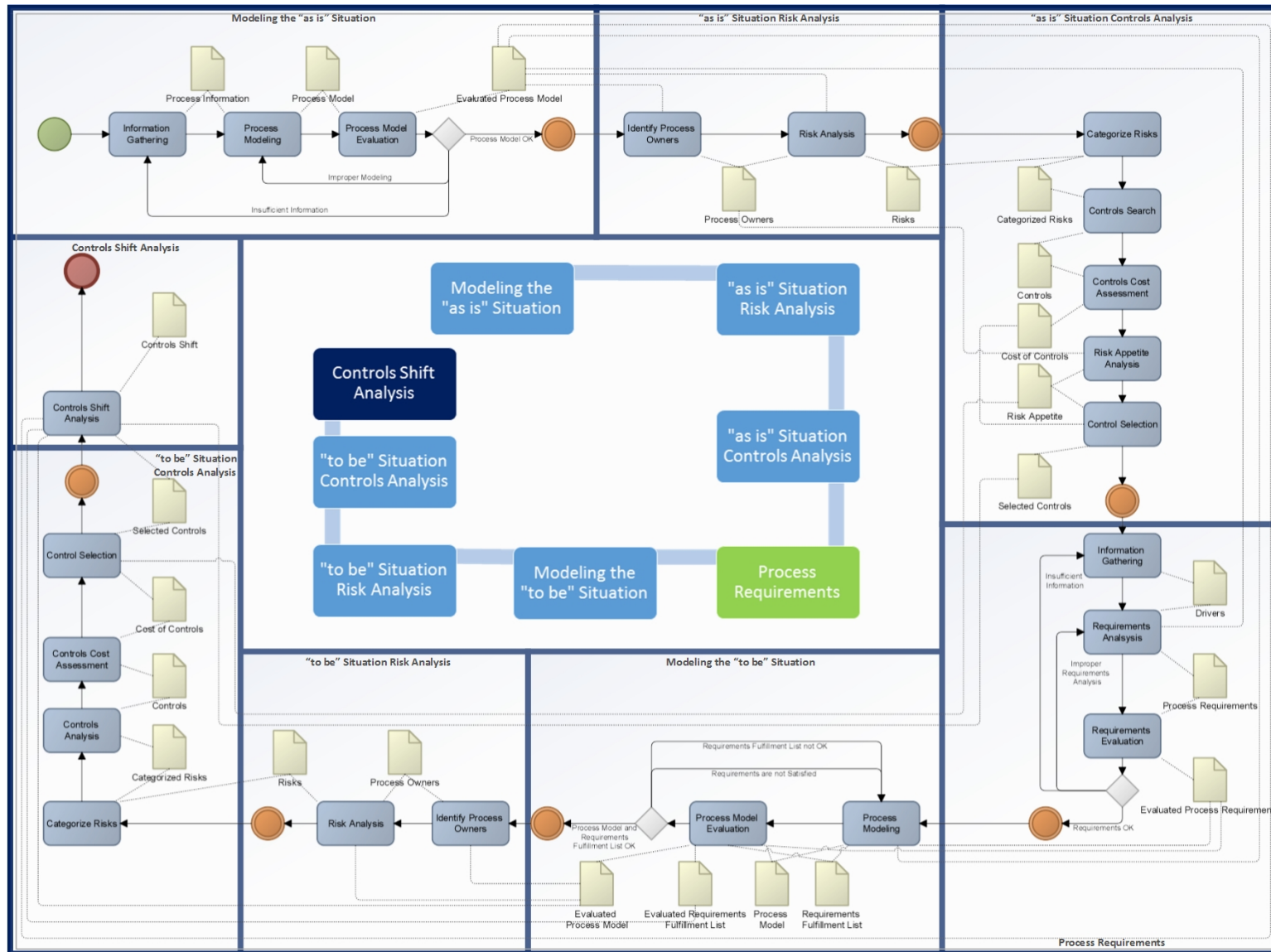


Figure 22. Methodology Outline

## 10.1 Modeling the “as is” Situation

BPR describes that a model of the current processes should serve as a reference point for redesign (Shin and Jellema, 2002); (Lin et al., 2002). Therefore the first step in this methodology will be to establish a status quo for later comparison. This will be done by creating a process model for the process as it is currently. Kueng and Kawalek (1997) describe two important aspects within process modelling:

- Modeling the business process
- Evaluating the business process model

But before these two aspects can be conducted, information has to be gathered that will serve as input for the process modelling. While some process information may be already readily available, it is still important to consult experts to acquire knowledge about the whole process so it can be modeled. Having sessions with them will help to give a structured overview of the whole process. The process model overview for this step is given in figure 23.

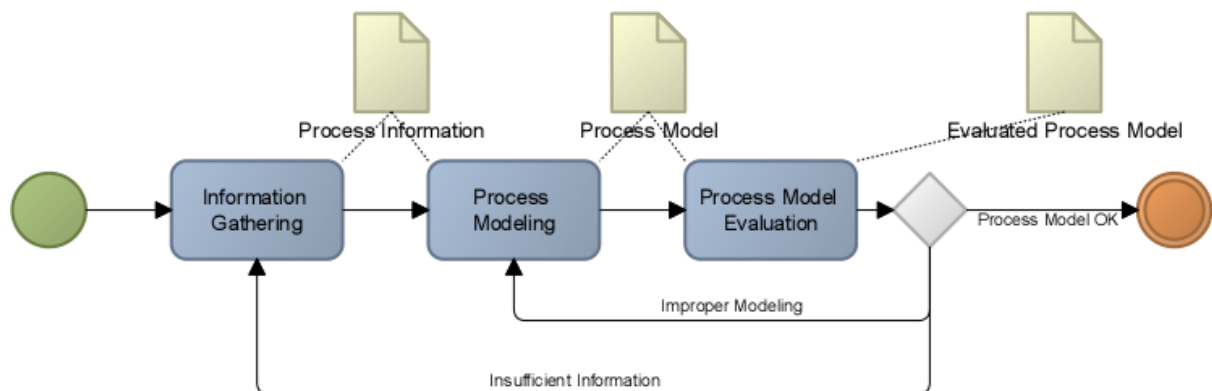


Figure 23. Process Model for Modeling the “as is” Situation

### 10.1.1 Information Gathering

#### *Approach*

Before beginning to model the “as is” situation, it is important to first gather enough information about the process to be modeled. As trivial as this may sound, one should first focus on consulting experts that are involved in the business process design project that is being performed or about to be performed. These experts might already have assessed redesign alternatives based on exploratory analysis of the current situation. They therefore have a better insight into the current situation and may also have already acquired additional information from the organization of which the process has to be redesigned itself.

#### *Method*

*Consulting experts:* Experts that have already initiated the project or are about to initiate it in the future are likely to have already gathered exploratory information about the process that has to be transformed. They also have access to internal documentation that helps to create an overview of the process. If information is not already gathered, one should do this him/herself by consulting the people involved in the current process.

*Field research:* Although it is recommended to consult the experts involved in the BPR project first, since they are already engaged in the information gathering for this project, additional research in the field may be required to fill the gaps that still exist within information gathered. These gaps may stem from the fact that the granularity provided within the information gathered is not sufficient for the modelling steps that follow.

#### *Deliverable: Process Information*

After consulting the experts, enough information should have been acquired to create a process model. This information could include:

- *Process documentation*: Documents that were already there, that describe in text how the process is currently structured. The documents can describe different levels of the process, which will be elaborated on later.
- *Transcripts of performed exploratory interviews/ result overviews based on interviews*: Depending if the BPR project has already been initiated and for how long, more extensive and deepening interviews will have been performed.
- *Process models*: Process models themselves may already be readily available within the organization. It is likely that organizations keep these for their own reference.

## 10.1.2 Process Modeling

### Approach

After gathering the required process information it is now possible to model the “as is” process. This process should reflect the information acquired during the information gathering and will be used as a status quo, which is needed to make the necessary analyses and comparisons in order to assess the impact of business process redesign decisions on internal control. Therefore it is of major importance to model the process clearly, so that experts involved in later stages have a clear overview (O’Neill and Sohal, 1999) of the process they need to analyze.

### Method

*BiZZdesign Architect*: In order to provide a clear process model, the tool we will use to model it will be BiZZdesign Architect (BiZZdesign, 2014). This tool is based on the Archimate 2.1 standard, which is a widely used and accepted standard for defining process models (The Open Group, 2014). This tool models business processes in three levels.

The process modeling levels described in BiZZdesign Architect and that we use in this methodology are the following:

- *The business level*: This level describes the consecutive process steps that have to be performed in order to go from the start of the process to the final product of the process. These steps describe a certain activity, like “receive a request from the client” or “enter data into system A”.
- *The application level*: This level consists of the different applications that support the different process steps. For example a “client information dashboard” support the “receive a request from the client” step by providing additional information about the client. The employee performing the process step now has further knowledge about the client history etc.
- *The technology level*: This level describes the infrastructure technology and hardware that is used in order to support the application within the application level. The “client information dashboard” for example is supported by the “Content Management Information System”, which is in turn enabled by the “Content Database” in which all the raw data is stored. This level also describes the information flow between the different systems, both internally and externally.

Per level, a number of semantics is given in Archimate2.1. Figure 24 shows the semantics that we will use in our research. We will now briefly elaborate on them:

#### Business Level

- *Actor*: represents an actor within the business process level. This actor is involved in a certain business process, but he or she is often not the owner of the process.
- *Role*: represents the role a certain actor performs. An employee of the company can for example fulfill the role of customer management.
- *Product*: represents a product which flows from the business process. This can be a report, a product etc.
- *Business process step*: represents an activity within the business process. The business level consists of multiple business process steps linked together from first input to final output.

#### Application Level

- *Application service*: represents an application service which is used to support the steps within the business level. For example the “registration of a new customer” is supported by the customer management application. A service

is delivered through an application interface. For visibility reasons we do therefore not model the interfaces explicitly. Each service is assumed to have its own interface.

- *Application system*: represents the system that support the application. The customer management application for example may run on a CRM system.

#### Technology level

- *Database/hardware*: represents the database, the server or the hardware on which a certain system is running.

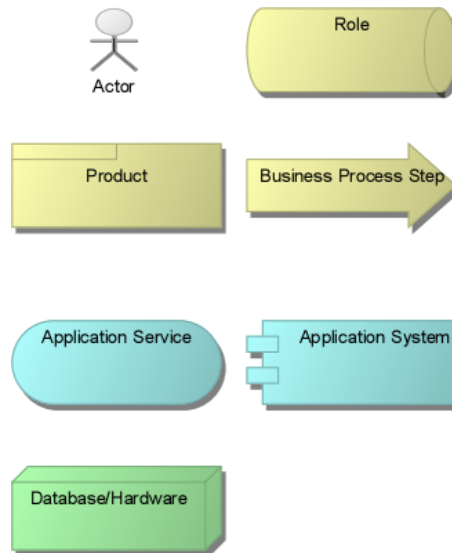


Figure 24. Achimate 2.1 Business Process Semantics

This tool specifically enables modeling a process in these three levels and therefore helps us to provide the process information on the granularity we need for our research. The reason we chose this granularity is because we are not only interested in the business level steps. As described in our scoping we look at compliance risks, but also at operation and IT risks. These cannot be found by only looking at business level steps. The enabling applications and technology might just be the reason a risk is caused. By only looking at process step we do not have enough information to base a risk analysis on.

#### *Deliverable: Process Model*

The results of this step is a process model that gives an overview of the different business process steps and the applications and the underlying technology that enables the fulfillment of these steps. Figure 25 gives an example of how a modeled process could look like.

It also shows which actor performs the different steps. This adds another dimension to the process overview that could be of important to the risk analysis. Risks could for example originate from the fact that certain actors do not have enough knowledge about a process step. These actors are not to be confused with the process and risk owners. A client is an actor in the process, but he or she is definitely not the owner of the process or the owner of the risks.

### 10.1.3 Process Model Evaluation

#### *Approach*

Before proceeding to the next step, it is important to evaluate the created process model (Kueng and Kawalek, 1997). This step is needed to make sure that the process model that is created is also complete and correct. If certain aspects are missing or modeled improperly, these should be found during this evaluation and added to the process model. Therefore the process model is evaluated for two reasons:

- *Correctness*: Is the information gathered properly modeled?
- *Completeness*: Is enough information gathered to create a model that represents reality and has the three layer granularity needed?

It might be that certain information may have been misinterpreted or misread, causing the process model to deviate from the situation described in the information. In this case the gathered process information should be studied again and the process model should be corrected.

As stated before in the information gathering phase, it may be that the process model is not complete because of the fact that the information provided did not give enough insight to create a process model of the needed granularity. Therefore it might be needed to gather information again and update the process model. This is an iterative process.

*Method*

*Consulting experts/Model inspection (Kueng and Kawalek, 1997):* The experts during the information gathering step should be consulted in order to assess the completeness of the process model. They are best able to assess if the information they provided is all present within the model and that various pieces of information have been well interpreted and synthesized.

If there are deficiencies between the information provided and the information presented within the process model, it should be revised. The deficiencies should be noted and we therefore recommend that printed copies of the process model should be brought to the evaluation session to directly draw any corrections or missing aspects in the model. After a potential revision has taken place the evaluation steps should be performed again.

*Simulation/prototyping (Kueng and Kawalek, 1997):* Evaluation can also be done by carrying out a simulation on hypothetical business cases, within a dedicated environment. Different aspects of the modeled process are walked through within different scenarios, in order to find out if no aspects are missing. This is a more rigorous method than consulting experts/modelling inspection, but it also takes more time since a dedicated environment needs to be build and different cases and scenarios have to be prepared.

*Deliverable: Evaluated Process Model*

If no more deficiencies between the provided information and information presented in the process model are found the final evaluated process model (Kueng and Kawalek, 1997) can be finalized and made ready for the next step of the process.

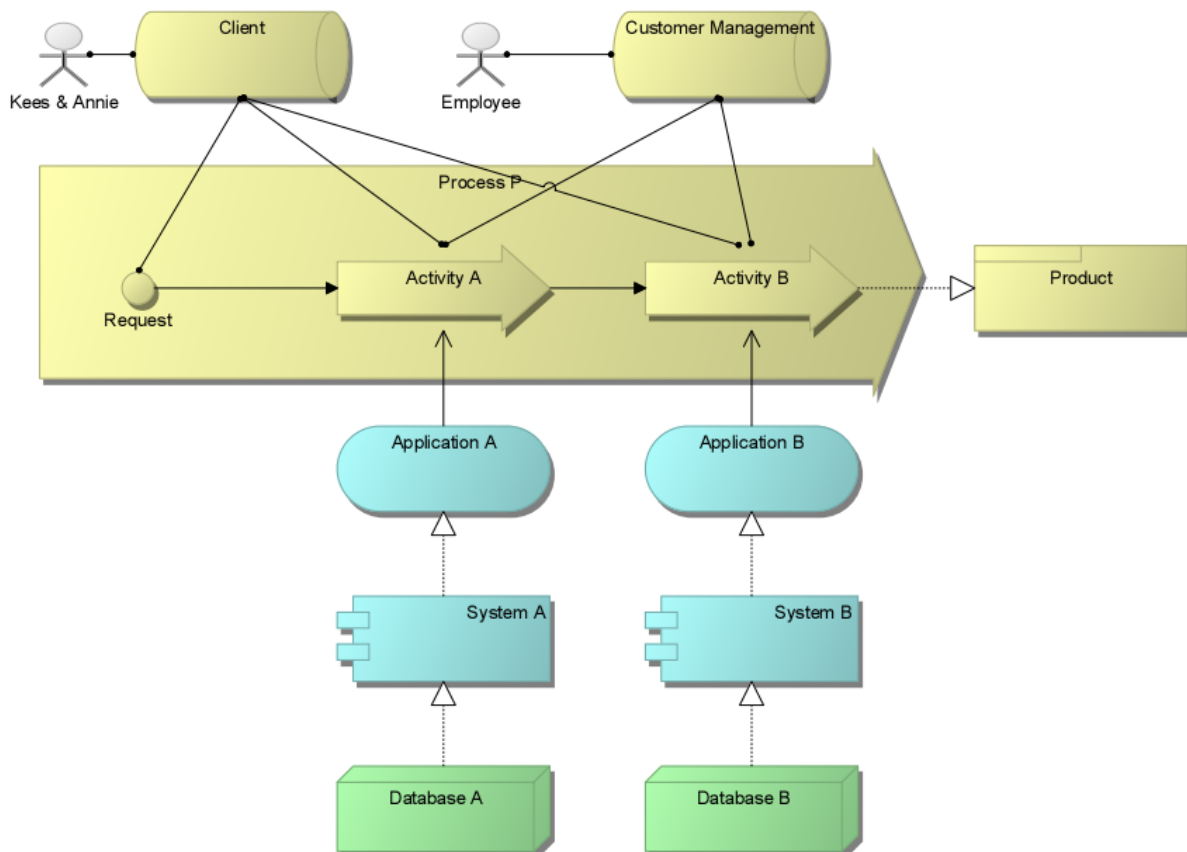


Figure 25. Process Modeling in BizDesign Architect

## 10.2 “as is” Situation Risk Analysis

The second step will be the analysis of risks within the process modeled to gain an understanding of the risk universe of the process. A process model overview for this step is given in figure 26.

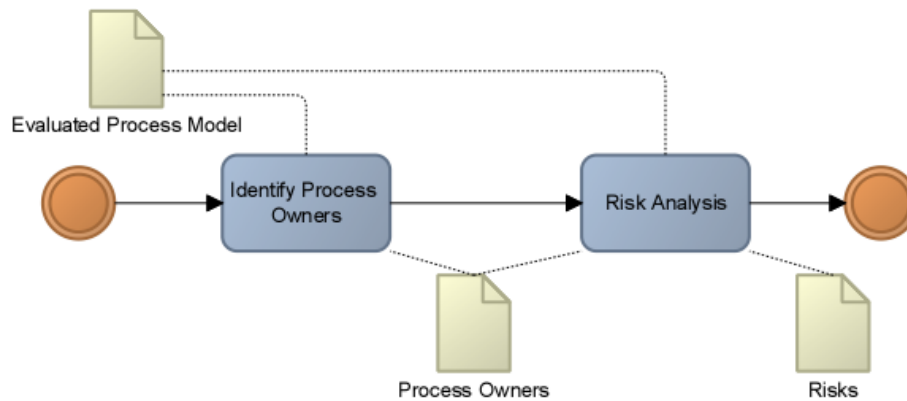


Figure 26. Process Model for the "as is" Situation Risk Analysis

### 10.2.1 Identify Process Owners

#### Approach

The first task in risk analysis is the identification of the process owners of the process studied. These people are responsible for the process who therefore feel the impact of the risks when they occur in the part of the process they own and are the ones that should mitigate the risks when needed, which also makes them the risk owners (Coles and Moulton, 2003); (Moulton and Coles, 2003). An important aspect in this is that they are also the persons who are able to mitigate the risks, since they have the power to change the process or add controls to the process.

#### Method

*Consulting experts:* Risk owner identification is done within Deloitte by performing exploratory meetings and sessions at the start of a project. Therefore experts that are already involved in the project about initiated or about to be initiated have the information needed about process owners/ potential risk owners.

*Best practice databases:* Most consulting companies maintain a database of past experiences, which serve as best practice templates for the future. The Deloitte database contains templates that connect standard process steps to process owners. These process owners are potential risk owners.

*Field research:* Another option is to perform field research. This means that meetings and sessions have to be performed by the person applying the method him/herself. This is only recommendable when no risk owner information is available yet.

*RACI:* Schepers (2007), mentions the RACI method of Malinverno (2006) in his thesis to assess what role a certain stakeholder has in a project. The method helps differentiating the role of stakeholders by assigning them four roles:

- *Responsible:* Responsible for the deliverables of a project. Is responsible towards the accountable person.
- *Accountable:* Has the authority to continue or cancel the project. Only one person can be accountable.
- *Consulted:* Has to be consulted before an action is taken. (Their approval may be optional.)
- *Informed:* Needs to be informed, but does not have decision rights.

We argue that this method can also be used to identify process owners within a process. We defined the process owners as the people responsible for the process who therefore feel the impact of risks when they occur and who are able and authorized to take actions to mitigate the risks. In the RACI method this means that someone is a process owner when he is at least responsible. An example RACI table is given in table 5, which is based on the original RACI table. We however argue that a stakeholder can have multiple roles and have therefore modified the table.



Table 5. Example RACI Table Based on: Malinverno (2006)

Process	Product Line Director	Customer Relationship Manager	Technical Support Manager	Call Centre Employee
Process P	A	R	R	I

*Deliverable: Process Owners*

It is important to carefully list all the process owners within the process and the process aspects they own. We suggest that a spreadsheet should be used for this. Since the accountable process owner is responsible for the whole process it is of no use to specify the process elements he is responsible for. Knowing which part of the process is owned by a certain responsible process owner helps placing the risks identified by that person within a context. Someone who is for example responsible for a certain application will most probably emphasize technology-related risks above for example human related risks. An example spreadsheet is given in table 6.

This process owner spreadsheet can then be used as a reference guideline for who to invite to a risk analysis session, when this is carried out, as internal experts. As many process owners as possible should be incorporated in the risk analysis sessions.

Table 6. Process Owner Spreadsheet

Process Owner	Process Aspects
Customer Relationship Manager	Activity A
Technical Support Manager	Applications, Technology and Infrastructure

10.2.2 Risk Analysis

*Approach*

Now we know the process owners and we have the process modeled, we can determine what risks can occur within the process. This is the first step as described by Lambert et al. (2006). We need to know these risks since it is one of the factors within the risk universe equation.

The Institute of Risk Management (2011) tell us that the risk universe contains all risk within the operating area of the organization. An organization chooses a certain operating area within the environment and the risks within that area become the risks of the organization. In this case the modeled process tells us how operations are done within a specific operating area so the risks identified are the risk universe of the process. So this step is crucial to later fill in the equation.

*Method*

*Risk matrix:* Literature showed us that the risk matrix is a good tool to visualize risks. The risk matrix is discussed in literature (Remenyi and Heafield, 1996); (Bass and Robichaux, 2001) as well as documents within the Deloitte database (Curtis and Carey, 2012); (Institute of Conflict Management, 2013). This risk matrix has the occurrence of a risk on the X-axis and the impact on the Y-axis. The risk matrix layout that we will use is provided in figure 27.

By mapping risks on this risk matrix, a clear overview of the risks and the relative importance to each other becomes clear. This is the second step as described by Lambert et al. (2006), since risks are measured in the relative important towards each other, using two variables. Visualizations like these are understandable for everyone and provide a clear starting point for the risk analysis session. Only a little explanation is needed to make everybody aware of the use of and logic behind the risk matrix.

*Risk analysis session:* In order to fill the risk matrix, risk owners as well as external experts from Deloitte are asked to attend in risk analysis sessions. Within these sessions, the process model and the risk matrix will be available and discussion about risks is possible. Risks are first identified and then they are mapped into the risk matrix. Preferably this is

done in one session, but the identification and mapping of the risks into the risk matrix can also be done in separate meetings. However it is important that the involved experts have a chance to review the choices of the other experts.

By doing this, various people with various kinds of expertise can discuss risks with each other in order to determine the final mapping of the risk on the risk matrix. Risks that are for example mapped as important by an IT specialist might be mapped as unimportant by a customer relationship manager. By putting all these people in one session, they can add nuance to each other’s identified risks. The final filled risk matrix is therefore more likely to be close to the truth. This is the third step as described by Lambert et al. (2006), in which risks are thoroughly evaluated by different experts.

An alternative to this is the automated version of the risk analysis session provided and used by Deloitte Risk Services. The idea looks like voting using buttons on a box. First participants are asked to identify risks within the process. The risks are then used as input for the voting session, in which each attendee of the risk analysis session is asked to use the voting box to choose the impact and chance of occurrence for each risk independently.

Finally, the computer combines all the results and provides a risk matrix with all the risks plotted in it. One advantage of using this alternative is the fact that the computer makes the results a bit more quantitative since attendees are asked to give a number for the degree of impact and chance of occurrence.

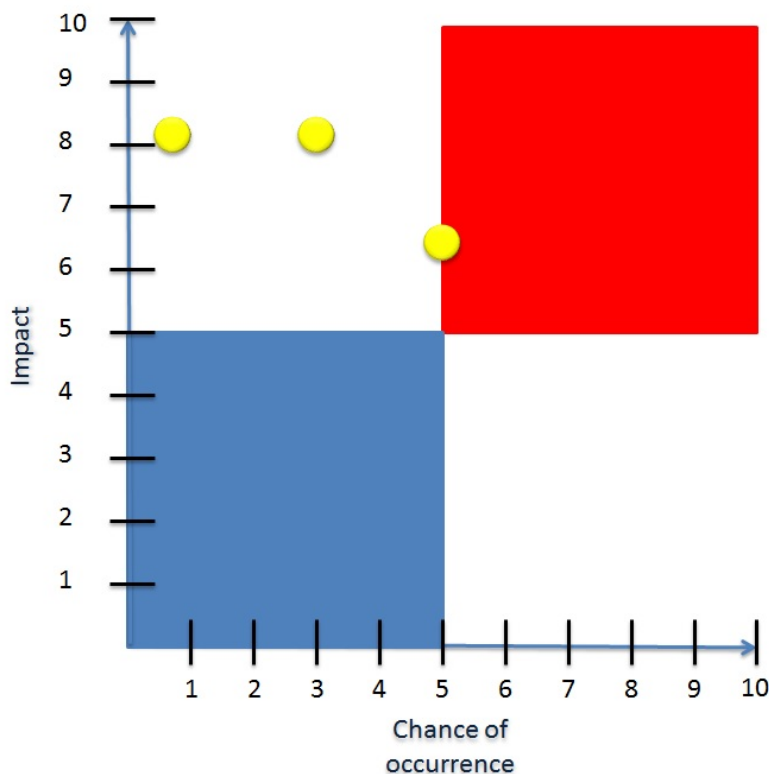


Figure 27. Risk Matrix Layout

*Consult risk analysis documents:* Since the “as is” situation modeled is already been in operation in the bank, risks analyses might already have been performed. This was pointed out by colleagues within Deloitte Risk Services. One should look for risks analysis documents, since they show the risks previously identified in the “as is” situation by process owners and often experts from a consulting company. Risks identified by the process owners identified in the previous task should be searched for. These risks should then be put in a risk matrix together with external experts in order to incorporate the experience they have.

*Deliverable: Risks in Risk Matrix and Risk Table*

The final deliverable of this step is a risk matrix that is filled with risks in the various levels represented in the business process model, but also risks that occur because of the connections between and within the various areas and risks that may flow from human interaction with the process.

Next to this risk matrix, a spreadsheet containing a textual description of the risks, the process activities the risks occur in, the specific process elements within the activity in which the risks occurs, and the risk owners has to be created. Table 7 gives an example of this, which is based on formats found in Deloitte resources. The format used is:

- *Risk ID*: Each risk is numbered.
- *Risk Description*: A short description of the potential risk.
- *Risk Elements*: The specific elements in the process model in which the risk occurs. This can either be in a process step itself, in the information technology supporting the business process step, or a combination of both.
- *Impact*: The impact factor, derived from the risk matrix.
- *Occurrence*: The occurrence factor, derived from the matrix.
- *Owner*: The owner of the risk.

Table 7. Risk Identification Spreadsheet Based on: Deloitte Resources

ID	Identified Potential Risk	Risk Elements	Impact	Occurrence	Owner
1	Errors occur through automated data conversion	System A	8	5	Technical support manager
2	Data conversion processes are out of synch (Global - Local). A control process for data synchronization is not in place	Database B	1	3	Technical support manager
3	Too many manual intervention points will exist	Activity A, Activity B	2	2	Product line director
4	Errors occur through manual data conversion	Activity A	6	6	Customer relationship manager

### 10.3 “as is” Situation Controls Analysis

In the third step the risks that have been identified have to be linked to appropriate controls. This will be done by first categorizing the risks into the scoped risk categories and then searching for controls to mitigate the risks. After that the costs of these controls is assessed and the risks appetite is determined. The risk appetite and the cost of controls are then used to select the controls that need to be implemented. The process model for the “as is” situation controls analysis is given in figure 28.

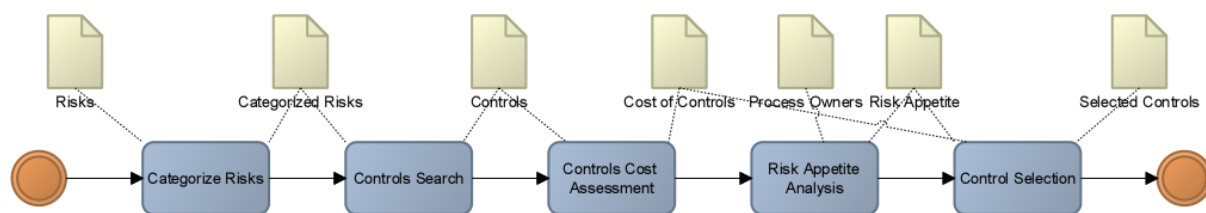


Figure 28. Process Model of the “as is” Situation Controls Analysis

#### 10.3.1 Categorize Risks

##### Approach

Now that in the previous step the risks have been determined, this task is about categorizing the risks into the different risk categories scoped on within this methodology. The three layer granularity we used in the process modeling enables us to find these categories of risks. These risk categories were chosen, because they are most affected by business process redesign through the drivers described.

By categorizing the risks into the risk categories, a status quo is established for the risk distribution within the process. Based on this status quo a comparison between risk distribution can later be made with the “to be” process. This shift in risk distribution can later be combined with the shift in controls.

## Method

*FIRM risk categories mapping:* The three risk categories scoped on that are derived from the FIRM risk framework by DNB (De Nederlandsche Bank, 2014) will be used to categorize the identified risks on. We will briefly elaborate on the risk categories again:

- *Operational Risk:* Risks that flow from the operations process. These are risks that flow from the different activities within the business process that are not caused by the underlying IT support.
- *IT Risk:* All risks that flow from the usage of IT to support processes.
- *Legal Risk:* These are the risks when looking at compliance to laws and regulations. Even though the process activities and the IT support is carried out correctly, it may not be done according to laws and regulations.

*Consulting experts:* External experts have experience on mapping risks into different risk categories. These experts should be incorporated in the categorization of risks in order to include their expertise into the process as a validation.

## Deliverable: Categorized Risks

The deliverable of this task should be an overview of the risks acquired from the previous step with their risk category. An example of such an overview is given in table 8, which shows the risks identified earlier, which now have their risk category added. The format used is:

- *The Risk Category:* The risk is of one of the scoped risk categories.
- *Risk ID:* This is the same number that was used in the risk analysis.
- *Risk Description:* A short description of the risk, already documented in the risk analysis step.
- *Risk Elements:* The specific elements in the process model in which the risk occurs. This can either be in a process step itself, in the information technology supporting the business process step, or a combination of both.
- *Impact:* The impact factor, derived from the risk matrix.
- *Occurrence:* The occurrence factor, derived from the matrix.
- *Owner:* The owner of the risk, who is also identified earlier in the risk analysis step.

For example, manual data conversion by an employee for example is an operational risk, which is under the responsibility of the customer relationship manager, while automated data conversion is an it risk, which is under the responsibility of the technical support manager.

Table 8. Categorization of Risks

Risk Category	ID	Risk	Risk Elements	Impact	Occurrence	Owner
IT	1	Errors occur through automated data conversion	System A	8	5	Technical support manager
IT	2	Data conversion processes are out of synch (Global - Local). A control process for data synchronization is not in place	Database B	1	3	Technical support manager
Operational	3	Too many manual intervention points will exist	Activity A, Activity B	2	2	Product line director
Operational	4	Errors occur through manual data conversion	Activity A	6	6	Customer relationship manager
Legal						

## 10.3.2 Controls Search

### Approach

Now that the risks have been determined and categorized, controls have to be assigned to these risks in order to make these risks manageable. This is part of the fourth described by Lambert et al. (2006). This can be done by using controls frameworks, consulting the risk and controls register of the bank studied and consulting experts. One important assumption that is made in this step is:

- The control linked to the risk is retrieved from best practices, which means it is the appropriate control for mitigating the risk.

As described in literature, control frameworks serve as best practice frameworks to link controls to certain risks within an organization (Pederiva, 2003); (Rikhardsson and Best, 2006). Control framework describe certain control practices and their underlying control objectives, such as IT controls and their objectives as described within the CobiT framework. Risk and controls registers are registers that are used by banks to keep an overview of all the risks in their processes and the consecutive controls to mitigate them.

### *Method*

*Control frameworks:* these frameworks serve as best practice frameworks in which control indications to certain risks are given and often elaborated on in control objectives, such as in the CobiT framework (Tuttle and Vandervelde, 2007). Because these frameworks are based on best practice, they are used in order to help find controls to the risks. Experts should be incorporated in this process, since they have extensive experience on linking risks to control activities and there have the knowledge to translate the somehow high level control objectives given in the control frameworks to more practical situation specific and applicable controls.

Multiple control frameworks are available for this, as described in the literature (Hermanson, 2000); (Pederiva, 2003); (Rikhardsson and Best, 2006). Deloitte however, uses the COSO framework as a structural guide and frameworks like CobiT as an implementation of its steps. As described before, the usage of multiple control frameworks in order to implement the COSO structure has led Deloitte Risks Services to choose for the implementation of an integrated control framework. This framework is however not ready yet and still has to be assessed for its effectiveness.

*Consult the risk and controls register:* As described before, it is not a new phenomenon that banks have to be in control of their processes. Therefore controls have been defined for all processes within the bank. These controls and their corresponding risks are stored within the risk and controls register. This was pointed out by colleagues within Deloitte Risk Services.

Table 9 gives an example of a possible layout of a risk and controls register. Per service area, multiple process and their sub processes are listed. Within these sub processes there are various activities (process steps) that have to be carried out. The risks per activity are identified and a control objective that describe that the risks need to be mitigated are linked to the risk. Then a control (control activity) is assigned to the risk and the type of control is given. This can be either an automated/manual control and a preventive, detective or corrective control (Bass and Robichaux, 2001); (Kliem, 2000); (Kliem, 2004); (Cavusoglu et al., 2004); (Kartseva et al., 2004); (Panko, 2006).

By consulting this register, the risks identified within the process can be linked to controls linked to the risks already described within the register. It is also important to incorporate the knowledge of experts here, since risks identified in the previous step may differ from the risks described in the register at first sight. Experts however are used to work with risk and controls registers and are therefore able to quickly identify the corresponding risk in the register. It is important to point out two things while using the risk and controls register:

- Not all risks within the register that are described for the process are risks identified within the previous step, since these risks are broader then the scope of our research and therefore the granularity of our process model.
- An assumption is made that the controls described in the risk and controls register are sufficient to mitigate the risks they are assigned to an acceptable level. In other words this means that application of the controls derived from this register means that all risks are therefore also mitigated to an acceptable level.

*Consulting experts:* Having the knowledge of both control frameworks and risk and controls registers, using experts results in case-specific controls to the identified risks to be mitigated. Their experience in the field enables them to quickly transform high level best practice controls into controls that are applicable in the specific situation.

### *Deliverable: Controls*

The deliverable here should be a set of controls. This set of controls is a subset of the controls described within the risk and controls register, or a number of controls derived from using control frameworks and consulting experts in order to link

risks to controls. We propose a similar format as given in table 10 should be used to create an overview of the risks and their controls. This format includes:

- *The Risk Category*: The risk is of one of the scoped risk categories.
- *Risk ID*: This is the same number that was used in the risk analysis.
- *Risk Description*: A short description of the risk, already documented in the risk analysis step.
- *Risk Elements*: The specific elements in the process model in which the risk occurs. This can either be in a process step itself, in the information technology supporting the business process step, or a combination of both
- *Impact*: The impact factor, derived from the risk matrix.
- *Occurrence*: The occurrence factor, derived from the matrix.
- *Owner*: The owner of the risk, who is also identified earlier in the risk analysis step.
- *The Control Objective*: This is description of the goal that needs to be achieved by implementing a control.
- *Control #*: Each control is given a specific number.
- *Control Activity*: A description of the control itself.
- *Control Frequency*: The frequency with which the control is carried out.
- *Control Type (Automated/Manual)*: The control is either carried out automated or in a manual fashion.
- *Control Type (Preventive/Detective/Corrective)*: Describes the type of control based the three different types of controls.

Table 9. Risk and Controls Register Example Based on: Deloitte Resources

Service Area	Process	Sub Processes	Activities	Risk Category	Risk No.	Risk Description	Control Objective	Control No.	Control Activity	Control Frequency	Control type (Automated/ Manual)	Control Type (Preventive/ Detective/ Corrective)	Control Owner
Primary Services	Mortgage Provisioning	Oriëntation	Create Dossier	IT	1	The risk that client enters wrong data format.	Right data format is entered.	1	System checks data format.	Adhoc	Automated	Preventive	Technical Support manager
Primary Services	Mortgage Provisioning	Oriëntation	Create Dossier	IT	2	The risk that the dossier is not saved.	Dossier is saved correctly.	2	System checks and sends notification to client.	Adhoc	Automated	Detective	Technical support manager
Primary Services	Mortgage Provisioning	Oriëntation	Create Dossier	IT	2	The risk that the dossier is saved incorrectly.	Dossier is saved correctly.	3	System sends copy of saved data to client for double check.	Adhoc	Automated	Preventive	Technical support manager
Primary Services	Mortgage Provisioning	Oriëntation	Register Income and Charges	Operational	3	Client registers invalid income and charges.	Income and charges are valid.	4	Bank employee performs a check on the income and charges.	Adhoc	Manual	Detective	Product line manager

Table 10. Controls List Example

Risk Category	ID	Risk	Risk Elements	Impact	Occurrence	Owner	Control Objective	Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C
IT	1	Errors occur through automated data conversion	System A	8	5	Technical support manager	Data is properly converted	3	System performs check	Adhoc	Automated	Detective
IT	2	Data conversion processes are out of synch (Global - Local). A control process for data synchronization is not in place	Database B	1	3	Technical support manager	Data synchronization	4	A control process for data synchronization is in place	Adhoc	Automated	Preventive
Operational	3	Too many manual intervention points will exist	Activity A, Activity B	2	2	Product line director	Manual interventions are correct	1	Manager corrects incorrect manual interventions	Adhoc	Manual	Corrective
Operational	4	Errors occur through manual data conversion	Activity A	6	6	Customer relationship manager	Data is properly converted	2	Bank employee performs a check	Daily	Manual	Detective
Legal												

### 10.3.3 Controls Cost Assessment

The third task is about determining the costs that need to be made when implementing the controls determined in the previous task. This is also part of the fourth step described by Lambert et al. (2006): "Risk acceptance and avoidance", since the cost of controls will be important for determining which controls will be implemented and which will not and therefore what risk will be addressed.

#### *Approach*

Literature (Bass and Robichaux, 2001); (Kliem, 2000); (Kliem, 2004); (Cavusoglu et al., 2004); (Kartseva et al., 2004); (Panko, 2006) showed us that there are three types of controls, namely preventive, detective and corrective. Controls can also be classified as manual or automated. This is often done by consultancy companies and also within Deloitte Risk Services. Manual controls are control activities that are performed manually by human intervention, while automated controls are control activities that are done in an automated fashion through technology. The aim here is to use these control types together with their frequency as an input for determining the effectiveness and efficiency of controls in order to determine the cost factor that is linked to each control.

#### *Method*

*Control frequency, effectiveness and efficiency assessment:* Each control is performed at a certain frequency, as is already indicated in the controls table determined in the previous task. The more times a control is performed, the higher the control effort.

Figure 13 (The Institute of Risk Management, 2011) in part 2 – Information Gathering gives a graphical representation of the risk universe, risk tolerance and risk appetite. Risk is described in literature as an event or condition that, if it occurs, has a negative or positive impact on an objective or performance (Project Management Institute, 2002).

Figure 13 also shows this by describing a positive and negative deviation in performance from the chosen direction. The space in between is the risk universe. It can also be seen that time plays an important role. The performance deviation increases when more time elapses. The later a risk is mitigated, the bigger the impact on performance.

When we combine this with the concept of preventive/detective/corrective controls as described in literature and visualized in figure 16 by Panko (2006) we assume that preventive controls will be more effective than detective controls and that detective controls will be more effective than corrective controls, because of their risk mitigation moment. Preventive, detective and corrective controls consecutively mitigate risks in time. While preventive controls mitigate risks before they occur, corrective controls fix the actual deviation after it happened. This means that the impact on performance is already higher and that a bigger effort is needed to mitigate it. The bigger the effort, the higher the costs.

However we purely look from an effectiveness perspective here, since the efficiency of controls also plays an important role. For example a manual control may be very effective in terms of effort needed but extremely inefficient in terms of the implementation of the effort, since it is carried out manually and it takes a lot of man-hours to complete the effort and is therefore costly. A corrective automated control on the other hand may be very efficient because it can be carried out by an information system taking a few machine-hours, but it may be less effective since the deviation has already occurred and has to be fixed, increasing the control effort.

Automated controls are likely to be much more efficient than manual controls, since they are far less time consuming because they are performed by information systems instead of humans. The computing power of information systems is much higher than that of a human, making it possible to perform far more control activities in the same time it would normally take a human to perform a control activity. Therefore automated controls are also more cost efficient than manual controls. Sadiq and Governatori (2010) give an indication about the efficiency of automated and manual controls by describing the two main approaches within detective controls. They state that detective controls can be done both manually and automated and that when using automated controls assessment time and correspondingly the time for remediation/mitigation of deficiencies is improved. This indicates that automated controls are more efficient than manual controls.



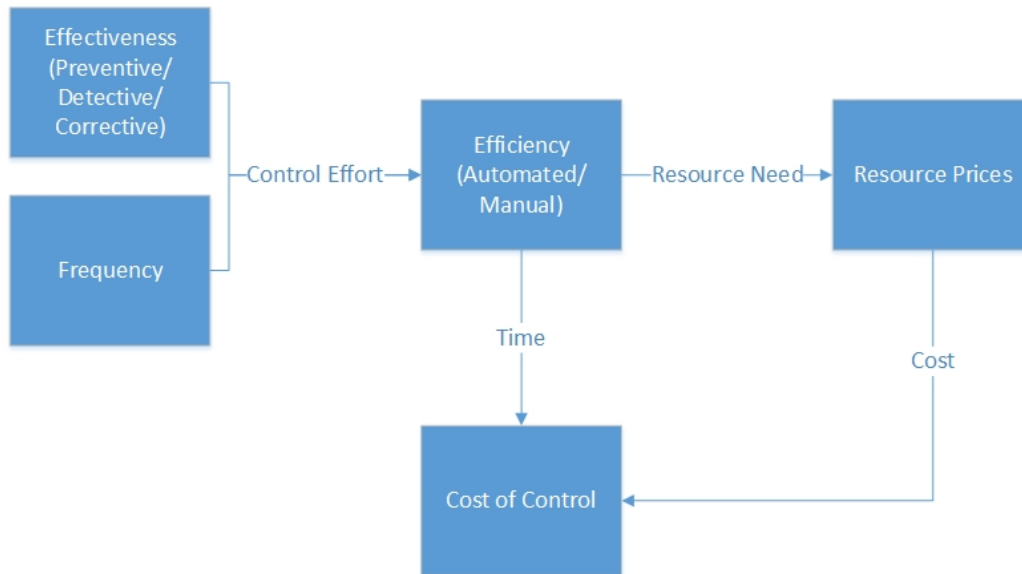


Figure 29. Indicators for Cost of Control

Based on these findings and knowledge provided by colleagues within Deloitte Risk Services, we recommend that the cost of control is indicated by the following four factors, as displayed in figure 29:

- *Frequency*: The frequency with which a control is performed.
- *Effectiveness*: The effectiveness of a control based on its type (P/D/C), as described above.
- *Efficiency*: The efficiency of a control based on its type (A/M), as described above.
- *Resource Prices*: The price of using certain resources.

Assessing the cost of controls based on frequency, efficiency and effectiveness as indicators has to be done in close cooperation with the experts, since they know from experience what controls are more effective than others, what controls are more efficient than others and how often controls are performed. They also have knowledge about cases like the example given above and can therefore make the connection between efficiency and effectiveness.

*Cost of controls assessment*: After assessing the frequency, effectiveness and efficiency of controls it is of major importance to know what controls will cost in terms of time and resources. We express cost of control in:

- *Cost*: The cost of the resources that are used to perform the control for an amount of time. This could also be expressed in costs per time unit in a quantitative analysis.
- *Time*: The amount of time that it takes to perform the control. This could also be expressed in time units in a quantitative analysis.

Multiplying these two factors results in the cost of control. When for example a control has a time requirements of five and cost requirement of 7, the cost of that control will be  $5 \times 7 = 35$ . While doing this assessment, we use one assumption:

- The control linked to the risk is performed to full extent.

This means that the time and cost factors have to be assessed for the case that a control is fully performed. While using this guideline, experts should be consulted in order to determine what the cost of control in terms cost and time of each control will be. Therefore this efficiency and effectiveness assessment made earlier serves as an important input.

### *Deliverable: Cost of Controls*

The final deliverable should be a table that represents the controls as described in the controls table and their costs. An example is given in table 11. The format is extended with:

- *Cost*: The factor indicating the cost of the resources that are used to perform the control for an amount of time.
- *Time*: The factor indicating the amount of time that it takes to perform the control.

Since it is hard to link exact amounts of money and time to controls within possible redesign decisions and this also not the aim of our research we suggest that a cost and time factor should be given to each control. This factor from 1-10 is used to indicate the relative cost and time of each control compared to the other. A factor of 1 means very low cost or a small amount of time, while a factor of 10 means a very high cost or a big amount of time. Of course, while performing the methodology on a case, one is free to choose another scaling or to give other descriptions to each factor.

Table 11. Cost of Controls Table Example

Risk Category	ID	Risk	Risk Elements	Impact	Occurrence	Owner	Control Objective	Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Cost	Time
IT	1	Errors occur through automated data conversion	System A	8	5	Technical support manager	Data is properly converted	3	System performs check	Adhoc	Automated	Detective	3	2
IT	2	Data conversion processes are out of synch (Global - Local). A control process for data synchronization is not in place	Database B	1	3	Technical support manager	Data synchronization	4	A control process for data synchronization is in place	Adhoc	Automated	Preventive	1	1
Operational	3	Too many manual intervention points will exist	Activity A, Activity B	2	2	Product line director	Manual interventions are correct	1	Manager corrects incorrect manual interventions	Adhoc	Manual	Corrective	5	6
Operational	4	Errors occur through manual data conversion	Activity A	6	6	Customer relationship manager	Data is properly converted	2	Bank employee performs a check	Daily	Manual	Detective	3	4
Legal														

### 10.3.4 Risk Appetite Analysis

The fourth task is about determining the risk appetite for the process. Now that the risks, the controls linked to the risks and the cost of these controls are determined, the risk appetite has to be determined in order to select the controls that need to be implemented. This is part of the fourth step described by Lambert et al. (2006).

#### *Approach*

Literature (Gai and Vause, 2005) tells us that risk appetite is based on two factors:

- *Risk aversion* (Danielsson, 2010); (Dungey et al., 2003)
- *Macroeconomic environment*

Within this task the goal is to assess these two factors in order to determine what the risk appetite is within this process. Experience is important in this process since risk aversion is highly dependent on “soft” factors as stated in the literature. Therefore both experts and process owners should be incorporated in this step.

#### *Method*

*Risk appetite analysis session:* This is a more bottom up approach of which colleagues within Deloitte Risk Services pointed out that the risk appetite has to be established with both internal experts and the person that is finally accountable for the process, which can be found in the RACI table. This is a useful approach when risk appetite is already well established and operationalized within process in a bank and accountable process owner is therefore aware of the risk appetite within his process.

External experts are very important within this step, since they are fully aware of the laws and regulations that are posed on the process. They do therefore know what risks must be mitigated by laws and regulations, but they do also know from previous experience what level of risk mitigation is best. They therefore reflect the macroeconomic environment.

The accountable process owner should be incorporated in order to provide some nuance. He/she reflects the risk aversion, because he/she has a better insight into the risk appetite policies set out within the company. It may even be the case that a risk appetite has been determined for every process on a higher level.

This can be related to figure 14, which shows the determinants of risk appetite as identified by Gai and Vause (2005). While accountable process owner has an intrinsic risk aversion that can only be assessed by having sessions with him/her, there is also the macroeconomic environment. External experts can be used to assess this environment in terms of laws and regulations and best practice, but accountable risk owners can be used to assess this environment in terms of internal policies.

*Risk appetite statement:* Another approach used by consulting companies is the establishment of a risk appetite statement (Deloitte, 2014). This top down approach is commonly used when a new risk appetite needs to be established on a strategic level. This risk appetite on a strategic level then needs to be translated and allocated to different units and groups in order to operationalize it to their processes. This is a time consuming approach that starts at the stakeholders and the board of directors and cascades through organizational levels to the final operationalization in processes. The different steps (shown in figure 30) are:

- *Establish risk appetite statement:* This statement is based on overall strategic goals and by consulting stakeholders. Finally the board approves the risk appetite statement.
- *Define a risk appetite framework:* A guiding framework that defines acceptable types and amounts of risk on an organizational level.
- *Implement the risk appetite framework:* The risk appetite statement and the risk appetite framework are communicated throughout the organization and translated and allocated to different organizational units and groups. The risk appetite statement and framework is then operationalized and monitored.

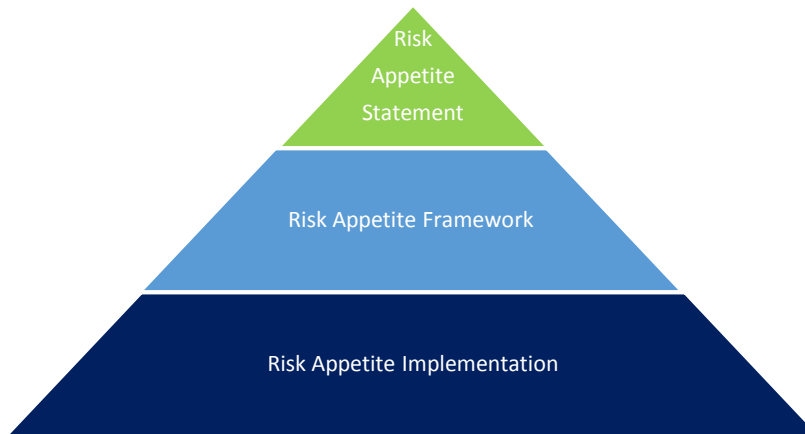


Figure 30. Risk Appetite Statement Approach Based on: Deloitte (2014)

*Consult risk appetite analysis documents:* Just as there might already be documents about risk analysis sessions already carried out in the past, it might be well possible that a risk appetite analysis also has been carried out in the past. One should search for documents describing this risk appetite analysis in order to find out what the identified accountable process owners described as their risk appetite. This risk appetite should then be discussed with external experts in order to incorporate the experience they have.

*Deliverable: Risk appetite*

The deliverable should be a determination of the risk appetite and therefore the level of unmitigated risk after the implementation of controls. This concretely means that the effect on performance (The Project Management Institute, 2000) will not cause an impact that is higher than the risk appetite. In practice this is described as an amount of money, which should not be exceeded by the total amount of all costs that are made when certain risks occur.

In this method however, risks are assessed in a qualitative fashion, using impact and occurrence factors. Multiplying these factors with each other gives a total impact indication. Risk five in table 11 for example has a total risk factor of  $8 \times 5 = 40$ . For this reason we therefore recommend that the risk appetite should also be expressed using a total risk factor, for example: Risk appetite = 100.

### 10.3.5 Control Selection

This task is about selecting the controls that will be used from the identified controls, based on the risk appetite. This is done by using the risk appetite and the equation determined using literature, which is given in figure 31. Risk universe has been replaced for determined risks here, since the risk determined in the previous task serves as the risk universe for the process studied here.



Figure 31. Risk Equation

The process of determining which risks should be mitigated and which risks should not be mitigated by means of selecting controls is also part of both the fourth and fifth step described by Lambert et al. (2006), since the controls finally selected will be used to manage the risks.

## Approach

The risk appetite determined in the previous tasks describes the degree of risk that is acceptable after risk mitigation. If there is no risk appetite, this means that all risks have to be mitigated completely. If there is a risk appetite, this implies that certain risks will be addressed and some will not be addressed (completely). This means that certain controls are not implemented or only to a limited extent. This task is about selecting the controls to be implemented based on the risk appetite.

## Method

*Control selection session:* Colleagues within Deloitte Risk Services pointed out that the selection of controls based on the risk appetite within a certain process is a difficult and time consuming process. Since we have a set of controls with the risks they are linked to on one hand and the risk appetite on the other hand, such a selection of controls should be made that the eventual unmitigated risk does not exceed the risk appetite.

The impact and occurrence of risks determined earlier, which is also shown in the risk matrix, is an important indicator for the fact whether a risk should be mitigated or not. While the sum of a number of low-level risks can be lower than the risk appetite, a high-level risk is likely to exceed the risk appetite on its own. One may choose to mitigate one risk to the highest extent possible, while this comes at a high cost because the cost factor of the linked controls is high. But it may also be better to mitigate multiple risks to a lower extent, since the controls linked to these risks have low cost factor.

Internal experts have extensive experience with mitigating risks and should therefore be consulted on order to establish a set of controls that together produce an amount of unmitigated risk that is lower than the risk appetite and is also the most favorable set in terms of cost of control. We recommend a control selection session, which uses the list of controls and risks, the risk matrix and the cost of controls determined in order to find the best set of controls that should be implemented and the degree in which they should be implemented.

## Deliverable: Selection of Controls

The final deliverable should be a set of controls selected from all the control identified. Per control it also determined in which degree a control is implemented. Based on this degree and the cost and time factor identified earlier, a final cost and time factor can be determined. Table 12 gives an example of a selected controls table. It uses the same format as the cost of controls table (table 11), except:

- *Final Cost:* The final factor indicating the cost of resources needed to perform a control, given the risk appetite.
- *Final Time:* The final factor indicating the time needed to perform a control, given the risk appetite.

While the IT risks have to be mitigated completely, risk three is not mitigated at all and risk four is only mitigated in a certain degree, resulting in a lower final cost of control. The selection of controls has to fulfill two criteria:

- After implementing the selection of controls, the amount of unmitigated risk is equal to or lower than the risk appetite.
  - Within this criterion, the set of controls with the lowest total cost of controls has to be selected

Table 12. Selected Controls Table Example

Risk Category	ID	Risk	Risk Elements	Impact	Occurrence	Owner	Control Objective	Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Final Time
IT	1	Errors occur through automated data conversion	System A	8	5	Technical support manager	Data is properly converted	3	System performs check	Adhoc	Automated	Detective	3	2
IT	2	Data conversion processes are out of synch (Global - Local). A control process for data synchronization is not in place	Database B	1	3	Technical support manager	Data synchronization	4	A control process for data synchronization is in place	Adhoc	Automated	Preventive	1	1
Operational	4	Errors occur through manual data conversion	Activity A	6	6	Customer relationship manager	Data is properly converted	2	Bank employee performs a check	Daily	Manual	Detective	2	3
Legal														

## 10.4 Process Requirements

The fourth step will be to derive process requirements from the drivers identified within part 2 – Information Gathering. Business process redesign literature describes that performance input from the current process is an important aspect that drives the need for change (Shin and Jellema, 2002). The drivers that stem from both this performance input as well as stakeholders need to be evaluated and translated into process requirements (Küng and Hagen, 2007) for the “to be” process. Comparing current performance with the performance level required by the drivers will help to establish new process requirements in order to increase the performance towards the desired level. The process model for this step is given in figure 32.

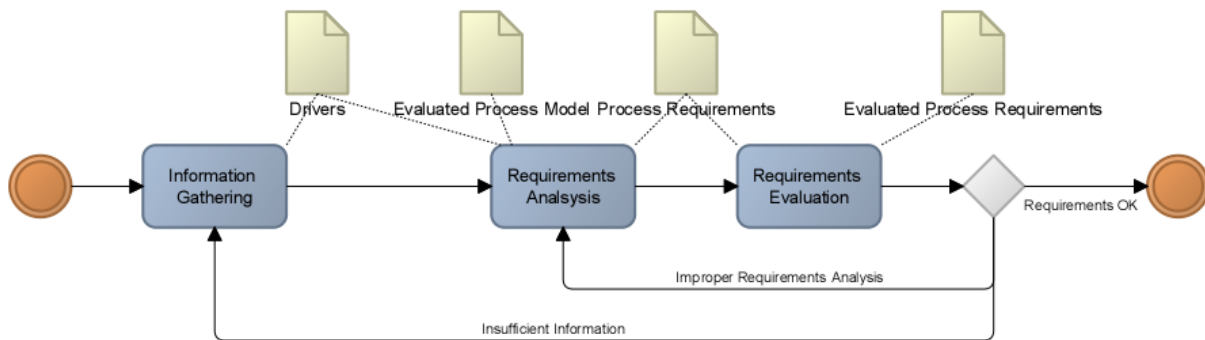


Figure 32. Process Model for the Process Requirements

### 10.4.1 Information Gathering

#### Approach

Before beginning to model the “to be” situation, it is important to first gather enough information about the drivers that initiated the redesigned process. Therefore one should again first focus on consulting experts that are involved in the business process design project that is being performed or about to be performed. These experts might already have assessed redesign alternatives based on exploratory analysis of the current situation. In order to do this they have already acquired driver information and analyzed the performance of the “as is” situation, since they need this to base the redesign decisions on. Therefore they may already have performed a driver analysis themselves. Process owners could be consulted as well.

#### Method

*Consulting experts:* Experts that have already initiated the project or are about to initiate it in the future are likely to have already gathered exploratory information about the process that has to be transformed. They also have access to internal documentation that helps to create an overview of the process and may even already have done a driver analysis themselves.

If they do not have a clear view about the drivers for business process redesign yet, because the project for example just started, one should consult the process owners of the current process identified earlier. They know the performance of the current process and they know what the expectations for the future process are. However they may not have such a good view about drivers of external parties and therefore it is always important to consult external experts.

#### Deliverable: Drivers

After consulting the experts, enough information should have been acquired to base a requirements analysis on. This information could include:

- *Driver documentation:* Documents that were already there, that describe in text what drivers are important within the process.
- *Slideshows based on exploratory interviews:* Drivers that are identified in exploratory meeting are often presented to the process owners by means of slideshows prepared by external experts.



- *Process models:* Process models that described parts of “to be” process themselves may already have been developed by external experts to present some ideas to the process owners. These process models reflect the implementation of drivers.

## 10.4.2 Requirements Analysis

### Approach

Now that the drivers for the business process redesign project have been identified, process requirements should derived from these drivers. This process is called the requirements analysis. Process requirements provide concrete aspects that should be met in the “to be” process. In order to model the “to be” process, one should therefore have a clear view of the requirements that have to be fulfilled by the “to be” process.

### Methodology

*Target Operating Model:* The methodology used by Deloitte to gather requirements is Target Operating Model, which is shown in figure 33. This methodology however is much broader then process requirements analyses alone. This methodology prescribes to take the current situation as input and to look at different drivers and translate them to requirement for a future situation on different levels, for example the product and services level which tells what products should be delivered, the process level which describes how the process should look like, but also the information and technology level which describes how the underlying information architecture should look like and even the physical level which shows were certain hardware and buildings should be located.

This methodology therefore offers a complete solution for redesign of operations as a whole and it therefore looks at requirements on more levels then the levels we look in this methodology, but it includes the requirements on the levels we need, namely the process and Information and technology level. Therefore it could be used as a methodology to perform a requirement analysis.

*BiZZdesign Architect:* BiZZdesign Architect also offers a methodology for requirements analysis based on drivers from stakeholders. It uses the semantics defined in Archimate 2.1, which offers a best practice approach for performing a requirements analysis. We will briefly elaborate on the semantics, which are displayed in figure 34 and an example which is displayed in figure 35.

We use part of the Archimate 2.1 semantics, which are shown in figure 34:

- *Stakeholder:* represents a stakeholder with a certain process.
- *Driver:* represents a driver from one or multiple stakeholders regarding the performance of the process.
- *Assessment:* represents an assessment of the current performance related to the performance desired by the drivers. This is where the performance information from the “as is” information is needed.
- *Goal:* represents a goal in order to achieve the desired performance.
- *Requirement:* represents a requirement for the “to be” process in order to make sure that the goals are reached.

Within our methodology it important to derive process requirements that relate to the three levels within the process model as described above. Multiple requirements analysis methodologies can be used for this, as long as they produce the requirements for the three levels. Since the Target Operating Model used by Deloitte and BizDesign (Archimate 2.1) do

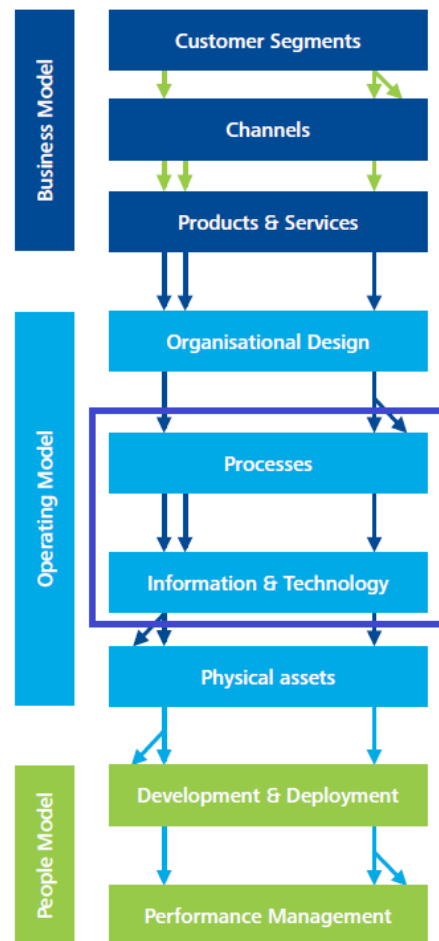


Figure 33. Target Operating Model Based on: Deloitte Resources

this, these could be tools to be used within the methodology. However other tools that are found suitable can be used as well.

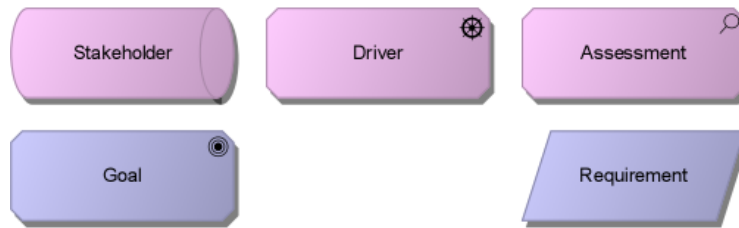


Figure 34. Archimate 2.1 Requirements Analysis Semantics

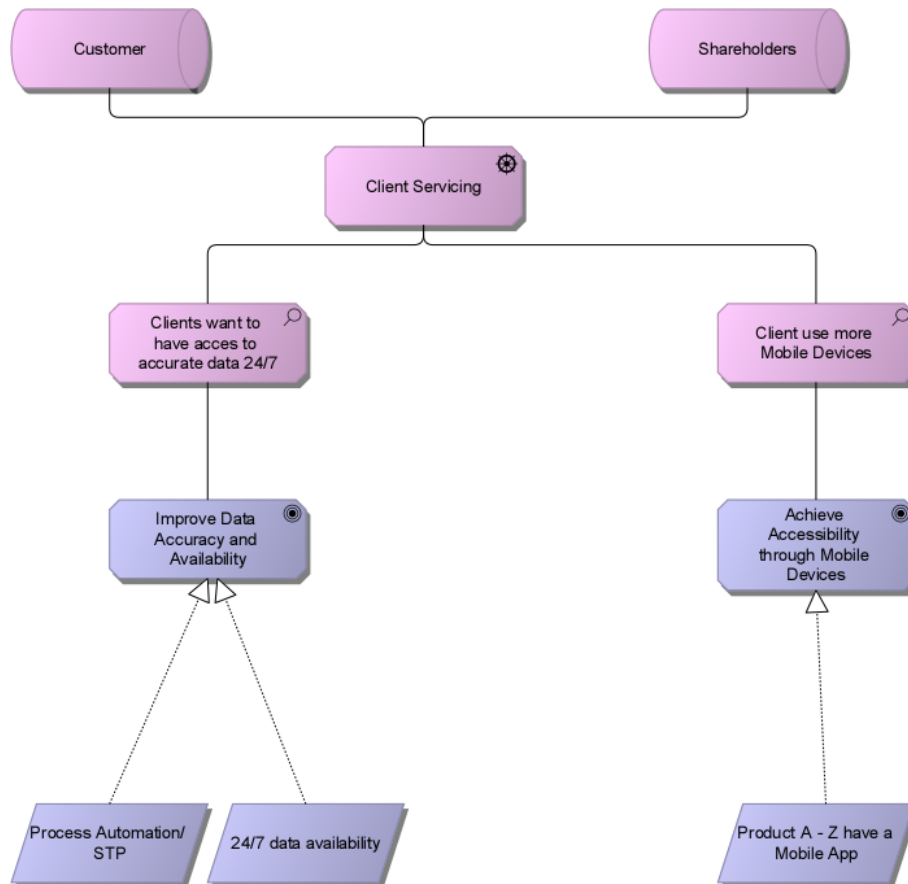


Figure 35. BiZZdesign Requirements Analysis Example

*Deliverables: Representation of Process Requirements and their Drivers*

At the end of this step a representation of the process requirements and their related drivers should be made, such as the example in figure 35. This representation will serve as input for the evaluation session that follows to make sure that all requirements are captured. A list of the requirements and a more detailed description can also be made in order to provide more information on each requirement.

10.4.3 Requirements Evaluation

*Approach*

Both the BiZZDesign requirements analysis and the process requirements spreadsheet provide a central document for expert evaluation. The evaluation of requirements is an important step, since the “to be” situation will be based on these requirements. Therefore it is important to make sure that the requirements derived are agreed on by all experts. The requirements are evaluated for two reasons:

- *Correctness*: Are the requirements derived correctly from the drivers during the requirements analysis?
- *Completeness*: Is enough information gathered to properly execute a requirements analysis?

In both cases, an iterative approach is needed. One or two of the previous phases have to be conducted again. The requirements analysis might have to be performed again in a more extensive manner, or even new information has to be gathered before performing the requirements analysis again.

*Method*

*Consulting Experts*: Especially external experts are of great value here, since they are the experts within process transformation based on previous experiences. It is therefore important to discuss the results of the requirements analysis with them, in order to identify missing or redundant requirements or to improve existing ones.

Creating representations like the two mentioned above also serves as a tool to link certain redesign decisions back to requirements and therefore back to their drivers. By doing this, there can be made sure that all drivers are sufficiently translated into the process model. The Target Operating Model mentioned earlier in this section also specifically links drivers to requirements and consecutively to design decisions. Therefore the idea of the representations we just discussed is more or less incorporated in this methodology. But because representation is an important aspect within this methodology and it could be possible that other requirements analysis methodologies do not prescribe to make one, we want to emphasize the creation of such a representation by means of adding it as a specific aspect within this methodology.

*Deliverable: Evaluated Process Requirements*

The deliverable should be a final overview of the evaluated process requirements. These evaluated process requirements are agreed on by all consulted experts and are therefore a rigid input for the design of the “to be” process.

### 10.5 Modeling the “to be” Situation

Lin et al. (2002) describe that it is important to represent the “to be” process in order to evaluate it against the “as is” situation. In this method this means that the risks and therefore controls within both situations are compared. This step is about visualizing the “to be” process by means of process modelling, which has also been done for the “as is” situation. The process model for this step is given in figure 36.

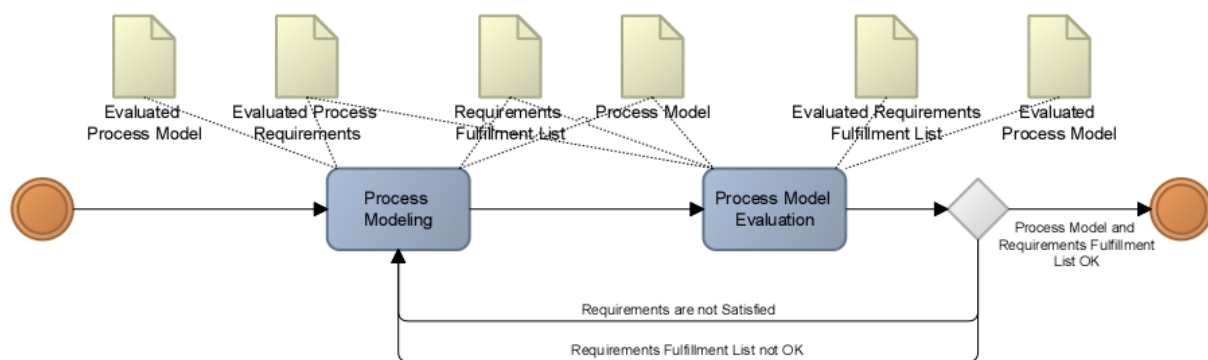


Figure 36. Process Model for Modeling the "to be" Situation

#### 10.5.1 Process Modeling

*Approach*

The requirements gained within the previous step as well as the process information acquired by modeling the “as is” situation can now be used together to design the “to be” situation (Larsen and Myers, 1999). However, requirements can be given shape in numerous forms. Therefore there is no single “to be” situation, but multiple alternatives based on different design decisions.

The process of BPR is an iterative process as can be seen in the literature about BPR (zur Muehlen and Ho, 2006). Certain design decisions are expected to produce a certain performance and impact the implementation of future design decisions

since the BPR is part of the bigger business process management lifecycle. A decision within one aspect influences other aspects as well. Therefore it might be very well possible that one design decision limits the alternatives for a future design decisions. The implementation of system A for example, may cause the choice for application B, since application C cannot be supported by system A. One redesign decision may therefore influence other redesign decision.

Since the BPR process is already initiated or about to be initiated, it may be well possible that a possible “to be” situation is already designed. In this case, one should find out what redesign decisions are made according to the process requirements and where these redesign decisions can be found implemented in the design of the “to be” situation. Concretely this means that a process model of the design should be made in elements within it should be traced back to the redesign decisions made.

## *Method*

*Linking Requirements to Redesign Decisions with Experts:* it is important that before the redesign decisions are being modelled, the alternatives are evaluated. Requirements can be fulfilled by different redesign decisions. It is important to acquire an overview of the requirements and the redesign decisions that will fulfill these requirements. A redesign decision may also be based on multiple requirements. This redesign decision then fulfills the need expressed in multiple requirements.

Experts need to be consulted to identify and evaluate the different alternatives. Preferably these experts have experience of previous BPR projects and therefore know how different redesign decisions can fulfill requirements. Therefore it is recommended to incorporate experts within this step. Brainstorming with them will show what redesign decision fulfills each requirement.

In case a design for the “to be” situation is already made, experts should be consulted to find out what redesign decisions were made and where the implementation of these redesign decisions can be seen in the designed “to be” situation.

*BizzDesign Architect:* The “to be” situation based on the redesign decisions determined will have to be modeled in order to base further risk assessments on, as well as enabling experts to evaluate the redesign decisions. If a design of the “to be” situation is already made, this design should be modelled in order to link already made redesign decisions to certain process elements. The tool we propose for this process modeling is the same as proposed for modeling the “as is” situation. Using the same tool will enhance the comparability of both situations and it experts involved in previous steps will have experience with “reading” the process model. The reason we choose for this modeling tool is already elaborated on in the first step.

## *Deliverable: Process Model and Requirements Fulfillment List*

*Process Model:* One deliverable should again be a process model, but this time for the “to be” situation. Because there are several alternatives to implementing the process requirements as discussed above, multiple process models can be created. Another option is to model different design decisions within one model, but we do not recommend this because it will add unnecessary complexity to the process model. If a design of the “to be” situation is already made, this design should be modelled.

*Requirements Fulfillment List:* The second deliverable should be a list stating redesign decisions and the requirements they fulfill. This list should refer to the model and we therefore recommend that redesign decisions are described in terms of process elements implementing the decisions. If the redesign decision means that process elements in the “as is” situation need to be transformed, these process elements should be listed as well. An example for one requirement is given in table 13. This list enables later linkage of shift in controls to redesign decisions. The format used is:

- *Design Decision:* Description of the design decision made in the “to be” process design in order to implement the requirement(s).
- *Requirements:* The requirement(s) that is/are fulfilled by the redesign decision.
- *Fulfilled by Process Elements in “to be”:* The specific elements in the process by which the redesign decision is fulfilled. This can either be a process step itself, the information technology supporting the business process step, or a combination of both. The elements can also be shown a process model.

- Fulfilled by Process Elements in "as is"*: The specific elements in the process that are transformed in order to fulfill the redesign decision. This can either be a process step itself, the information technology supporting the business process step, or a combination of both. If no "as is" process elements are transformed, this column is left empty. The elements can also be shown in a process model.

Table 13. Requirements Fulfillment List Example

Redesign Decision	Requirement	Fulfilled by Process Elements in "to be":	Transformation of Process Elements in "as is":
All customer activities can be done using an online application.	Customer can perform the whole process online	Online Application A, Online Application C, Online Application B, System A, System B, System C, Database A, Database B, Database C	Application A, Application B, System A, System B, Database A, Database B
	Customer can see his data online.		

### 10.5.2 Process Model Evaluation

Now that the "to be" process has been modeled it important to evaluate it (Kueng and Kawalek, 1997). This is done by assessing if the requirements derived in the previous steps are sufficiently satisfied by the process modeled. This also means evaluation of the created requirement fulfillment list. When this is not the case, the process needs to be remodeled.

#### Approach

The approach should be the same as described in 10.1.2.

#### Method

The method should be the same as described in 10.1.2.

#### Deliverable: Evaluated Process Model and Requirement Fulfillment List

*Evaluated Process model*: should be the same as described in 10.1.2.

*Evaluated Requirement Fulfillment List*: The list should be evaluated for completeness and correctness. Also when changes are made to the process model, the requirements fulfillment list has to be changed accordingly.

### 10.6 "to be" Situation Risk Analysis

The sixth step is the "to be" situation risk analysis. After the "to be" situation has been modeled and different alternative redesign decisions are therefore made clear, it is important to assess the risks for these redesign decisions. This risk analysis is done the same way as the risk analysis was done for the "as is" situation. The process model for this step is given in figure 37.

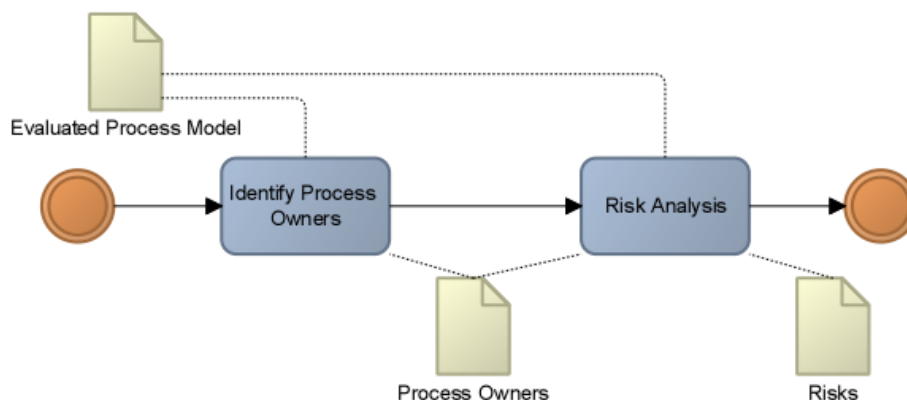


Figure 37. Process Model for the "to be" Situation Risk Analysis

### 10.6.1 Identify Process Owners

*Approach*

Process owners for the “to be” process have to be identified before risks can be identified. This is done in the same fashion as described in subsection 10.2.1. While it is most likely that the process owners have not changed, it can still be the case that new people are involved in the “to be” process because of the new design.

*Method*

*Consulting experts:* As stated before, experts may already have started to model the “to be” process based on the requirements. These experts may also have already identified the process owners within the process, which will become the risk owners as soon as risk occurs inside the aspects they are responsible for.

*Best practice databases:* Described in subsection 10.2.1.

*Field research:* Described in subsection 10.2.1.

*Deliverable: Process Owners*

The deliverable should be the same as described in 10.2.1.

### 10.6.2 Risk Analysis

*Approach*

*Risk matrix:* Described in subsection 10.2.2.

*Risk analysis session:* Described in subsection 10.2.2

*Method*

The method should be the same as described in 10.2.2.

*Deliverable: Risks in Risk Matrix and Risk Table*

The deliverable should be the same as described in 10.2.2.

## 10.7 “to be” Situation Controls Analysis

In the seventh step the risks that have been identified have to be linked to appropriate controls. This will be done by first categorizing the risks into the scoped risk categories and then performing a controls analysis in order to find controls to mitigate the risks. After that the costs of these controls is assessed. The risk appetite and the cost of controls are then used to select the controls that need to be implemented. The process model for the controls analysis is given in figure 38.

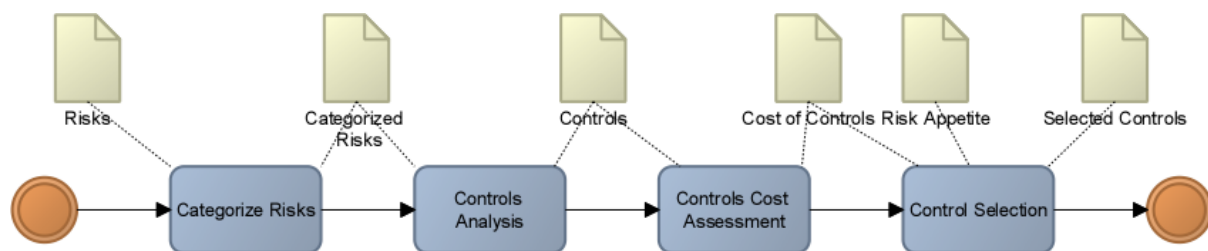


Figure 38. Process Model for the "to be" Situation Controls Analysis

### 10.7.1 Categorize Risks

*Approach*

As described in subsection 10.3.1 it is important to categorize the risks into the different risk categories scoped on within this methodology. By categorizing the risks into the risk categories the risk distribution within the process is visualized.

Based on this a comparison with the risk distribution within the “as is” situation can be made. This shift in risk distribution can provide extra insight into the shift in controls.

### *Method*

The method should be the same as described in 10.3.1.

### *Deliverable: Categorized Risks*

The deliverable should be the same as described in 10.3.1.

## 10.7.2 Controls Analysis

### *Approach*

Now that the risks within the “to be” situation have been determined and categorized, controls have to be assigned to these risks in order to make these risks manageable. As described in subsection 10.3.2, control frameworks serve as best practice frameworks to link controls to certain risks within an organization (Pederiva, 2003); (Rikhardsson and Best, 2006). Control framework describe certain control practices and their underlying control objectives, such as IT controls and their objectives as described within the CobIT framework.

Risk and controls registers can only be used here if certain process steps have remained the same in the “to be” situation. But since business process redesign is defined as the fundamental rethinking and radical redesign of processes resulting in dramatic performance improvement (Gunasekaran and Nath, 1997); (Al-Mashari and Zairi, 1999); (O’Neill and Sohal, 1999); (Khong and Richardson, 2003), it is most unlikely that process steps have remained the same. We therefore assume that in some cases only very little process steps have remained the same and that risk and controls registers are almost of no use within this task. Therefore another approach should be used within this task.

### *Method*

*Control frameworks:* Described in subsection 10.3.2.

*Risk and controls register:* Although this register is a list all current processes with their risks and the concurrent controls, this register could still be used for finding controls in the “to be” situation. Risks in the “to be” situation may be of the same nature as risks within the “as is” situation, or when risks have changed or new risks have emerged the risk and controls register may still provide valuable information that helps finding suitable controls. Therefore we recommend that this register is also consulted.

*Best practice databases:* Consulting companies often maintain databases of best practices based on past experiences in order to incorporate this experience in new project. Therefore overviews of possible risks and the controls to these risks are also kept within a database. Although these risks and controls might not be case-specific they provide valuable insight into the mitigation of the risks that have been identified within the “to be” situation.

Table 14 gives a simplified overview of such a best practice database, linking risks to control activities. There is often no scoping on sub processes, since a higher granularity level is used. This is because of the fact that the data is a synthesis of past experiences.

Table 14. Best Practice Database Example Based on: Deloitte Resources

Service Area	Process	Risk Category	Risk Description	Control Objective	Control Activity	Control Frequency	Control type (Automated/Manual)	Control Type (Preventive/Detective/Corrective)
Primary Services	Mortgage Provisioning	IT	The risk that client enters wrong data format.	Right data format is entered.	System checks data format.	Adhoc	Automated	Detective
Primary Services	Mortgage Provisioning	IT	The risk that the dossier is not saved.	Dossier is saved correctly.	System checks and sends notification to client.	Adhoc	Automated	Detective
Primary Services	Mortgage Provisioning	IT	The risk that the dossier is saved incorrectly.	Dossier is saved correctly.	System sends copy of saved data to client for double check.	Adhoc	Automated	Preventive
Primary Services	Mortgage Provisioning	Operational	Client registers invalid income and charges.	Income and charges are valid.	Bank employee performs a check on the income and charges.	Adhoc	Manual	Detective

*Consulting experts:* Having the knowledge of both control frameworks, risk and controls registers and best practice databases, using experts results in case-specific controls to the identified risks to be mitigated. Their experience in the field enables them to quickly transform high level best practice controls into controls that are applicable in the specific situation.

*Deliverable: Controls*

The deliverable here should be a set of controls. This set of controls can be a combination of controls derived from the sources mentioned above. For comparability reasons we recommend that they are listed and described in the same format that was described in subsection 10.3.2.

### 10.7.3 Controls Cost Assessment

*Approach*

The approach should be the same as described in 10.3.3.

*Method*

The method should be the same as described in 10.3.3.

*Deliverable: Cost of Controls*

The deliverable should be the same as described in 10.3.3.

### 10.7.4 Control Selection

*Approach*

The approach should be the same as described in 10.3.5.

*Method*

The method should be the same as described in 10.3.5.

*Deliverable: Selection of Controls*

The deliverable should be the same as described in 10.3.5.



## 10.8 Controls Shift Analysis

Internal control is a set of controls aimed at mitigated the risks within business processes and the transactions and information technology within these processes. (Neiger et al., 2006); (Rikhardsson and Best, 2006); (Zhang et al., 2007). The eighth and final step will be the determination of the shift in controls and therefore the assessment of the impact on business process redesign decisions on internal control. This will be done by using multiple sources of data created in the previous steps in a controls shift analysis. The process model for the controls shift analysis is given in figure 39.

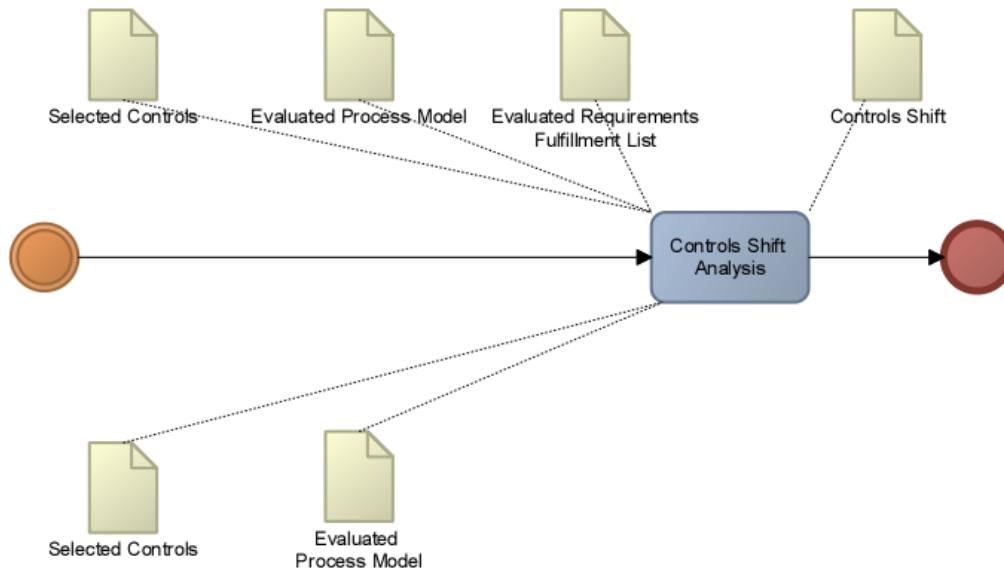


Figure 39. Process Model for the Controls Shift Analysis

### 10.8.1 Controls Shift Analysis

#### Approach

Now that we know the controls that are needed in both the “as is” and the “to be” situation, based on modeling both situations, analyzing the risks and linking these risks to controls, we can determine and visualize the controls shift between the two situations. The risks to be mitigated have been categorized for both situations, making a comparison between the risk distributions of the two situation possible.

#### Method

*Listing the controls needed in both situations:* Risks have been linked to risk elements and the requirements fulfillment list describes what elements are covered by a redesign decisions. Therefore a subset of controls tables of both the “as is” and “to be” situation can be made per redesign decisions. Table 15 and 16 give an example of possible control table subsets for the “as is” and “to be” elements covered by a redesign decision.

*Controls “as is” versus “to be” Table (with experts):* After the listing is done, a list of controls needed in both situations can be made as shown in table 17. When a control appears multiple times the amount of time changes. Control number 2 for example is needed in both situations, but in the “to be” situation it is needed two times which increases the time factor. However since a qualitative scale is used, the time factor of risks occurring multiple times cannot simply be added up. Therefore in case a control happens to be needed multiple times within a redesign decision, experts should be consulted to reassess the time factor. In the example the total amount of is assesses with a factor 4. Therefore we suggest the following semantics for the Controls “as is” versus “to be” Table, for both situations:

- *Control #:* Corresponds with the control number from the control table.
- *Control Activity:* A description of the control itself.
- *Control Frequency:* The frequency with which the control is carried out.

- *Control Type (Automated/Manual)*: The control is either carried out automated or in a manual fashion.
- *Control Type (Preventive/Detective/Corrective)*: Describes the type of control based the three different types of controls.
- *Final Cost*: Corresponds with the final cost of the control within the control table.
- *Total Final Time*: Corresponds with the final time of the control within the control table, in case the control occurs once. Otherwise a total final cost assessment has to be made with experts.

Furthermore can be seen in the example that control number 3 is needed in both situations the same number of times and control number 19 is needed as an additional control in the "to be" situation.

Table 15. "as is" Risk Elements Control Table Subset

Risk Category	ID	Risk	Risk Elements	Impact	Occurrence	Owner	Control Objective	Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Final Time
IT	1	Risk B	System A	8	5	Technical support manager	Mitigate Risk B	3	Control activity B	Ad hoc	Automated	Detective	3	2
Operational	4	Risk A	Activity A	6	6	Customer relationship manager	Mitigate Risk A	2	Control activity A	Daily	Manual	Detective	2	3

Table 16. "to be" Risk Elements Control Table Subset

Risk Category	ID	Risk	Risk Elements	Impact	Occurrence	Owner	Control Objective	Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Final Time
Legal	4	Risk H	Activity Z	4	2	Process Manager	Mitigate Risk H	19	Control Activity G	Weekly	Automated	Preventive	1	5
Operational	8	Risk C	Activity D	7	4	Customer relationship manager	Mitigate Risk C	2	Control Activity A	Daily	Manual	Detective	2	3
Operational	9	Risk D	Activity F	7	4	Customer relationship manager	Mitigate Risk D	2	Control Activity A	Daily	Manual	Detective	2	3
IT	10	Risk B	System A	8	5	Technical support manager	Mitigate Risk B	3	Control Activity B	Ad hoc	Automated	Detective	3	2

Table 17. Controls "as is" versus "to be"

"as is" Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Total Final Time	"to be" Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Total Final Time
2	Control Activity A	Daily	Manual	Detective	2	3	2	Control Activity A	Daily	Manual	Detective	2	4
3	Control Activity B	Ad hoc	Automated	Detective	3	2	3	Control Activity B	Ad hoc	Automated	Detective	3	2
							19	Control Activity G	Weekly	Automated	Preventive	1	5

### *Deliverable: Controls Shift Table and Controls Shift Matrices*

*Controls shift table:* Now the controls shift table can be created easily. This is done by eliminating the same controls that are needed in both situations at the same rate. In the example this means that control number 3 is eliminated. The results is the controls shift table as presented in table 18.

*Controls shift matrices:* Although the table provides a clear overview, we recommend that corresponding controls shift matrices are created for management and decision purposes. Figure 40 gives an example of how these matrices could look like. Representing data like this for both situations enables putting multiple dimensions of data into one clear overview, which can quickly be consulted in order to base decisions on. The semantics are as follows:

- *Cost of controls:*
  - *X-axis: Cost*
  - *Y-axis: Time*
- *Control:*
  - *Shape (Control type P/D/C):*
    - *Circle:* Preventive control.
    - *Square:* Detective control.
    - *Triangle:* Corrective control.
  - *Color (Control type A/M):*
    - *Green:* Automated control.
    - *Yellow:* Manual control.

The example shows that in the “to be” situation there are two controls instead of one in the “as is” situation. Also control number 2, which is in both situations, has increased in total cost of control because of the fact that the control is performed for a bigger amount of time.

Table 18. Controls Shift Table

"as is" Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Total Final Time	"to be" Control #	Control Activity	Control Frequency	Control Type A/M	Control Type P/D/C	Final Cost	Total Final Time
2	Control Activity A	Daily	Manual	Detective	2	3	2	Control Activity A	Daily	Manual	Detective	2	4
							19	Control Activity G	Weekly	Automated	Preventive	1	5

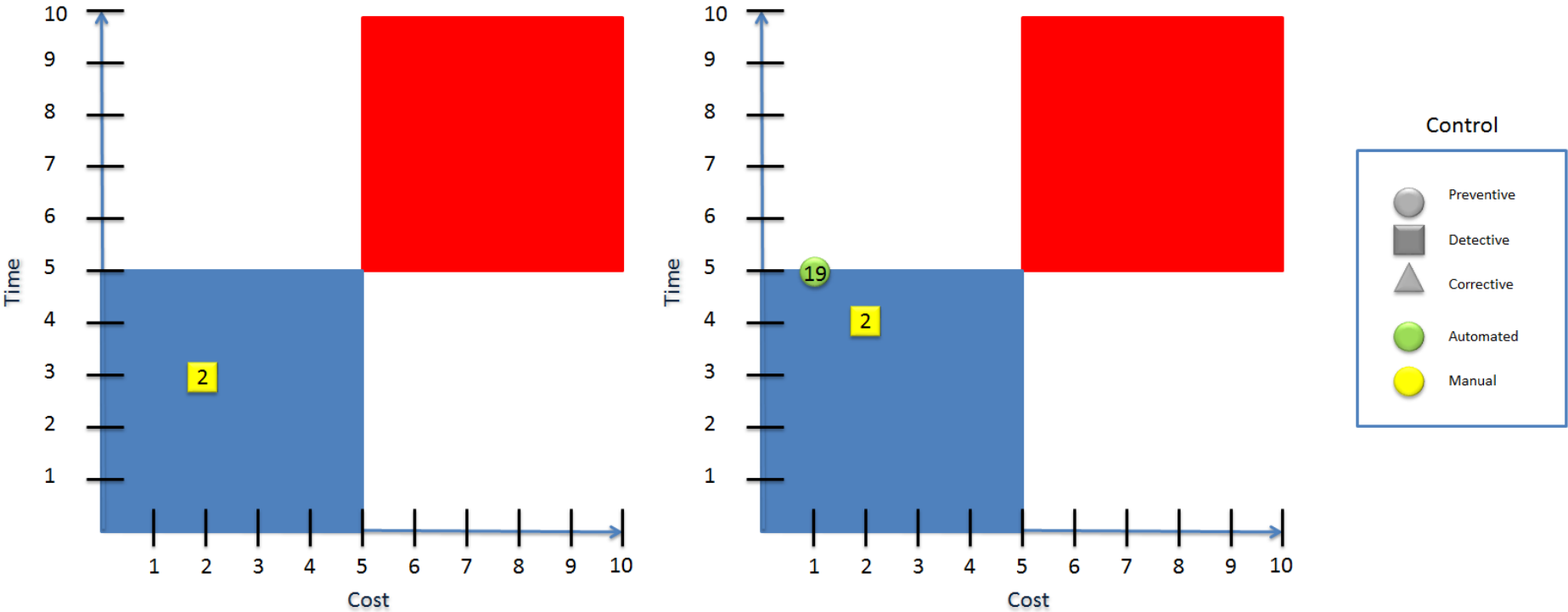


Figure 40. Control Shift Matrices

# 11 Demonstration

## 11.1 Introduction

In order to test the methodology for applicability and soundness, we will apply it within a demonstration. During this demonstration the methodology will be applied on a process in a real bank with the goal to demonstrate that the methodology goals can be reached by performing the different steps described within the methodology and that the steps deliver sound results. This demonstration is performed under close supervision and with close collaboration of internal experts within Deloitte. Information for this demonstration was also gained by consulting these experts and having brainstorm session with them. For confidentiality reasons, the bank used in the demonstration is called Bank. However the data used and the results reflect a real bank situation and should therefore be treated as such. Also because of time constraints and the limited availability of experts, several sessions were cut into smaller sessions in which a varying selection of experts participated.

The process studied in this demonstration is the mortgage provision process, from the initial orientation of the client to the actual acceptance of the tender. The reason this process is chosen is because a BPR project is currently performed for this project and Deloitte Risk Services has access to sufficient information about this project. Experts from Deloitte Consulting were also consulted, because of their involvedness in the project. They provided input regarding the process and the drivers and requirements for business process redesign.

The results of this demonstration will be evaluated by experts within Deloitte for their soundness and usefulness within future practice. This will be done during five evaluation interviews with colleagues from Deloitte Risk Services and Deloitte Consulting that are closely related to this research. Four colleagues from Deloitte Risk Services were interviewed, of which three were also closely involved in the demonstration. One colleague from Deloitte Consulting was interviewed, who was also closely involved in the demonstration.

**---- Confidential (General conclusions are given in de Conclusions Chapter. Corresponding Appendices E, F and G are also confidential) ----**

---

# PART 4 – RESULTS AND CONCLUSIONS

---

## 12 Discussion

This chapter discusses the relevant results of the research. This is done based on a discussion of the methodology goals and designed methodology in relation with the conducted demonstration with experts. For this discussion, four colleagues from Deloitte Risk Services and one colleague from Deloitte Consulting were given a presentation of the methodology and the demonstration and were consecutively interviewed. All of these colleagues, except one manager from Deloitte Risk Services, were actively involved in the demonstration itself. An overview of the interview questions and summarization of the answers per interview can be found in Appendix F. Evaluation Interview Overview.

In section 12.1 the research relevance in relation to the main research question is discussed, as well as the methodology goals formulated in order to base a methodology on that answers the main research question. In section 12.2 the goal regarding business process redesign and process modelling is discussed. Section 12.3 discusses the relevant results regarding the risk analysis by means of the associated goals. Section 12.4 discussed the relevant results regarding the controls analysis by means of the associated goal and the relevant results regarding the impact on internal control by means of the associated goal are discussed in section 12.5. Section 12.6 discusses the future potential of the methodology.

### 12.1 Research Relevance and Methodology Goals

There is a clear need for a structured approach to assess the impact of business process redesign decisions on internal control. All five experts agreed on this based on their experience in practice. They all note that financial institutions struggle with integrating business process redesign with risk management and compliance. Most financial institutions focus on being compliant and the laws and regulations related to compliancy. Process redesign is often also driven by compliancy and the risk related to this, but there is no integral approach towards internal control related to process redesign. Financial institutions often change their process first and afterwards take a good look at the change in risks and controls. This is too late. Another expert stated that there is attention paid to compliancy in business process change in some cases, but getting a clear view of the cost of controls is already a challenge and coupling this to business process redesign is a step that has not yet been made.

Integrating the concepts is seen as a unique selling point, since financial institutions have a great need for better internal control within their processes. It is valuable to assess what process redesign will mean for internal control, so that better decision can be done.

All experts also agree on the fact that a methodology based on these goals is adequate to give structure to this approach as a guideline. The goals describe all the aspects that are needed to integrate the different concepts. The concepts described within the goals are not essentially new but the linkage between them is. Therefore some of the experts also see a resemblance to work they currently perform within the goals. One expert stated that monitoring of controls should be a valuable addition to the goals but that it is not within the scope of this research. Two experts mentioned that although the goals describe all the needed aspects, the exact implementation of the goals is very important. Also the governance around and during the execution of the methodology is important, as is the timing. It is key to assure that high quality input is acquired to successfully achieve the goals.

When discussing the operationalization of the methodology goals within the proposed methodology a number of important findings was done:

- The steps are logically structured within the methodology. One expert stated that in practice the “as is” situation and the desired “to be” situation modelled first and then a gap analysis is made in order to determine the process requirements, but that this approach is logically structured. Another stated that sometimes both situations are analyzed for risks parallel, but since the redesign decisions are often not clear it is better to do it as described within the methodology.
- The goals of the various steps are in line with the listed goals e.g. achieving the goals of the steps results in achieving the listed goals.
- Two experts state that the offered methods and tools are sufficient to perform the associated task properly. One expert states that he is not entirely confident about the modelling method and tool, since he has not enough experience with it, but that the other methods and tools are sufficient. The two other experts state that some of the offered methods tools are not sufficient to perform the associated task properly. They express the need for:
  - More guidance to ensure quality of input by means of governance and timing of the methodology
  - Research towards the usage of the other risk categories
  - Research towards the possibilities of a qualitative scale.
- The recommended format or semantic for describing or visualizing the results is clear and sensible. However, one expert stated that the results can be expressed in a shorter fashion and two others stated that the quality of the results is more important than the way in which they are expressed. Also the detail level of the models is important. This has to be assessed per situation.

## 12.2 Business Process Redesign

The business process redesign is visualized within the methodology by means of modelling and requirements analysis. The first goal of this methodology refers to this:

**G1: Determining the “to be” situation by modelling the process through combining the “as is” process model with the information from the requirements analysis.**

This goal was found to be achieved within the research. The “as is” situation was modelled using the approach and method described and successfully evaluated by experts within the BPR project. Also the requirements analysis was conducted and successfully evaluated by the experts. The “to be” situation was modelled using the “as is” process model and information and the results from the requirements analysis as described in the methodology. The result was successfully evaluated by the experts, confirming this goal was reached. Therefore the visualization of BPR through process modelling argued by Kueng and Kawalek (1997), O’Neill and Sohal (1999) and Lin et al. (2002) was achieved.

However we do argue that the chosen method for modelling; BizDesign Architect (BizDesign, 2014) as tooling and Archimate 2.1 (The Open Group, 2014) as standard, could not be the only suitable method. Many more tools and standards exist, which could be used as well. BizDesign Architect was found to be restrictive by one of the experts, based on her experience during the demonstration. ARIS was proposed to be a suitable tool as well. Important requirements for a good tool are:

- Ability to drill down to actors and documents, by for example using coloring coding and timestamps
- Clear modelling of inputs and outputs

## 12.3 Risk Analysis

The second major aspect within the methodology is risk analysis. One goal was formulated with regard to risk analysis:

**G2: Identifying risks for both situations by performing a qualitative risks analysis, in which the process models serve as an input.**

This goal was also found to be achieved within the research. During the demonstration, risks were successfully identified in cooperation with experts during risk session, in which the created process models served as input. Risks were structurally linked to risks elements within the process model, making it able to plot the risks within the model. Both the risk table and the risk matrix could be made, since impact and occurrence were assessed by the experts. Although a certain detail level was used, experts were positive about the fact that the approach and methods described in the methodology could also be



used to identify risks on other detail levels. Given the time constraints most experts were confident that right risks were identified. The other experts stated that the quality of the analysis is very important, which means that for example the right experts are used and the right process owners are incorporated. This requires proper governance around the methodology.

However there were two shortcomings during the risk analysis. The first shortcoming is the fact that while process owners were successfully identified, they could not be incorporated in the risk analysis. Thus, their insights were not reflected in the risks identified. Secondly, however the goal states a qualitative approach, some of the experts mentioned that a quantitative approach could also be useful. Particularly, in this demonstration some risk groups were created because of time and space constraints. One could imagine that this is done more often in future usage of the methodology. When this happens and risk groups later have to be split up into various redesign decisions, one would greatly benefit from having quantitative values for impact and occurrence, making the splitting of risk groups easier.

When asked about the possibilities of a qualitative approach, experts agreed on the fact that this could be an addition to the methodology since it helps stakeholders and other involved people to better understand the ratings in terms of impact/occurrence and therefore prevents possible long discussions. However several experts noted that a qualitative risk assessment is still undeveloped and is therefore very hard to carry out. Therefore the general consensus was that a quantitative approach is best for the moment, although one could try to make things better understandable by means of quantitative labels etc.

## 12.4 Control Analysis

The third major aspect within the methodology is the controls analysis. Two goals were formulated with regard to this aspect:

**G3: Linking controls to the risks by using control frameworks as well as other best practice information and assessing the cost of these controls by means of a qualitative approach.**

This goal was also found to be achieved, since controls could successfully be identified and linked to the risk by using the prescribed semantics and by using best practices and consulting experts. The risk and controls register mentioned in the methodology was not used due to confidentiality concerns, but experts were positive that given the time available the relevant controls were identified efficiently. Again it was stated that the quality of the analysis is very important. This requires proper governance around the methodology. For example, implementation costs of systems that are needed to perform automated controls need to be passed on to the cost factor of these controls.

The cost of controls could also be assessed by means of a qualitative approach. Experts were consulted in order to do this because of their extensive knowledge based on future experiences, as proposed in the methodology. However, just as for assessing the impact and occurrence factor, experts made us aware of the fact that a quantitative would also have some advantages here. Although experts agreed on the fact that a quantitative approach is very hard, they stated that it would make communication of the costs towards the involved stakeholders easier. One expert provided the anecdote in which she stated *“Many people still think that double checking by another employee is safer than an automated process”*. Expressing controls and their costs and the shift of controls and their costs in quantitative values would help convince the people. Also we argue that when the same control is used more often in a redesign decision and the total cost and time needs to be assessed, it is easier to calculate with quantitative values than to make a new assessment based on qualitative values instead.

**G4: Determining a selection of controls to be implemented by combining the risks with their identified controls, the cost of these controls and the risk appetite, using a qualitative approach.**

Although this goal it was not extensively tested during the demonstration, because the risk appetite was set to 0 because both time constraints as the fact that the accountable process owner could not be consulted, the experts were positive about the approach within methodology. Therefore we argue that this goal was achieved. As a result of setting the risk appetite to 0, all identified controls were automatically selected as controls that had to be implemented. However, experts

stated that the controls to be implemented are selected in practice by performing table sessions in which the risks and their controls, the cost of these controls and the risk appetite serve as input.

This is the same approach as described in the methodology. One expert stated that having scored both the risks and their associated controls, combining this with the risk appetite would make selecting controls to be implemented possible. It was also noted by two other experts that it is often very hard to determine the risk appetite, since it is in practice very hard to determine the real accountable process owner. Process owners tend to push accountability towards other people and accountable process owners often have very little to say about the risk appetite since the pressure from internal and external authorities is very high.

## 12.5 Impact on Internal Control

The last major aspect within the methodology is the assessment of impact on internal control by means of visualizing the controls shift. This is the final results and deliverable of the methodology. One goal was formulated with regard to this major aspect:

**G5: Assessing and visualizing the impact on internal control by representing the controls of both the “as is” and the “to be” situation into one overview by using their cost and type.**

All experts agreed on the fact that this goal was achieved. By using the controls shift tables and the controls shift matrices a clear assessment and visualization of the controls shift was provided. One expert stated: *“I very much like the visualization”*. Experts also stated some minor point for improvement:

- One overview for the whole process in which all redesign decisions are mapped can maybe be made. This would provide more management information.
- The usage of the color green instead of blue and dividing the colors by one diagonal line from 10 to 10
- Providing a legend with the control numbers and their description
- Providing the redesign decision on the same sheet as the matrices

However, the legend and the redesign decisions are already in the methodology in the shape of controls shift tables and requirements fulfillment lists or models of the redesign decisions. Therefore one could use these to make a sheet of his/her liking. We also argue that providing one overview in which all redesign decisions are mapped is very hard because of the qualitative approach used. Transforming all controls with their cost and time factor into one dot on the overall matrix is difficult since the total or average factors cannot be calculated. This would require further assessments. Also information about the control types would be lost.

We have argued that a methodology that serves as a guideline based on these goals serves as an answer our main question:

**How can we assess impact of business process redesign decisions on internal control within banks?**

We have determined that there is a clear need for a structured approach to assess the impact of business process redesign decisions on internal control. All experts also agree on the fact that a methodology based on the five listed methodology goals is adequate to give structure to this approach as a guideline. Subsequently all five methodology goals are found to be achieved by the experts, which means that the methodology developed is adequate to serve as a guideline to assess the impact of business process redesign decisions on internal control within bank. Therefore our methodology serves as an answer to the main research question.

## 12.6 Future Potential

The experts named a number of strong points of the methodology:

- The methodology is thought through very well. It's not only a plan of action, it is well substantiated. The goals of the step substantiate the methodology goals. Aspects that are often looked at only a little are also present within the methodology, such as the process requirements.
- The end of the methodology is strong. We have never assessed and visualized the controls shift like this. If more people are made aware of this, we could surely make our clients aware of it.
- The methodology combines all the different aspects within one integral approach from front to end.
- Showing the difference between "as is" and "to be" controls is a very strong aspect of the methodology.
- The steps are ordered in a logical fashion and the methodology provides very much insight on the effect of redesign decisions you make.

Also a number of areas for improvement was given:

- More research towards a quantitative approach.
- More research towards the governance and timing of the methodology. The quality of data and analysis is important since carrying out the various tasks within the methodology based on bad quality data and analyses will still result in a bad assessment. Therefore governance and timing in the form of for example making clear who is responsible for carrying out certain tasks and when is important.
- More research towards the concrete execution of the various tasks (for example the tooling for process modelling).

The experts were asked for the future potential of the methodology in terms of usage and the added value for both Deloitte and the client. All of the experts agreed on the added value of the methodology. Most of the experts explicitly agreed on the added value for both Deloitte and the client. Furthermore a number of important findings were done:

- The methodology serves as an enrichment to the current methodologies used and offered. Therefore the methodology is a valuable addition to our portfolio.
- Through its various steps, the methodology helps constructively working together. In cases long cooperation of different people is needed the methodology can surely help since it forces people to work together.
- Various steps and concepts in the methodology are not new, but the linkage between concepts is. The methodology serves as a proper guideline.
- The methodology is a good starting point for discussion. It offers sufficient basis to develop it further into a concrete approach that can be applied at the client.

## 13 Conclusions

This chapter describes the conclusions of this research, based upon the methodology designed and illustrated in the demonstration and on the analysis of the evaluation meetings. The main research question is answered within this chapter. The main research question is:

**How can we assess the impact of business process redesign decisions on internal control within banks?**

In order to answer the main research question, the answers to the sub-questions are shortly described in section 13.1. The limitations of this research and suggestions for further research are discussed in section 13.2 and the contribution of this research to both theory and practice are discussed in section 13.3.

### 13.1 Research Questions

This research is based on a number of concepts all related to the main concepts of compliance, risk, internal control and business process management. Other literature talks about the main concepts of governance, risk management and compliance. These concepts form the basis of the methodology. These concepts are discussed in two groups in subsections 13.1.1 and 13.1.2. Firstly, management and compliance are discussed; this answers research questions 1,2,3,4 and 5. Secondly, business process management, business process redesign and the relation to risk management is discussed; this answers research questions 6, 7 and 8. Finally, in subsection 13.1.3 the methodology and its demonstration and the evaluation of the methodology and its demonstration are discussed, answering research questions 9 and 10.

#### 13.1.1 Compliance Risks and Internal Control

This subsection discusses the concepts of compliance, risk and internal control and the underlying concepts. Answers are provided on research questions 1, 2, 3, 4 and 5. These questions are:

1. What is compliance and what is the added value of being compliant?
2. What is risk and how can it be analyzed?
3. What is internal control and how does it contribute to mitigating risks?
4. What are controls and risk appetite and how do these concepts relate to internal control?
5. What are control frameworks and how does an integrated control framework ensure internal control?

In section 5.1 compliance and the added value of compliance are discussed.

*“Compliance is defined as ensuring that business processes, operations, and practice are in accordance with a prescribed and/or agreed set of norms. Compliance requirements may stem from legislature and regulatory bodies (e.g., Sarbanes-Oxley, Basel II, HIPAA), standards and codes of practice (e.g., SCOR, ISO9000), and also business partner contracts.” (Sadiq and Governatori, 2010)*

Sutinen and Kuperan (1999) describe different determinants of compliance, as shown in figure 60. Regulatory compliance is the compliance to existing regulations (Damania et al., 2004).

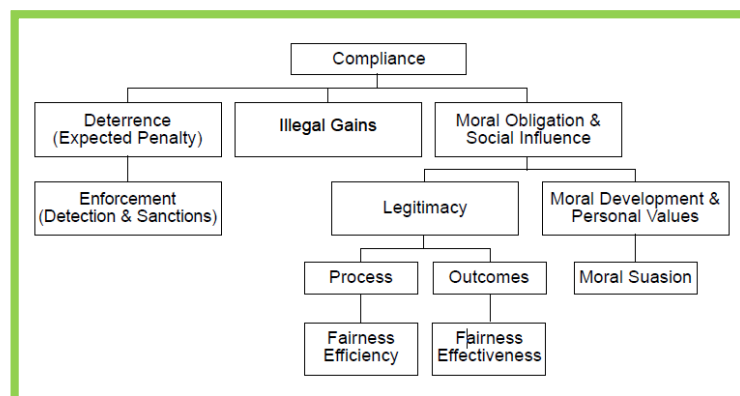


Figure 60. The Determinants of Compliance Source: Sutinen and Kuperan (1999)

Compliance has an added value because of several reasons:

- Compliance to certain laws and regulations is an opportunity to make business processes and operation more effective and efficient (Sadiq and Governatori, 2010) and therefore save costs.
- Being compliant to regulations ensures that certain risks are analyzed and mitigated.
- Compliance can serve as a competitive advantage, since it reflects responsibility and customers and investors are nowadays sensitive to this, because they do not want to be referred to as being irresponsible (Potoski and Prakash, 2005); (Lubin and Esty, 2010).
- The cost of being non-compliant is expressed in penalties that banks receive when they are found not compliant. Big amounts of money are connected to these penalties. The fact that a bank does not have to pay these fines, because it is compliant, can also be seen as the added value of being compliant.

Section 5.2 discusses risk. The Project Management Institute defines risk as: *“an uncertain event or condition that, if it occurs, has a positive or negative effort on a project objective”* (Project Management Institute, 2000)

Risk can be seen as a deviation from how things are expected to go or perform. Lambert et al. (2006) describe that a risk assessment can be done through five steps:

- Risk identification
- Risk measurement
- Risk evaluation
- Risk acceptance and avoidance
- Risk management

Research by Kliem (2000) describes three ways to analyze risks. Quantitative risk analysis, qualitative risk analysis and a combination of both. Quantitative risk analysis uses mathematic calculations while qualitative risk analysis uses judgment as a primary basis to determine the relative importance of one risk to the others and the respective probability of occurrence. To determine the importance of a risk three questions have to be answered (Kaplan, 1997) (Kliem, 2004):

- What can happen?
- How likely is it to happen? (Occurrence)
- If it does happen, what are the consequences? (Impact)

A widely use visualization tool to map this risk importance is the risk matrix, which is also elaborated on in documents of Deloitte (Curtis and Carey, 2012); (Institute of Conflict Management, 2013). It combines the frequency of occurrence on the X-axis with the impact on the Y-axis. Figure 61 gives an impression of a risk matrix.

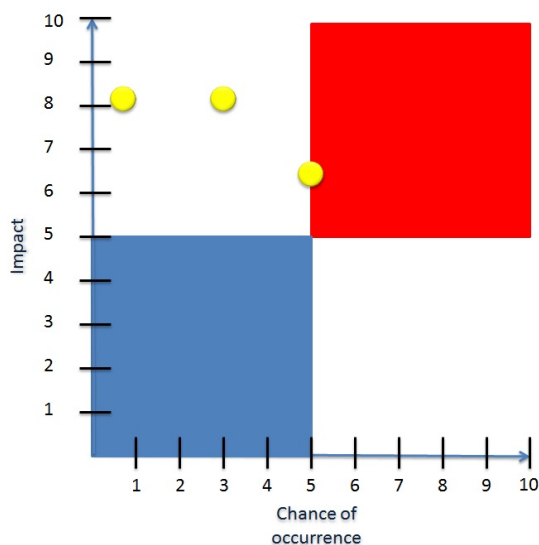


Figure 61. Risk Matrix

Section 5.3 and 5.4 elaborate on internal control and the concepts of controls and risk appetite and their relation to internal control. Internal control is a system aimed at assessing, minimizing and controlling risk associated with company business processes, business transactions, information technology applications and information dissemination to internal and external decision makers (Neiger et al., 2006); (Rikhardsson and Best, 2006).

The focus on internal control has grown quickly in the last years, due to the fact that new laws and regulations require banks to report on their internal control (Hermanson, 2000). The Sarbanes-Oxley Act (SOX) is an example of this. This act mandates internal control (Zhang et al., 2007); (Ashbaugh-Skaife et al., 2008). Assuring that there is enough internal control is done through auditing by external parties (Ashbaugh-Skaife et al., 2007); (Ashbaugh-Skaife et al., 2008).

Aligning control objectives that stem from laws and regulations with business processes in order to mitigate risks is a major challenge for organizations (Sadiq and Governatori, 2010) and especially for banks, since they operate in a highly regulated industry (Breux et al. 2004). Figure 62 shows this process. Control objectives prescribe that certain risks should be mitigated. This mitigation asks for internal control, which in turn is interrelated with the tasks within business process structure that is in place. Business processes models describe how certain tasks are carried out and how tasks are interrelated. These business processes in turn often need information system support, which also impact internal control the use of information systems may determine whether controls are being automated or not and internal control also needs to cover the information systems.

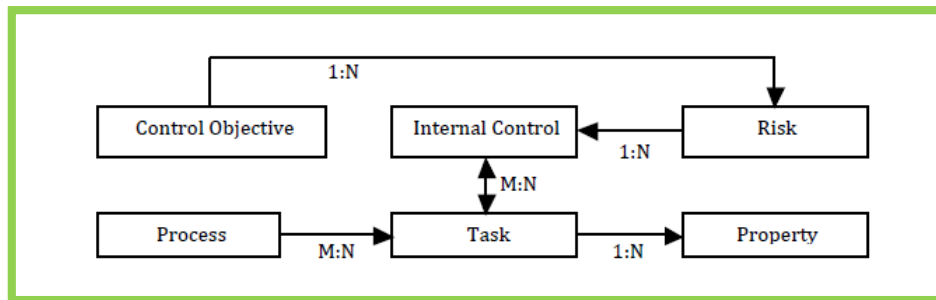


Figure 62. Relationship between Process Modeling and Internal Control Source: Sadiq and Governatori (2010)

Figure 63 shows how a control objective is translated into one or multiple controls, which together with other controls comprises the internal control environment. The internal control environment is a set of controls (Ge and Mcvay, 2005), stemming from the control objectives.

Control Objective	Internal Control
Customer due diligence	All new customers must be scanned against provided databases for identity checks. Accounts must maintain a positive balance, unless approved by bank manager, or for VIP customers.
Record keeping	Retain history of identity checks performed.

Figure 63. Control Objective and Related Controls Source: Governatori and Sadiq (2009)

Figure 64 shows the risk universe, the risk tolerance and the risk appetite. The risk universe contains all the risks within the environment of an organization. The risk tolerance is the amount of risk an organization might just be able to bear. An organization chooses a certain operating area within the environment and the risks within that area become the risks of the organization. Processes also have risk universe, these are all the risks that might be faced within a process. Process also has a specific risk appetite, which has to be established (Deloitte, 2014).

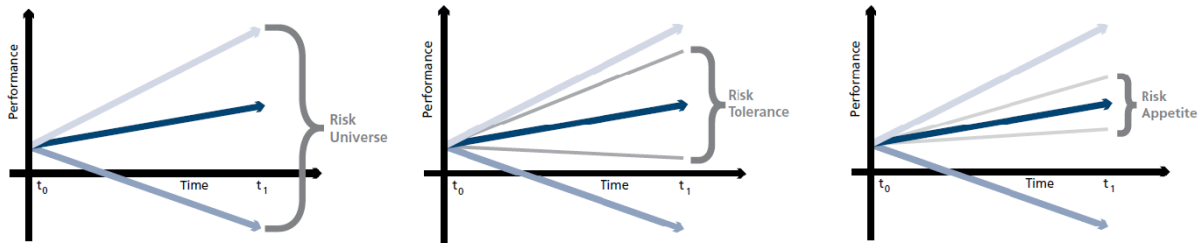


Figure 64. Risk Appetite Source: The Institute of Risk Management (2011)

The risk appetite is the extent in which the organization is willing to take risks (Power, 2009). The risk appetite may shift over time, because of changing uncertainties (Gai and Vause, 2005) and depends on two factors:

- *Risk aversion*: The intrinsic makeup of investors and other people finally responsible. (Danielsson, 2010); (Dungey et al. 2003); (Adrian et al. (2009).
- *Macroeconomic environment*: Uncertainties within the environment of the organization, such as financial distress and laws and regulations.

The amount of risk should be within this risk appetite (zur Muehlen and Ho, 2006). The risk appetite is normally smaller than the risk tolerance, since organizations always want or have to mitigate a certain amount of risk. The amount of risk a company wants to mitigate can be determined using an equation shown in figure 65. The risk universe consists of risk appetite and the amount of risk to be mitigated. Risk mitigation is done by putting controls in place. Therefore by using this equation, the needed controls can be determined.



Figure 65. Risk Universe Equation

Controls are a way to help a corporation achieve its objectives, such as producing accurate financial reports, despite the presence of threats (Panko, 2006). Controls are put in place as measures to mitigate the risks that are identified and labeled as risks that have to be mitigated, using the equation described above. There are three types of controls according to Bass and Robichaux (2001), Kliem (2000); (2004), Cavusoglu et al. (2004), Kartseva et al. (2004) and Panko (2006):

- *Preventive*: mitigate the impact of a risk or stop it before having impact. Deviations are prevented from occurring.
- *Detective*: Deviations are detected so that action can take place.
- *Corrective*: determine the impact of a risk and establish measures to preclude future impacts. Deviations have occurred and have to be fixed.

Section 5.5 discusses control frameworks by elaborating on two widely used frameworks; COSO and CobiT. COSO is a control framework that is widely used for financial reporting control (Hermanson, 2000); (Rikhardsson and Best, 2006) since the introduction of the Sarbanes-Oxley act, which requires financial institutions to use a control framework to evaluate internal controls. The CobiT (Control Objectives for Information Related Technology) framework (Tuttle and Vandervelde, 2007), links risk management practices to business processes as well as to internal control (Pederiva, 2003); (Rikhardsson and Best, 2006). It helps organizations balance their IT risk and investments in control.

While COSO is very often used within organizations like Deloitte to serve as a structural guide for internal control assessment, CobiT is more or less a control framework that is used to implement some of the steps that are described in COSO. But on its turn, it does not describe how for example decision-making structures should be implemented and controlled (Simonsson and Johnson, 2006). This is how the integrated control framework is built up by Deloitte Risk Services. It serves as an integrated approach to assess of organizations are in control of their processes.

### 13.1.2 Business Process Redesign

This subsection discusses the concept of business process management and more specifically business process redesign and its relation to risk management. Answers are provided on research question 6, 7 and 8. These questions are:

6. What are the main drivers for banks to redesign their processes?
7. What is business process redesign?
8. What is the relation between business process redesign and risk?

Chapter 6 discusses the various drivers for bank to redesign their processes. This is done using the stakeholder point of view. The drivers stem from pressure of financial authorities, shareholders, customers and competitors. The drivers are:

- Efficiency
- Transparency
- Client servicing
- Compliance to laws and regulations

Chapter 7 elaborates on business process redesign and its relation to risk management. Business process redesign (BPR), or Business Process Re-engineering (Larsen and Myers, 1999), is defined as the fundamental rethinking and radical redesign of processes resulting in dramatic performance improvement (Gunasekaran and Nath, 1997); (Al-Mashari and Zairi, 1999); (O'Neill and Sohal, 1999); (Khong and Richardson, 2003). It is about redesigning existing business processes and implementing new ones (Earl et al., 1995) and it requires “out of the box” thinking to explore things outside what has been done before (Grover and Malhotra, 1997). It therefore improves cost efficiency, speed, productivity, competitiveness (Attaran, 2004) and service effectiveness (Abdolvand et al., 2008).

Figure 66 shows the major elements of BPR when using information technology to improve client servicing. Information technology is seen as (one of) the most effective enabling technology for BPR (Grover and Malhotra, 1997); (Gunasekaran and Kobu, 2002); (Teng et al., 2008); (Attaran, 2004). While this case talks about simplification and standardization as major process restructuring aspects, our research focuses more in real-time information accessibility etc.

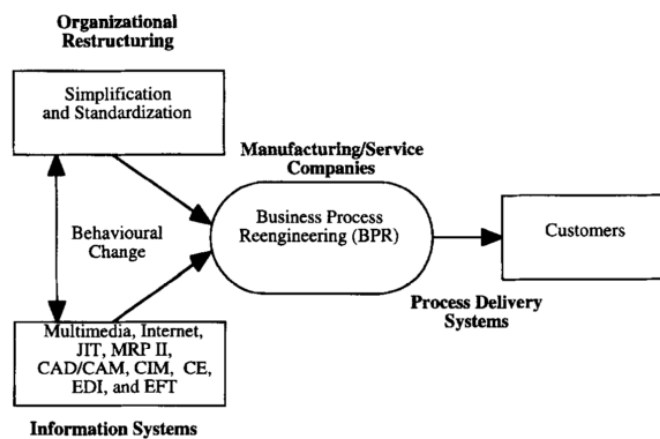


Figure 66. Major BPR Elements when using IT to Improve Client Servicing Source: Gunasekaran and Nath (1997)

BPR is part of a bigger cycle, the Business Process Management (BPM) cycle. Figure 67 shows this cycle. The inner cycle is that of the design, implementation, enactment and evaluation of the process. Goals and process monitoring deliver new input for the process. This research focuses on specific drivers for banks, which serve as goals within this overview. These drivers demand the process to be redesigned. But drivers also serve as process monitoring, since laws and regulations pose certain requirements on the process that have to be monitored.



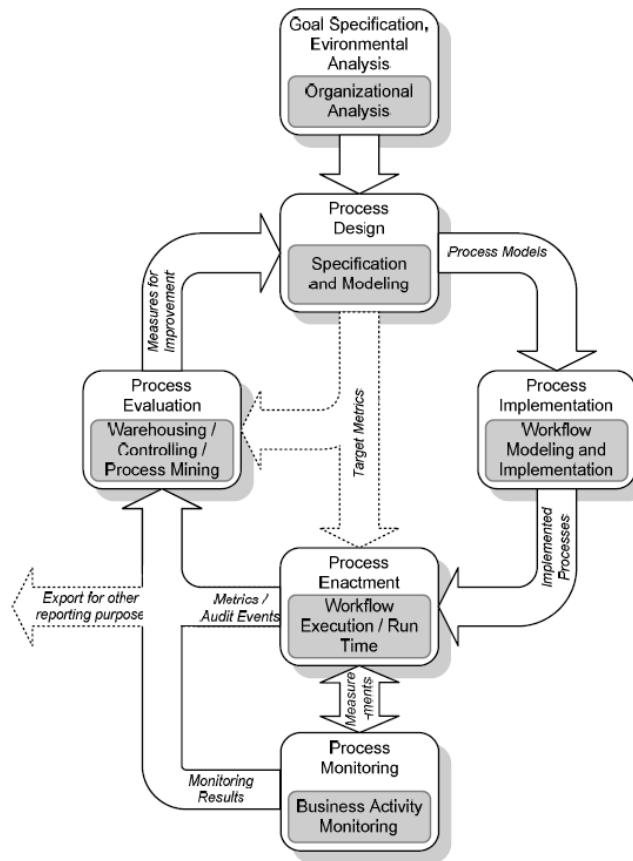


Figure 67. The Business Process Management (BPM) Lifecycle Source: zur Muehlen and Ho (2006)

The research of Khong and Richardson (2003) tells us that while a number of BPR projects fail (Grover and Jeong, 1995), the organizational improvements in cost reduction, better client servicing and increased speed are evident. An important factor in the process of redesigning processes is the evolution of information technology (Shin and Jemella, 2002). New information technologies enable certain process steps to be done faster and more efficient, or even automatically. Manual steps in the process can now be done automatically by machines and information systems.

Business process redesign consists of four different steps that have to be taken (Shin and Jellema, 2002): Energize, focus, invent and launch. Within the invent step it is important to analyze different design decisions in the context of the requirements (Larsen and Myers, 1999) and to analyze what impact certain redesign decisions will have on risks. Redesigning certain process steps will often result in shifting risks, because risks are coupled to certain process steps. Doing these steps differently or replacing them with new steps, will also mean that risks will change or new risks will occur. Consecutively, the controls to mitigate these risks will also change. New controls will have to be implemented or existing controls will have to be updated.

O'Neill and Sohal (1999) wrote a literature review about BPR, also summarizing a number of techniques that are commonly used in BPR, stating that the focus of a BPR project should be on the outcome and not on the tasks themselves:

- *Process visualization*: Model the end state or vision of the process. It will serve as a goal to work towards.
- *Process mapping/operational method study*: Use tools of operational method studies for reengineering tasks.
- *Change management*: Focus on the human side of reengineering. Managing the change is the largest task.
- *Benchmarking*: Compare your process with processes within other organizations to develop a goal.
- *Process and customer focus*: The primary aim of BPR is to redesign processes with regard to improving performance from the customer perspective.

Based on these insights it might be concluded that in order to perform BPR it is important to visualize the “to be” situation, in order to determine how to move to this situation with the “as is” situation as a starting point. This is also supported by Lin et al. (2002) who state that visualization through business process modelling serves two important purposes:

- Capture existing processes and structurally representing them
- Represent new processes in order to evaluate them

There are multiple techniques to visualize the “to be” situation, of which process modeling (Kueng and Kawalek 1997) is a prominent one. Important other techniques that should be kept in mind are change management, benchmarking and a customer (Motwani et al., 1998) and process focus.

### 13.1.3 Design

This subsection discusses the methodology and its demonstration and the validation of the methodology and its demonstration. Answers are provided on research questions 9 and 10. These questions are:

9. Can we define a methodology to assess the impact of various business redesign decisions on internal control?
10. What is the impact of various business process redesign decisions on internal control within the mortgage provision process?

In chapter 8, based on the literature study a research model was created, which is shown in figure 68. Then a mapping of the read and analyzed literature was done on the concepts forming the research model. The method for doing this is described by Webster and Watson (2002). The resulting concept matrix indicates the importance of this research.

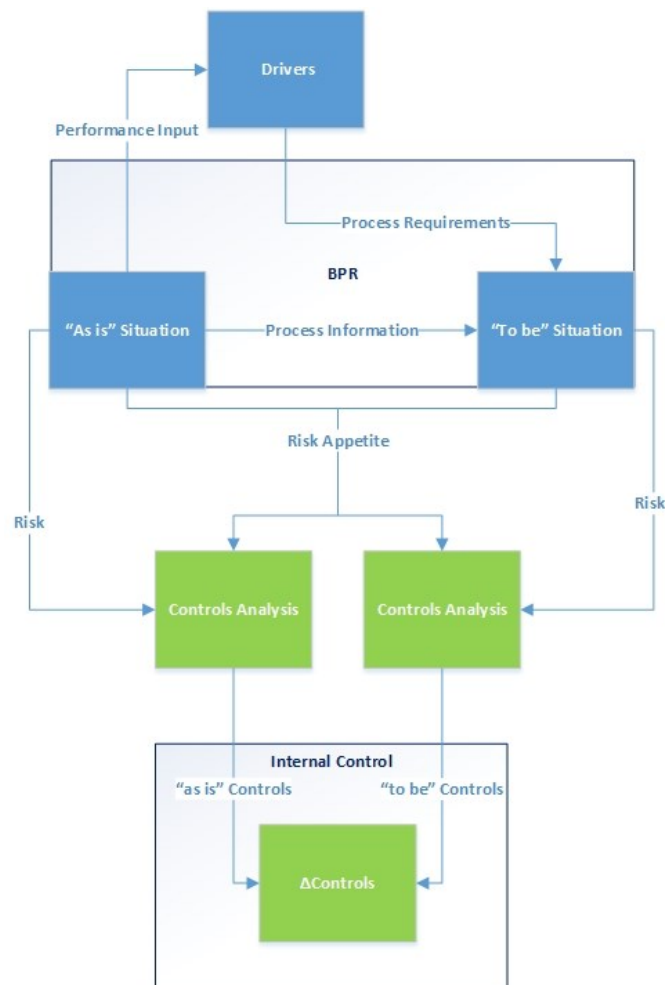


Figure 68. Research Model

The findings derived from the concept matrix suggest that more research towards a comprehensive and complete methodology is needed in order to assess the impact of Business Process Redesign decisions on internal control. Based on the research model a number of methodology goals was formulated in chapter 9:

**G1: Determining the “to be” situation by modelling the process through combining the “as is” process model with the information from the requirements analysis.**

**G2: Identifying risks for both situations by performing a qualitative risks analysis, in which the process models serve as an input.**

**G3: Linking controls to the risks by using control frameworks as well as other best practice information and assessing the cost of these controls by means of a qualitative approach.**

**G4: Determining a selection of controls to be implemented by combining the risks with their identified controls, the cost of these controls and the risk appetite, using a qualitative approach.**

**G5: Assessing and visualizing the impact on internal control by representing the controls of both the “as is” and the “to be” situation into one overview by using their cost and type.**

These methodology goals were then operationalized in a detailed methodology description provided in chapter 10. The structure used to describe this methodology is based on a thesis written by Schepers (2007). An overview of the different steps within the methodology is given in figure 69. The methodology has eight steps:

1. *Modelling the “as is” Situation*: Creating a process model overview of the current situation.
2. *“as is” Situation Risk Analysis*: Identifying the scoped risks within the process.
3. *“as is” Situation Controls Analysis*: Categorizing the risks and determining what controls are needed based on the risk appetite determined.
4. *Process Requirements*: Transforming stakeholder drivers into process requirements for the “to be” situation.
5. *Modelling the “to be” Situation*: Creating a process model overview for a possible future situation.
6. *“to be” Situation Risk Analysis*: Identifying the scoped risks within the future process.
7. *“to be” Situation Controls Analysis*: Categorizing the risks and determining what controls will be needed based on the risk appetite determined
8. *Controls Shift Analysis*: Determining and visualizing the shift in controls between the “as is” and “to be” situation.

The methodology was then demonstrated in on a real bank example, in which the mortgage provision process was analyzed. This was done to demonstrate its applicability and soundness. The process is undergoing business process redesign and by applying the methodology several business process redesign decisions were assessed for their impact on internal control by means of controls shift. Chapter 11 gives a detailed overview of the demonstration and its results.

The general trend that can be seen in this demonstration is a higher total cost in IT risk related controls due to an increased control effort because of a bigger reliance on IT architecture reflected in one redesign decision and a decreased overall cost of control caused by the shift from relatively expensive manual and detective/corrective controls towards the relatively cheap automated and preventive controls reflected in the other redesign decisions. However no exact conclusions can be tied to these findings, since the cost and time factors are based on a purely qualitative scale.

The evaluation was based on a discussion of the methodology goals and designed methodology in relation with the conducted demonstration with experts. The discussion is provided in chapter 12. For this discussion, four colleagues from Deloitte Risk Services and one colleague from Deloitte Consulting were given a presentation of the methodology and the demonstration and were consecutively interviewed. All of these colleagues, except one manager from Deloitte Risk Services, were actively involved in the demonstration itself. During this evaluation a number of findings was done regarding the research relevance and methodology goals:

- There is a clear need for a structured approach to assess the impact of business process redesign decisions on internal control. All five experts agreed on this based on their experience in practice. They all note that financial institutions struggle with integrating business process redesign with risk management and compliance.

- All experts also agree on the fact that a methodology based on the five listed methodology goals is adequate to give structure to this approach as a guideline. The goals describe all the aspects that are needed to integrate the different concepts. The concepts described within the goals are not essentially new but the linkage between them is.
- When discussing the operationalization of the methodology goals within the proposed methodology a number of important findings was done:
  - The steps are logically structured within the methodology.
  - The goals of the various steps are in line with the listed goals e.g. achieving the goals of the steps results in achieving the listed goals.
  - The offered methods and tools are found sufficient to perform the associated task properly by two expert while one expert states that he is not entirely confident about the modelling method and tool. The two other experts state that some of the offered methods tools are not sufficient to perform the associated task properly. The express the need for:
    - More guidance to ensure quality of input
    - Research towards the usage of the other risk categories
    - Research towards the possibilities of a qualitative scale.
  - The recommended format or semantic for describing or visualizing the results is clear and sensible. However, one expert states that the results can be expressed in a shorter fashion and two others state that the quality of the results is more important than the way in which they are expressed. Also the detail level of the models is important. This has to be assessed per situation.

Consecutively it was discussed whether the five listed methodology goals were achieved, after which the future potential of the methodology was also discussed:

- All five listed methodology goals were found to be achieved by applying the methodology. Therefore the methodology is found to provide the structured approach needed to assess the impact of business process redesign decisions on internal control. However governance and timing of the methodology is an important aspect and more research should be conducted towards a quantitative approach. Also more research should be conducted towards the concrete execution of the steps and tooling for modeling.
- The methodology was found to have future potential. It serves as an enrichment to the current methodologies used and offered. Therefore the methodology is a valuable addition to our portfolio. Through its various steps, the methodology helps constructively working together. In cases long cooperation of different people is needed the methodology can surely help since it forces people to work together. Although various steps and concepts in the methodology are not new, but the linkage between concepts is. The methodology serves as a good guideline and is a good starting point for discussion. It offers sufficient basis to develop it further into a concrete approach that can be applied at the client. Therefore the methodology has added value for both Deloitte and her clients.

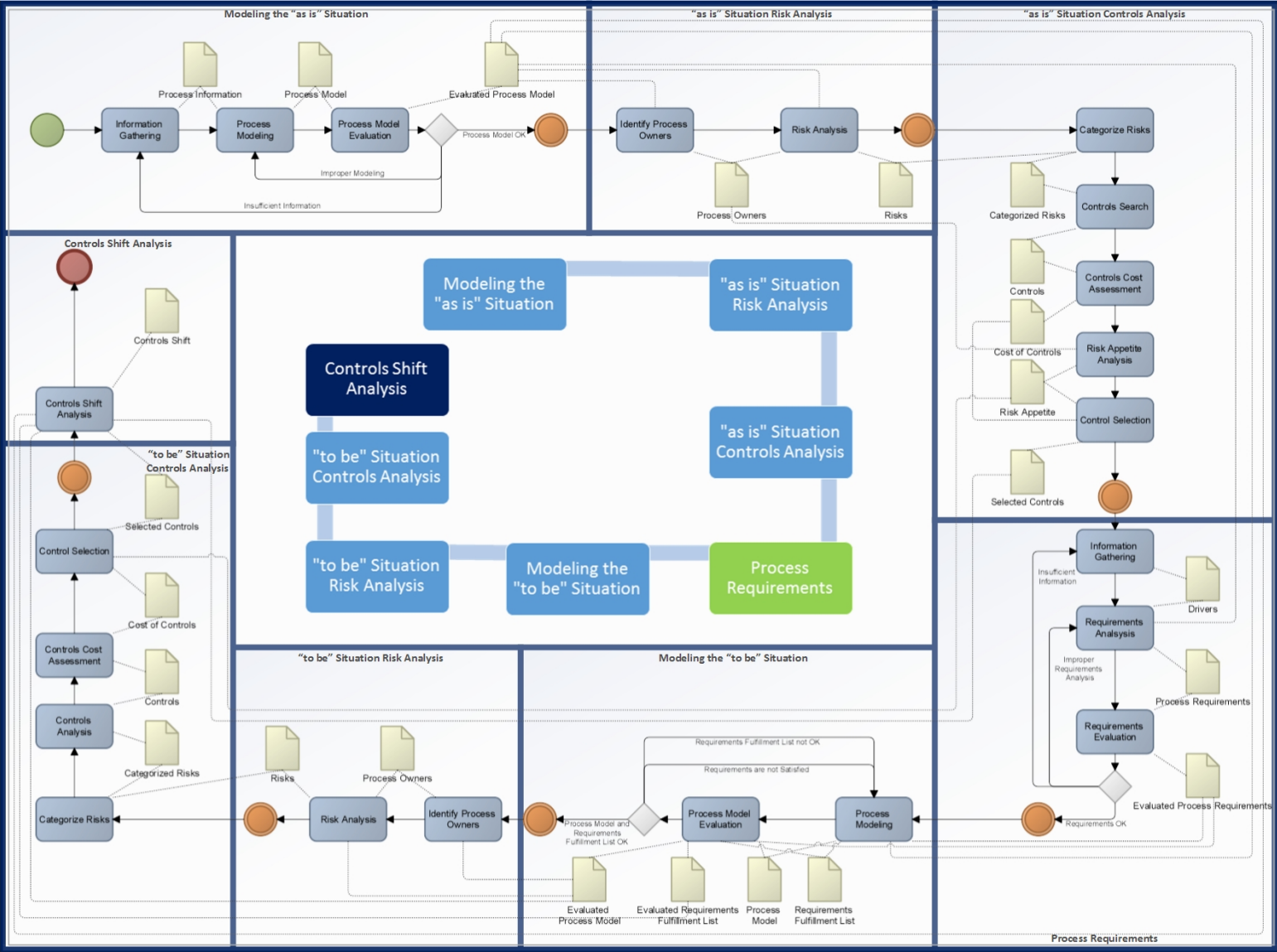


Figure 69. Methodology Outline

## 13.2 Limitations and Suggestions for Further Research

This research has some limitations, which will be discussed in this section. Further research has to be conducted with regard to these limitations. The limitations have to do with:

- The scope of the research, based on the risk categories
- The qualitative approach used within the research
- The concrete execution of the various steps
- The lack of internal experts used during the demonstration
- The governance and timing of the methodology

The first limitation is the scope of this research. The scoping used is based on the risk categories described within the FIRM framework of DNB (De Nederlandsche Bank, 2014). This research limits itself to three of the six of the non-financial risk categories. Also the financial risk categories are not addressed within the research. For further research we therefore advice to analyze the characteristics of the other categories of risk in order to determine whether they can fit into the methodology and how this should be done.

One important step here is to determine whether these categories of risks can be identified by using a risks analysis approach in which process models serve as the input. The risk categories should be analyzed for the fact if they can be identified within a process model, or that additional information is required. If the latter is the case, the additional information required should be described and the method for acquiring this information should be added to the methodology.

The second limitation is the fact that this research was conducted using qualitative approaches. This was done because of reasons described within literature and because the aim of this research was to provide a methodology that would serve as a guideline for assessing the impact of business process redesign decisions on internal control. We however advice that more research should be conducted on the specific implementation of the various steps described within the methodology. This research serves as a starting point for more research on implementing and executing the various steps. We do therefore not exclude the possibility that these steps can also be implemented and executed by means of quantitative approaches or other qualitative approaches. A quantitative approach would be make the second assessment needed when controls occur multiple times within a redesign decision redundant.

The third limitation is closely related to the second. Since our goals was to provide a guideline to assess the impact of business process redesign decisions on internal control, we offered a number of methods and tools for each task within each step. Some experts stated the need for more research towards the concrete execution of the steps. In this research it is important to find the methods and tools best suitable to perform the tasks within the steps.

The fourth limitation is the lack of internal expert involvement during the demonstration. Literature consulted describes that it is important that internal experts are consulted during several steps of the methodology. For example process owners should be incorporated in the risk analysis session and the accountable process owner should be involved in determining the risk appetite of the process. Because of confidentiality reasons the internal experts involved in the process used could not be consulted during our demonstration. We advise that further research of the methodology will focus on the involvement of internal experts.

The final limitation is the governance and timing of the methodology. Experts expressed that the quality of the input is very important, since carrying out all the steps correctly with low quality input will still result in a low quality result. Therefore more research should be conducted towards the governance and timing of the methodology. Important questions to ask for example are: *“Who is responsible for each step and when?”* and *“How do we ensure that the input quality is high?”*

## 13.3 Contributions

### 13.3.1 Contribution to Theory

The contribution of theory lies in the fact that different concepts described in literature are combined into one methodology. The concepts themselves are not contributions to theory since they are taken from the literature, but the synthesis of the concepts made within this methodology is. By means of offering an approach in which the concepts are used in complementary and sequential steps in order to operationalize them, answer can be given to a specific question: *What is the impact of business process redesign decisions on internal control within banks?*

More specifically, the need for more research towards to the integration of the concepts of business process management, risk management and compliance (Racz et al., 2010); (Rikhardsson and Best, 2006); (Sadiq et al., 2007) and its specific application on banks (Shin and Jellema, 2002) is identified by means of creating a concept matrix and interviewing experts and subsequently addressed within this research. While the integration of these already big research areas results in an even bigger research area, we looked deeper into the case of business process redesign and the shift in risks and controls in relation with compliance that occurs there. This is the first contribution to theory of this research, expressed in two of the four contributions described in part 1 – Research Introduction:

1. Extending current theory by identifying the need for more research towards a structured approach for assessing the impact of business process redesign decisions on internal control. This is a contribution to theory.
3. Extending current theory by providing valuable insights in how business process redesign impacts risks and consecutive controls within banks. This is a contribution to theory

The second contribution to theory that is made within this research lies in the fact that different concepts are linked in a clear overview by means of a methodology. We have shown that literature failed to address this until now, by performing a literature mapping on a concept matrix. This mapping and the methodology provide a starting point for further research into the specific implementation of the steps and tasks within the methodology. Each task requires methods and tools and by conducting this research we have shown the methodology functions as a guideline and we have offered methods and tools as a starting point for more research and discussion. This contribution is expressed in one of the four contributions described in part 1 – Research Introduction:

2. Extending current GRC theory by providing a methodology in which the contents of GRC are specifically linked and operationalized. This is a contribution to theory.

### 13.3.2 Contribution to Practice

The contribution to practice made within this research lies in the fact that a usable methodology that serves as a guideline for assessing the impact of business process redesign decisions on internal control is designed, which can be further developed and used by Deloitte and possibly other consulting companies in order to address the needs of their clients better. The methodology is made more practical by combining concepts and methods from the literature with best practice initiatives.

The methodology proposed is described in such detailed steps that it can be understood and implemented right away by various means. Suggestions on methods and tools made within several tasks and the description of specific input and output needed for every task enable the users of the methodology to perform further research towards the implementation and execution in order to personalize it to their companies' or clients' taste. There is not one single way to implement the methodology, it can be done by several means. We argue that this flexibility enables for a wider usage of the methodology, which we hope will lead to more information on the applicability of the methodology and more research towards it. Furthermore we have demonstrated the methodology on a real world bank, providing valuable insight into the impact of business process redesign decisions made there on internal control. This contribution is expressed in one of the four contributions described in part 1 – Research Introduction:

4. Also providing Deloitte Risk Services with valuable insights in how business process redesign impacts risks and consecutive controls within banks, and with a methodology as a guideline to assess this impact. This is a contribution to practice.

## 14 References

- Abdolvand, N., Albadvi, A., & Ferdowsi, Z. (2008). Assessing readiness for business process reengineering. *Business Process Management Journal*, 14(4), 497–511.
- ABN AMRO. (2013). *Private Banking welcomes you* (pp. 1–6), [http://www.abnamroprivatebanking.com/en/images/000\\_PBI\\_Global/Brochure/Private\\_Banking\\_welcomes\\_you/Private\\_Banking\\_welcomes\\_you.pdf](http://www.abnamroprivatebanking.com/en/images/000_PBI_Global/Brochure/Private_Banking_welcomes_you/Private_Banking_welcomes_you.pdf) (accessed, February 2014).
- Adrian, T., Etula, E., & Shin, H. (2009). Risk appetite and exchange rates. *Federal Reserve Bank of New York Staff Report*, 361, 1–41.
- Allen, B., Chan, K. K., Milne, A., & Thomas, S. (2012). Basel III: Is the cure worse than the disease? *International Review of Financial Analysis*, 25, 159–166.
- Al-Mashari, M., & Zairi, M. (1999). BPR implementation process: an analysis of key success and failure factors. *Business Process Management Journal*, 5(1), 87–112.
- Angelini, P., & Clerc, L. (2011). Basel III: Long-term impact on economic performance and fluctuations. *FRB of New York Staff Report*, (485), 1–22.
- Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., & LaFond, R. (2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. *The Accounting Review*, 83(1), 217–250.
- Ashbaugh-Skaife, H., Collins, D. W., & Kinney, W. R. (2007). The discovery and reporting of internal control deficiencies prior to SOX-mandated audits. *Journal of Accounting and Economics*, 44(1-2), 166–192.
- Attaran, M. (2004). Exploring the relationship between information technology and business process reengineering. *Information & Management*, 41(5), 585–596.
- Bank for International Settlements, & Basel Committee on Banking Supervision. (2006). *The Joint Forum: High-level principles for business continuity* (pp. 1–38), <http://www.bis.org/publ/joint14.pdf> (accessed, March 2014).
- Barth, J. R., Caprio, G., & Levine, R. (2004). Bank regulation and supervision: what works best? *Journal of Financial Intermediation*, 13(2), 205–248.
- Bass, T., & Robichaux, R. (2001). Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations. *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No.01CH37277)*, 1, 64–70.
- Bekaert, G., Hoerova, M., & Scheicher, M. (2009). What do asset prices have to say about risk appetite and uncertainty? *European Central Bank*, (1037), 1–47.
- BiZZdesign. (2014). BiZZdesign Architect: volledige ondersteuning van ArchiMate 2.1. *BiZZdesign*, <http://www.bizzdesign.nl/tools/architect/> (accessed, March 2014).
- Bouker, M. (2008). De Essentials van CoBIT. *IT Service Management Forum*, 16(6), 18–21, <http://www.itmg.nl/itmg-wp-content/Artikelen/COBIT/Training/De%20essentials%20van%20COBIT.pdf> (accessed, February 2014).
- Breaux, T., Vail, M., & Anton, A. (2006). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. *Requirements Engineering*, 14th IEEE International Conference, 49–58.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, 47(7), 87–92.
- Coles, R., & Moulton, R. (2003). Operationalizing IT risk management. *Computers & Security*, 22(6), 487–493.



- Constantinides, E. (2010). Connection Small and Medium Enterprises to the New Consumer: The Web 2.0 as Marketing Tool. *Global Perspectives on Small and Medium Enterprises*, 1–21.
- Constantinides, E. (2013). *Global Strategy and Marketing*. Lecture notes on the master's course for Business Administration and Business Information Technology at the University of Twente.
- Crowe, T. J., Fong, P. M., Bauman, T. a., & Zayas-Castro, J. L. (2002). Quantitative risk level estimation of business process reengineering efforts. *Business Process Management Journal*, 8(5), 490–511.
- Curtis, P., & Carey, M. (2012). Risk Assessment in Practice. *Committee of Sponsoring Organizations of the Treadway Commission*, 1–28, <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dtll-grc-riskassessmentinpractice.pdf> (accessed, March 2014).
- Damania, R., Fredriksson, P., & Mani, M. (2004). The persistence of corruption and regulatory compliance failures: theory and evidence. *Public Choice*, 363–390.
- Damianides, M. (2005). Sarbanes–Oxley and it Governance: New Guidance on it Control and Compliance. *Information Systems Management*, 22(1), 77–85.
- Danielsson, J., Shin, H. S., & Zigrand, J.-P. (2010). Risk Appetite and Endogenous Risk. Financial Markets Group.
- De Nederlandsche Bank. (2014). Handboek FIRM. *De Nederlandse Bank*, <http://www.toezicht.dnb.nl/4/2/1/50-203958.jsp> (accessed, March 2014).
- Deloitte. (2014). *Risk appetite in the financial services industry: A requisite for risk management today* (pp. 1–20), [http://www.deloitte.com/assets/Dcom-UnitedStates/Local/Assets/Documents/AERS/us\\_aers\\_grrs\\_riskappetite\\_03102014.pdf](http://www.deloitte.com/assets/Dcom-UnitedStates/Local/Assets/Documents/AERS/us_aers_grrs_riskappetite_03102014.pdf) (accessed, March 2014).
- Demirgüç-Kunt, A., & Detragiache, E. (2011). Basel Core Principles and bank soundness: Does compliance matter? *Journal of Financial Stability*, 7(4), 179–190.
- Demirgüç-Kunt, A., Detragiache, E., & Tressel, T. (2008). Banking on the principles: Compliance with Basel Core Principles and bank soundness. *Journal of Financial Intermediation*, 17(4), 511–542.
- Doyle, J., Ge, W., & McVay, S. (2007). Accruals quality and internal control over financial reporting. *The Accounting Review*, 82(5), 1141–1170.
- Doyle, J., Ge, W., & McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44(1-2), 193–223.
- Drew, M. (2007). Information risk management and compliance — expect the unexpected. *BT Technology Journal*, 25(1), 19–29.
- Dungey, M., Fry, R., González-hermosillo, B., & Martin, V. (2003). Characterizing Global Risk Aversion for Emerging Markets During Financial Crises. International Monetary Fund.
- Earl, M., Sampler, J., & Short, J. (1995). Strategies for business process reengineering: evidence from field studies. *Journal of Management Information Management*, 12(1), 31–56.
- Euro Banking Association. (2007). *Banks Preparing for SEPA: Issues to Be Addressed to Achieve SEPA Compliance* (pp. 1–25), <https://www.google.nl/#q=Banks+preparing+for+sepa> (accessed, March 2014).
- European Central Bank. (2009). *The Single Euro Payments Area (SEPA): An Integrated Retail Payments Market* (pp. 1–32), [http://www.ecb.europa.eu/pub/pdf/other/sepa\\_brochure\\_2009en.pdf](http://www.ecb.europa.eu/pub/pdf/other/sepa_brochure_2009en.pdf) (accessed, March 2014).
- Fox, C., & Zonneveld, P. (2003). IT Control Objectives for Sarbanes–Oxley. *IT Governance Institute, Rolling Meadows, IL*.

- Frigo, M., & Anderson, R. (2009). A strategic Framework for Governance, Risk, and Compliance. *Strategic Finance*, 90(8), 20–61.
- Gai, P., & Vause, N. (2005). Measuring investors' risk appetite. *International Journal of Central Banking*, 167–188.
- Ge, W., & Mcvay, S. (2005). The Disclosure of Material Weaknesses in Internal Control after the Sarbanes-Ocley Act. *Accounting Horizons*, 19(3), 137–158.
- Gericke, A., Fill, H.-G., Karagiannis, D., & Winter, R. (2009). Situational Method Engineering for Governance, Risk and Compliance Information Systems. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*, 24–35.
- Governatori, G., & Sadiq, S. (2009). The journey to business process compliance. *Handbook of Research on BPM*, 1–38.
- Grembergen, W. Van, Haes, S. De, & Moons, J. (2005). Linking business goals to IT goals and COBIT processes. *Information Systems Control Association*, 4, 18–21.
- Grover, V., & Jeong, S. (1995). The implementation of business process reengineering. *Journal of Management Information Systems*, 12(1), 109–144.
- Grover, V., & Malhotra, M. K. (1997). Business process reengineering: A tutorial on the concept, evolution, method, technology and application. *Journal of Operations Management*, 15(3), 193–213.
- Gunasekaran, a., & Kobu, B. (2002). Modelling and analysis of business process reengineering. *International Journal of Production Research*, 40(11), 2521–2546.
- Gunasekaran, A., & Nath, B. (1997). The role of information technology in business process reengineering. *International Journal of Production Economics*, 50(2), 91–104.
- Hammer, M., & Stanton, S. (1999). How process enterprises really work. *Harvard Business Review*, 77, 108–120.
- Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11(1), 55–61.
- Härle, P., & Lüders, E. (2010). Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation. *Online Verfügbar Unter Http://www. Mckinsey.com/clientervice/Financial\_Services/Knowledge\_Highlights/~/\_media/Reports/Financial\_Services/Basel% 20III% 20and% 20European% 20banking% 20FINAL. Ashx, Zuletzt Geprüft Am, (November), 1–30.*
- Hermanson, H. M. (2000). An Analysis of the Demand for Reporting on Internal Control. *Accounting Horizons*, 14(3), 325–341.
- Huang, W., Chen, Y., & Hee, J. (2006). STP technology: An overview and a conceptual framework. *Information & Management*, 43(3), 263–270.
- Institute of Conflict Management. (2013). *Risk Rating Matrix* (pp. 1–2), <http://www.conflictmanagement.org/icm/Downloads/Documents/Example of a NHS Risk rating matrix.pdf> (accessed, March 2014).
- ISO/IEC. (2005). *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management* (Vol. 2005, pp. 1–115), <http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf> (accessed, March 2014).
- Kaplan, S. (1997). The Words of Risk Analysis. *Risk Analysis*, 17(4), 407–417.
- Kartseva, V., Gordijn, J., & Tan, Y.-H. (2004). Analysing preventative and detective control mechanisms in international trade using value modelling. *Proceedings of the 6th International Conference on Electronic Commerce - ICEC '04*, 51–58.

- Kaufmann, C., Weber, M., & Haisley, E. (2013). The Role of Experience Sampling and Graphical Displays on One's Investment Risk Appetite. *Management Science*, 59(2), 323–340.
- Kharbili, M. El, & Stein, S. (2008). Towards a Framework for Semantic Business Process Compliance Management. *Proceedings of the Workshop of Governance, Risk and Compliance for Information Systems*, 1–15.
- Khong, K. W., & Richardson, S. (2003). Business process re-engineering in Malaysian banks and finance companies. *Managing Service Quality*, 13(1), 54–71.
- Klamm, B., & Watson, M. (2009). SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. *Journal of Information Systems*, 23(2), 1–23.
- Kliem, R. (2004). Managing the Risks of Offshore it Development Projects. *Edpacs*, 32(4), 12–20.
- Kliem, R. L. (2000). Risk Management for Business Process Reengineering Projects. *Information Systems Management*, 17(4), 1–3.
- Klomp, J., & Haan, J. De. (2012). Banking risk and regulation: Does one size fit all? *Journal of Banking & Finance*, 36(12), 3197–3212.
- Kueng, P., & Kawalek, P. (1997). Goal-based business process models: creation and evaluation. *Business Process Management Journal*, 3(1), 17–38.
- Küng, P., & Hagen, C. (2007). The fruits of Business Process Management: an experience report from a Swiss bank. *Business Process Management Journal*, 13(4), 477–487.
- Kunreuther, H. (2002). Risk analysis and risk management in an uncertain world. *Risk Analysis : An Official Publication of the Society for Risk Analysis*, 22(4), 655–64.
- Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics*, 93(2), 259–275.
- Lambert, J., Jennings, R., & Joshi, N. (2006). Integration of risk identification with business process models. *Systems Engineering*, 9(3), 187–198.
- Larsen, M., & Myers, M. (1999). When success turns into failure: a package-driven business process re-engineering project in the financial services industry. *The Journal of Strategic Information Systems*, 8(1999), 395–417.
- Lin, F.-R., Yang, M.-C., & Pai, Y.-H. (2002). A generic structure for business process modeling. *Business Process Management Journal*, 8(1), 19–41.
- Lindow, P., & Race, J. (2002). Beyond traditional audit techniques. *Journal of Accountancy*, 28–33.
- Lubin, D., & Esty, D. (2010). The sustainability imperative. *Harvard Business Review*, (May), 43–50.
- Malinverno, P. (2006). Sample Governance Mechanisms for a Service-Oriented Architecture. *Gartner*.
- Motwani, J., Kumar, A., Jiang, J., & Youssef, M. (1998). Business process reengineering: A theoretical framework and an integrated model. *International Journal of Operations & Production Management*, 18(9), 964–977.
- Moulton, R., & Coles, R. (2003). Applying information security governance. *Computers & Security*, 22(7), 580–584.
- Muehlen, M. zur, & Ho, D. (2006). Risk management in the BPM lifecycle. *Business Process Management Workshops*, 454–466.
- Namiri, K., & Stojanovic, N. (2007). A Formal Approach for Internal Controls Compliance in Business Processes. *8th Workshop on Business Process Modelling, Development, and Support*, 1–9.

- Neiger, D., Churilov, L., Muehlen, M. zur, & Rosemann, M. (2006). Integrating risks in business process models with value focused process engineering. *16th Australasian Conference on Information Systems*, (December), 1–10.
- Nielsen, J. R., & Mathiesen, C. (2003). Important Factors Influencing Rule Compliance in Fisheries Lessons from Danish Fisheries. *Marine Policy*, 27(5), 409–416.
- Object Management Group. (2014). Object Management Group Business Process Model and Notation. *Object Management Group*, <http://www.bpmn.org/> (accessed, March 2014).
- O'Neill, P., & Sohal, A. S. (1999). Business Process Reengineering A review of recent literature. *Technovation*, 19(9), 571–581.
- Panko, R. (2006). Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks. *Communications of the Association for Information Systems*, 1–29.
- Pederiva, A. (2003). The COBIT® maturity model in a vendor evaluation case. *Information Systems Control Journal*, 3, 26–29.
- Peffer, K., Tuunanen, T., Rothenberger, M. a., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45–77.
- Potoski, M., & Prakash, A. (2005). Green Clubs and Voluntary Governance: ISO 14001 and Firms' Regulatory Compliance. *American Journal of Political Science*, 49(2), 235–248.
- Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34(6-7), 849–855.
- Project Management Institute. (2000). A Guide to the Project Management Body of Knowledge (PMBOK Guide). *Project Management Institute*.
- PwC. (2013). Internal Control, Integrated Framework. *Committee of Sponsoring Organizations of the Treadway Commission*, (December 2011), 1–156, [http://www.coso.org/documents/coso\\_framework\\_body\\_v6.pdf](http://www.coso.org/documents/coso_framework_body_v6.pdf) (accessed, February 2014).
- Rabobank. (2013). *Vernieuwen en verbinden: Visie 2016* (pp. 1–19), <https://www.rabobank.com/nl/images/2013%2001%2025%20Rabobank%20Visie%202016%20NL.pdf> (accessed, February 2014).
- Racz, N., Weippl, E., & Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). *Communications and Multimedia Security*, (January), 106–117.
- Racz, N., Weippl, E., & Seufert, A. (2010). A process model for integrated IT governance, risk, and compliance management. *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*, 155–170.
- Remenyi, D., & Heafield, A. (1996). Business process re-engineering: some aspects of how to evaluate and manage the risk exposure. *International Journal of Project Management*, 14(6), 349–357.
- Ribeiro, J., & Gomes, R. (2009). IT governance using COBIT implemented in a high public educational institution: a case study. *Proceedings of the 3rd International Conference on European Computing Conference*, 41–52.
- Rikhardsson, P., & Best, P. (2006). Business Process Risk Management, Compliance, and Internal Control: A Research Agenda. *Management Accounting Research Group Working Paper M-2006-05, presented at the Second Asia/Pacific Research Symposium on Accounting Information Systems, University of Melbourne, Melbourne*.
- Sadiq, S., & Governatori, G. (2010). Managing regulatory compliance in business processes. *Handbook on Business Process Management 2*, 1–23.
- Sadiq, S., & Governatori, G. (2009). A methodological framework for aligning business processes and regulatory compliance. *Handbook of Business Processes Management 2*, 159–176.

- Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling Control Objectives for Business Process Compliance. *Business Process Management*, 149–164.
- Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, 749–753.
- Schepers, T. (2007). A Lifecycle method for Service Oriented Architecture governance. *MSc Thesis University of Twente the Netherlands*, 1–134.
- Shin, N., & Jemella, D. F. (2002). Business process reengineering and performance improvement: The case of Chase Manhattan Bank. *Business Process Management Journal*, 8(4), 351–363.
- Simonsson, M., & Johnson, P. (2006). Assessment of IT Governance-A Prioritization of Cobit. *Proceedings of the Conference on Systems Engineering Research*, 1–10.
- Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis*, 20(1), 1–11.
- Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: some thoughts about affect, reason, risk, and rationality. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 24(2), 311–22.
- Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640–661.
- Sutinen, J. G., & Kuperan, K. (1999). A socio-economic theory of regulatory compliance. *International Journal of Social Economics*, 26(1/2/3), 174–193.
- Teng, J., Fiedler, K., & Grover, V. (1998). An exploratory study of the influence of the IS function and organizational context on business process reengineering project initiatives. *Omega*, 26(6), 679–698.
- The Institute of Risk Management (2011). Risk Appetite and Tolerance. (2011). *The Institute of Risk Management*, 1–42, [http://theirm.org/publications/risk\\_appetite.html](http://theirm.org/publications/risk_appetite.html) (accessed, February 2014).
- The Open Group. (2014). ArchiMate®. *The Open Group*, <http://www.opengroup.org/subjectareas/enterprise/archimate> (accessed, March 2014).
- Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, 8(4), 240–263.
- United States Agency for International Development. (2000). *Business Process Reengineering: EFS Technical Report NO.21* (pp. 1–50).
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99–104.
- Webster, J., & Watson, R. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), 13–23.
- Werkgroep Tariefstructuren en Infrastructuur in het Betalingsverkeer. (2002). *Tariefstructuren en Infrastructuur in the Nederlandse massale Betalingsverkeer* (pp. 1–99), [http://www.dnb.nl/en/binaries/tariefstructuur\\_infrastructuur\\_tcm47-145685.pdf](http://www.dnb.nl/en/binaries/tariefstructuur_infrastructuur_tcm47-145685.pdf) (accessed, February 2014)
- Zalewska-Kurek, K. (2013). *Global Strategy and Marketing*. Lecture notes on the master's course for Business Administration and Business Information Technology at the University of Twente.
- Zhang, Y., Zhou, J., & Zhou, N. (2007). Audit committee quality, auditor independence, and internal control weaknesses. *Journal of Accounting and Public Policy*, 26(3), 300–327.

# Appendices

## Appendix A. List of Figures

Figure 1. Drivers for Business Process Redesign .....	4
Figure 2. Interconnection of Business Process Management and Controls Management Source: Sadiq and Governatori (2010).....	4
Figure 3. The Governance, Risk and Compliance Model Source: Racz et al. (2010).....	5
Figure 4. Conceptual Model.....	8
Figure 5. FIRM Risk Framework (DNB).....	10
Figure 6. Research Methodology .....	12
Figure 7. Design Science Research Methodology for Information Systems Source: Peffers et al. (2007).....	12
Figure 8. Literature Review Steps .....	14
Figure 9. The Determinants of Compliance Source: Sutinen and Kuperan (1999) .....	16
Figure 10. Risk Matrix .....	19
Figure 11. Relationship between Process Modelling and Internal Control Source: Sadiq and Governatori (2010) .....	20
Figure 12. Control Objective and Related Controls Source: Governatori and Sadiq (2009).....	20
Figure 13. Risk Appetite Source: The Institute of Risk Management (2011).....	21
Figure 14. Determinants of Risk Appetite Based on: Gai and Vause (2005).....	21
Figure 15. Risk Universe Equation.....	22
Figure 16. Controls within a Process Source: Lambert et al. (2006).....	23
Figure 17. Controls Source: Panko (2006).....	23
Figure 18. COSO Framework Source: PwC (2013).....	25
Figure 19. Major BPR Elements when using IT to Improve Client Servicing Source: Gunasekaran and Nath (1997) .....	30
Figure 20. The Business Process Management (BPM) Lifecycle Source: zur Muehlen and Ho (2006) .....	31
Figure 21. Research Model .....	34
Figure 22. Methodology Outline.....	39
Figure 23. Process Model for Modeling the "as is" Situation.....	40
Figure 24. Achimate 2.1 Business Process Semantics.....	42
Figure 25. Process Modeling in BizDesign Architect.....	43
Figure 26. Process Model for the "as is" Situation Risk Analysis.....	44
Figure 27. Risk Matrix Layout.....	46
Figure 28. Process Model of the "as is" Situation Controls Analysis.....	47
Figure 29. Indicators for Cost of Control.....	53
Figure 30. Risk Appetite Statement Approach Based on: Deloitte (2014) .....	57
Figure 31. Risk Equation.....	57
Figure 32. Process Model for the Process Requirements .....	60
Figure 33. Target Operating Model Based on: Deloitte Resources .....	61
Figure 34. Archimate 2.1 Requirements Analysis Semantics .....	62
Figure 35. BiZZdesign Requirements Analysis Example .....	62
Figure 36. Process Model for Modeling the "to be" Situation .....	63
Figure 37. Process Model for the "to be" Situation Risk Analysis .....	65
Figure 38. Process Model for the "to be" Situation Controls Analysis.....	66
Figure 39. Process Model for the Controls Shift Analysis .....	69
Figure 40. Control Shift Matrices .....	73
Figure 60. The Determinants of Compliance Source: Sutinen and Kuperan (1999) .....	80
Figure 61. Risk Matrix .....	81
Figure 62. Relationship between Process Modeling and Internal Control Source: Sadiq and Governatori (2010) .....	82
Figure 63. Control Objective and Related Controls Source: Governatori and Sadiq (2009).....	82
Figure 64. Risk Appetite Source: The Institute of Risk Management (2011).....	83
Figure 65. Risk Universe Equation.....	83

Figure 66. Major BPR Elements when using IT to Improve Client Servicing Source: Gunasekaran and Nath (1997) ..... 84

Figure 67. The Business Process Management (BPM) Lifecycle Source: zur Muehlen and Ho (2006) ..... 85

Figure 68. Research Model ..... 86

Figure 69. Methodology Outline ..... 89

## Appendix B. List of Tables

Table 1. Mapping of DSRM to Research Steps .....	13
Table 2. Research Overview .....	13
Table 3. COSO Principles Source: PwC (2013) .....	25
Table 4. CobiT Conceptual Model Example Based on: Tuttle and Vandervelde (2007) .....	27
Table 5. Example RACI Table Based on: Malinverno (2006) .....	45
Table 6. Process Owner Spreadsheet .....	45
Table 7. Risk Identification Spreadsheet Based on: Deloitte Resources .....	47
Table 8. Categorization of Risks .....	48
Table 9. Risk and Controls Register Example Based on: Deloitte Resources .....	51
Table 10. Controls List Example .....	51
Table 11. Cost of Controls Table Example .....	55
Table 12. Selected Controls Table Example .....	59
Table 13. Requirements Fulfillment List Example .....	65
Table 14. Best Practice Database Example Based on: Deloitte Resources .....	68
Table 15. "as is" Risk Elements Control Table Subset .....	71
Table 16. "to be" Risk Elements Control Table Subset .....	71
Table 17. Controls "as is" versus "to be" .....	71
Table 18. Controls Shift Table .....	73



## Appendix C. Concept Matrix

Table C1. The Concept Matrix




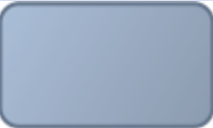


Article	Year	Drivers	Performance Input	Process Requirements	"As is" Situation	Process Information	"To be" Situation	BPR/ BPM	Risk/ Risk Analysis	Risk Appetite/ Risk Appetite Analysis	Controls	ΔControls/ Controls Shift Analysis	Internal Control	Total
Earl, M., Sampler, J., & Short, J.	1995	X						X			X		X	4
Grover, V., & Jeong, S.	1995	X						X						2
Remenyi, D., & Heafield, A.	1996							X	X					2
Grover, V., & Malhotra, M. K.	1997	X						X						2
Gunasekaran, A., & Nath, B.	1997	X		X			X	X						4
Kaplan, S.	1997								X					1
Kueng, P., & Kawalek, P.	1997							X						1
Motwani, J., Kumar, A., Jiang, J., & Youssef, M.	1998							X						1
Teng, J., Fiedler, K., & Grover, V.	1998	X						X	X					3
Al-Mashari, M., & Zairi, M.	1999							X						1
Hammer, M., & Stanton, S.	1999								X					1
Larsen, M., & Myers, M.	1999	X	X		X	X	X	X						6
O'Neill, P., & Sohal, A. S.	1999							X						1
Sutinen, J. G., & Kuperan, K.	1999	X												1
Hermanson, H. M.	2000										X		X	2
Kliem, R. L.	2000							X	X		X			3
Project Management Institute.	2000								X					1
Sjöberg, L.	2000								X					1
United States Agency for International Development.	2000	X		X			X	X						4
Bass, T., & Robichaux, R.	2001								X		X			2
Crowe, T. J., Fong, P. M., Bauman, T. a., & Zayas-Castro, J. L.	2002								X					1
Gunasekaran, a., & Kobu, B.	2002	X						X						2
Kunreuther, H.	2002								X					1
Lin, F.-R., Yang, M.-C., & Pai, Y.-H.	2002				X		X	X						3
Lindow, P., & Race, J.	2002								X		X		X	3
Shin, N., & Jemella, D. F.	2002	X			X	X	X	X						5
Werkgroep Tariefstructuren en Infrastructuur in het Betalingsverkeer.	2002	X												1
Coles, R., & Moulton, R.	2003								X					1
Dungey, M., Fry, R., González-hermosillo, B., & Martin, V.	2003									X				1
Fox, C., & Zonneveld, P.	2003							X			X		X	3
Khong, K. W., & Richardson, S.	2003			X				X						2
Moulton, R., & Coles, R.	2003								X					1
Nielsen, J. R., & Mathiesen, C.	2003	X												1
Pederiva, A.	2003				X				X		X		X	4
Spira, L. F., & Page, M.	2003									X	X		X	3
Attaran, M.	2004	X						X						2



Gericke, A., Fill, H.-G., Karagiannis, D., & Winter, R.	2009	X						X	X		X		X	5
Governatori, G., & Sadiq, S.	2009										X		X	2
Klamm, B., & Watson, M.	2009										X		X	2
Laeven, L., & Levine, R.	2009	X						X	X					3
Power, M.	2009									X				1
Ribeiro, J., & Gomes, R.	2009	X									X		X	3
Sadiq, S., & Governatori, G.	2009	X						X	X		X		X	5
Constantinides, E.	2010	X												1
Danielsson, J., Shin, H. S., & Zigrand, J.-P.	2010								X					1
Härle, P., & Lüders, E.	2010	X							X					2
Lubin, D., & Esty, D.	2010	X												1
Racz, N., Weippl, E., & Seufert, A.	2010	X							X					2
Racz, N., Weippl, E., & Seufert, A.	2010							X	X		X		X	4
Sadiq, S., & Governatori, G.	2010	X						X	X		X		X	5
Angelini, P., & Clerc, L.	2011	X												1
Demirgüç-Kunt, A., & Detragiache, E.	2011	X												1
The Institute of Risk Management	2011									X				1
Allen, B., Chan, K. K., Milne, A., & Thomas, S.	2012	X												1
Curtis, P., & Carey, M.	2012								X					1
Klomp, J., & Haan, J. De.	2012	X							X					2
ABN AMRO.	2013	X												1
Constantinides, E.	2013	X												1
Institute of Conflict Management.	2013								X					1
Kaufmann, C., Weber, M., & Haisley, E.	2013									X				1
PwC.	2013										X		X	2
Rabobank.	2013	X												1
Zalewska-Kurek, K.	2013	X												1
Deloitte.	2014									X				1
		48	5	8	6	3	6	34	39	13	38	0	36	236

## Appendix D. Used BPMN Semantics

Table D1. Used BPMN Semantics

Construct	Representation
A <i>start event</i> represents the start of the process.	
An <i>end event</i> represents the end of the process	
An <i>intermediate event</i> represents an event that takes place between the start and end of a process. In our methodology it means the end of a step and the beginning of a new one.	
A <i>task</i> represents a task that has to be carried out within the process.	
A <i>data object</i> represents how data is required or produced by different tasks. Data objects are connected to task by associations.	
A gateway represents a certain decision that has to be made in-between tasks.	

Based on BPMN (Object Management Group, 2014)

## Appendix E. Models

--- Confidential ----

## Appendix F. Risks and Controls

---- Confidential ----

## Appendix G. Controls Shift

---- Confidential ----

## Appendix F. Evaluation Interview Overview

### Goals

As the primary contribution of this research we argue that we can combine the various concepts discussed within the literature research and described within the research model into a sound methodology that serves as a guideline for assessing the impact of business process redesign decisions on internal control. This statement can be split into multiple goals, each describing one or more linkages within the research model:

1. **Determining the “to be” situation by modelling the process through combining the “as is” process model with the information from the requirements analysis.**
2. **Identifying risks for both situations by performing a qualitative risks analysis, in which the process models serve as an input.**
3. **Linking controls to the risks by using control frameworks as well as other best practice information and assessing the cost of these controls by means of a qualitative approach.**
4. **Determining a selection of controls to be implemented by combining the risks with their identified controls, the cost of these controls and the risk appetite, using a qualitative approach.**
5. **Assessing and visualizing the impact on internal control by representing the controls of both the “as is” and the “to be” situation into one overview by using their cost and type.**

### Questions

1. All concepts of which the methodology consists are elaborately described in literature and used multiple times, but are seldom combined. GRC literature describes the need for more integration between risk management, governance and compliance. Within this integration, the visualization of processes and process changes plays an important role. Do you also recognize the need for a more structured approach for assessing the impact of business process redesign decisions on internal control?
2. Do you agree that a methodology based on these goals is adequate to structure such an approach?
3. Are the listed goals sufficiently operationalized in the designed methodology, which means:
  - a. Are the steps logically structured within the methodology?
  - b. Are the goals of the various steps in line with the listed goals e.g. does achieving the goals of the steps result in achieving the listed goals?
  - c. Are the offered methods and tools sufficient to perform the associated task properly?
  - d. Is the recommended format or semantic for describing or visualizing the results clear and sensible?
4. The demonstration shows the application and the soundness of the methodology, applied on the mortgage provision process of a bank. During the demonstration you have agreed in our conversations that the information provided by you is correctly processed. Do you still share that opinion after seeing the presentation?
5. The listed goals have been operationalized in the demonstration by means of an application of the methods and tools described in each task.
  - a. The first goal was to Determine the “to be” situation by modelling the process through combining the “as is” process model with the information from the requirements analysis. This is done by gathering information and using BizDesign Architect (Archimate 2.1) to both model both the process models and the requirement analysis. Has this goal been achieved?
    - Could other modelling tools be used as well?
  - b. The second goal was to identify risks for both situations by performing a qualitative risk analysis, in which the process models served as input. We have mapped the risks in the models and we later performed a scoring on impact/occurrence by making use of the risk matrix. Has this goal been achieved?
    - What are the possibilities for a quantitative approach?
  - c. The third goal was to link controls to the identified risks by using control frameworks and other best practice information and assessing the costs of these controls by means of a qualitative approach. We used the cost and time factor for this. Has this goal been achieved?
    - What are the possibilities for a quantitative approach?



- d. The fourth goal was to determine a selection of controls to be implemented. This was done by means of a qualitative approach, in which the risk appetite and the overview of the risks with their impact/occurrence scoring and their identified controls with their cost/time scoring served as input. In the demonstration the risk appetite was set to 0, so all controls were selected. Normally the risk appetite would be determined in risk appetite analysis session with the accountable process owners, or by determining the risk appetite statement, or by consulting risk appetite analysis documents. Do you think such an approach would mean the achievement of this goal?
  - e. The fifth and last goals was to assess and visualize the impact on internal control by representing the controls of both the “as is” and the “to be” situation into one overview by using their cost and type. This has been done by means of control shift tables and control shift matrices. Has this goal been achieved?
6. Looking at the results of this demonstration:
- a. How can this methodology be improved?
  - b. What are the strong points of this methodology?
7. Do you think that you or Deloitte Risk Services/ Deloitte Consulting or Deloitte can and will use this methodology?

## Interview 1

1. Yes, definitely when looking at GRC, this is what our work is based on. In the market and at clients we see that they have problems with the integration of the concepts in the business operations. In practice this is a unique selling point for us. We integrate the different concepts. I acknowledge that.
2. Yes the small details underneath it are also in our methodologies. This is a good summarization of these details for sure. I would like to see monitoring next to it as well, but that is out of scope in this methodology. We however do recommend our clients this. These are the five main goals for sure. In the various methodologies we use these goals appear as well for sure.
3.
  - a. We often take the “to be” and the “as is” situation and then make a gap analysis. In your methodology that gap analysis comes a little later. The approach can differ a bit, but the steps in your methodology are the steps within the process I think. Everything is present, even assessing the costs. Instead of assessing and visualizing the shift we often for example continue with monitoring. Assessing and visualizing the costs of the shift with regard to redesign is maybe something that is more a consulting thing. The order of steps is logical.
  - b. For people who have knowledge about this subject. For people who haven't the steps should be explained more clearly. I would personally make the steps bigger maybe, less smaller steps. *After a short explanation in which the first methodology goals is used as an example and all the sub goals within the methodology are looked through:* Yes everything is in it. The sub goals of the steps are in line with the methodology goals.
  - c. *After an explanation about modelling with BizDesign Architect and the RACI table as example:* I do not know the details, but if I see this structuring and if I look at the way we brainstormed about the qualitative approach of assessing the costs of control with relation to impact an occurrence, I think that the correct methods and tooling are used.
  - d. Sometimes a bit long-winded. I would look at the audience every time you present this. Specialist know the details. If you are going to present to people who don't know the details, you have to compress things. The format is useful and the tables are clear. If you put the matrices with the controls shift next to each other, you can clearly see the shift.
4. Yes, for the full 100%. We have addressed this in detail.
5.
  - a. Yes I think so. I do not know the process requirements by heart. How we have looked through the situation based on the info I have I think so.
    - I do not know other tools, but this tool is very decent.
  - b. Yes for sure. We have made the choice for a certain detail level to keep it manageable. We have done this correctly. A sensible risk analysis can be made based on these process models.
    - Yes we have talked about this earlier. It stays a choice. A qualitative approach is fine here. When working with clients it may be better to choose for a quantitative approach to prevent big discussions.
  - c. Yes.
    - We have also talked about a qualitative approach for rating the costs, for example by using a logarithmic scale. I think that if you want to show it to the customer, you have to use a quantitative approach. Theoretically, a qualitative approach is also possible.
  - d. Yes, for sure. In this case it was good to take a risk appetite of 0. But if you determine a risk appetite it is still possible to use a session to determine what controls have to be selected. The customer becomes more aware by doing this. They become more aware of their choices and will do the assessment of the controls and the implementation of them for sure.
  - e. Yes for sure, the goal has been reached. The matrices speak for themselves. The tables are not even required in the presentation. If you present this to a board you should only show the matrices. Maybe, in case of a more critical audience, you should show the tables. This depends on personal taste.

6.
  - a. Quantitative analysis. If controls are to be implemented this methodology will be part of bigger whole, of change management. Monitoring is also an important aspect in this and can be the next step after this methodology. Looking at your goals and scope, this is a good methodology.
  - b. This is thought through very well. It's not only a plan of action, it is well substantiated. The goals of the step substantiate the methodology goals, which we just looked at. There are even extra aspects in this methodology. Process requirements are often a small aspect which is used in the gap analysis. Here it is really a main goal to be sure that you are on the right track. The end of the methodology is strong. We also have never assessed and visualized the controls shift like this. If more people are made aware of this, we could surely make our clients aware of it.
7. Yes, as part of a new or combined methodology. We do not come up with methodologies based in theory ourselves, but we look at the client situation and this methodology can surely be part of what we offer the client. And in combination with other methodologies that are used within Deloitte Risk Services. I am sure that this is added value for both Deloitte Risk Services as the client.

## Interview 2

1. Yes, because when you look at the financial institutions I visit, I see a strong need for more process control. It is a good thing to be able to assess what process change will mean to your internal control environment and to make this measurable. This is needed to do proper decision making.
2. Yes, I think this is the methodology as we discussed it together. It logically links the different situations and the controls in both situations.
3.
  - a. Yes, but maybe you can do the steps for both situations parallel. But in my opinion this is a logical order, since redesign decisions are often not clear.
  - b. *After a short explanation in which the first methodology goals is used as an example and all the sub goals within the methodology are looked through:* Yes, the main goals give the constraints for the implementation of the sub goals. If you achieve the sub goals you also achieve the main goals.
  - c. In my opinion, yes.
  - d. If you talk about the tables with risks and controls, then they are in mostly in line with the structure of our standard risk and controls registers, so they are good. With regard to the process modelling and the format of the results, your method and tools are also good. There could possibly be other methods and tools as well. We also use other methods sometimes. The tables are logical when you look at the results you that is worked towards.
4. Yes
5.
  - a. Yes, the goal is achieved.
    - In my opinion, this tool is fine.
  - b. Yes, I think we were able to identify the most important risks. In the future, both for risks and controls, we can go to a higher level of detail. But with the time in regard, this is fine. The method behind it works and is good. In practice we could go a little deeper. We could further drill down stepwise.
    - I think that a quantitative risk analysis is still not properly developed. However, it will become more important in the future. This asks for further research, but I think it could work very well.
  - c. Yes, the same answer as to the previous question applies here. With the time and scoping in mind we have achieved the goal. If we continue to develop this, we could acquire more gain here. But again, quantitative analysis is very hard.
  - d. Yes, this is how we normally do this. To me this is certainly the way to achieve the goal.
  - e. Yes, I think that the matrices show very clearly what the impact of redesign decisions on internal control is. You can see that in case of the redesign decisions on IT the control cost drastically increases and that in case of the other redesign decisions the control cost drastically decreases as a result of the

automation. Maybe you could combine the impact of all redesign decisions within one model. By doing this you will have a higher aggregation level, through which the overview contains more management information.

6.
  - a. Quantitative analysis. Redesign decisions together in one overview. Besides that this is a logical methodology.
  - b. This methodology combines existing methodologies, which have been proven individually but have not been combined in such a degree that the whole chain is covered from end to end. This is a real integrated approach.
7. Yes, we have talked about this before. I think we could surely use it. Probably not completely in this shape, but in combination with other things we offer. It is part of a broader proposition. Valuable addition to the portfolio we currently offer.

### Interview 3

1. From my work experience I acknowledge this need. I do not know the literature exactly. For as far as I know GRC primarily focusses on the tooling. A number of big suppliers sell software to combine the different silos within companies. They only look at controls, laws and regulations and the regulation of it, but I think processes are not used in this. But if you look at the concepts of risk management, governance and process management I see that a process view is never used. GRC tooling could help with that, but it is not really doing that right yet. Your methodology can help there. Now a laws and regulations view is used to look at certain controls and where those controls then need to be plotted within the processes. But the effect that process change has on controls and being compliant is not looked at.
2. Yes I think so, because what I miss in my experience is that there is insufficiently looked at the processes and changes in processes in practice. Identification of risks and the associated controls is not new on its own, but combined with the processes and the shift it is complete.
3.
  - a. Yes, in my opinion it is logical. The way it is described it is very naturally. You visualize something, you do this another time, and afterwards you map the old and new situations against each other to look at the shift. Another order is logically not possible.
  - b. *After a short explanation in which the first methodology goals is used as an example and all the sub goals within the methodology are looked through:* In my opinion, yes. The steps exactly reoccur in detailed steps within your model. It fits one on one.
  - c. *After an explanation about modelling with BizzDesign Architect as example:* The steps are clear. Except from those modelling tools I feel confident that I could execute the steps. I have no experience with modelling tools. But they are means to an end. The tasks and the methods you offer are the most important and based on these it would succeed.
  - d. Yes for sure, I for example found the shift analysis to be very handy. The implementation by means of types within one table is very nice, handy and efficient. I am really charmed by that. I work with the tables on a daily basis and for me it is standard and clear. The shift is new for me and a good addition. When I look at the processes and the visualization of the methodology as a whole it is just clear.
4. Yes, I have not seen odd things. Otherwise I would have said it.
5.
  - a. We have looked through the big process overviews and according to me you have modelled the process very detailed. Mission accomplished.
    - In order to really perform a good risk analysis on a process you minimally need the process and the underlying IT infrastructure. I would have used the same tool for this.
  - b. Yes.
    - A quantitative approach is very hard. There have been some attempts and it is a hot topic, but it is as good as impossible. If you do manage to do it, you can earn a lot of money with it.

- c. I think that linking the controls to the risks is done good and efficiently. We have also done a good effort linking the costs. Of course it stays qualitative. This is where you tend towards a quantitative approach. To some extent it is possible to link time and cost to controls, but to be very accurate is very difficult. The method which we have used now is good for the moment.
  - d. If you manage to clearly determine the risk appetite in cooperation with the process owners, it should be possible to make a good selection of controls in my opinion. The categorization which has been made with regard to the scoring of cost and time enables us to do this, because we can combine that with the risk appetite.
  - e. Yes, for sure. Like I said before: I am really charmed by this visualization. It clearly visualized what the change in controls in the new situation is.
- 6.
- a. Quantitative analysis would be very nice. If you would be able to give a more accurate scoring to cost and time it would be very nice, but in my opinion this is very hard in practice. Apart from the methodology I would like to see if the costs increase or decrease within the case.
  - b. The methodology combines a number of things. The visualization of the processes and the changes in the processes and their impact on controls certainly has an added value. GRC currently only focusses on integrating a number of departments within companies, but the underlying processes are often out of scope.
7. I do not know if I will use it, since I do not have the required seniority, but I am sure it can be used. The hard part is that when you go through a process like this, it is very extensive. You will need various disciplines with Deloitte. I think your methodology will greatly help to go through the process together very constructively by means of all steps, but I do not know if this will really happen in practice. Everybody tends to focus on his/her own thing, but it would greatly help to bring the different disciplines together. During a long cooperation project the methodology would surely help, because people are forced to do certain steps together. This is better for the client. Added value for both Deloitte and the client.

#### Interview 4 (Expert not involved in the demonstration)

1. Yes, I do not think that a lot of attention is paid to the proper substantiation of the redesign of a process. Companies have trouble enough with being in control of the current situation. The focus is on being compliant in the current processes. I think there is still attention paid for being compliant in processes to be developed, but to get a good assessment of the cost of controls is a challenge and linking this to business process redesign is a step that organizations have not made yet.
2. I do have some point of attention on a more detailed level per step. I think: "Is this the detail level you need or is it not needed?" Per goal:
  1. Yes I think this is correct.
  2. Correct, but I do not know if the timing is correct.
  3. If this can be done properly it is very useful. I do wonder if a qualitative approach, although a quantitative approach is difficult, is useful. Best practice information and controls frameworks are valuable context information, but you have to mind that you do not start to use a goal reasoning.
  4. *After some explanation of the goal:* You have to give a clear description. Qualitative approach is difficult here. I would expect a bigger difference between automated and manual controls in the demonstration.
  5. Is correct.

Eventually these are the goals a methodology should meet, but the way in which they are executed is important.
3.
  - a. I have some points of attention regarding modelling the "as is" situation. The scope is important here. In order to be complete you have to take the whole process and not a part of it. In case of the demonstration this is however sufficient, but you should not do this in practice. Determining the level of detail is key. Furthermore the steps are logically structured.
  - b. In my opinion, yes.

- c. I think it is limited to really properly execute the different tasks. *After explaining that the methods and tools offered are meant to provide guidance during the execution:* There is more guidance needed than only handles. For example, how are you going to involve the responsible persons? The power of good result lies here.
- d. Yes, but the quality of the risks is important. So what you write down is more important than the way you write it down. I also want to note that “as is” risks will often reoccur in the “to be” situation.
4. *Not applicable, since the expert was not involved in the demonstration.*
5.
  - a. I cannot really assess this, since I do not know enough about the contents. I cannot assess the tool. *Reasoning from the pure application of the approach given in the goal:* The quality of the information is key.
    - Level of detail is important, drilling down needs to be supported. Given that a tool can do this, it can be used.
  - b. Yes, provided that it is carried out properly. The qualitative character is very difficult and making sure that it is complete also. A lot of effort is put into this.
    - That is very hard, but I do really wonder if the assessment on impact and occurrence is relevant here. *After explaining the use of this in the controls selection:* I agree. This is what done in every risk management process. Fine by me, but it is linked to the draft and quality of the risks you identify.
  - c. Yes, but the contents are again important here. The quality of the controls is very important. In case of automated controls the development and implementation costs show up. These costs needs to be taken into account when assessing the cost factor of a control.
  - d. Yes, but I think it will be very hard to properly determine the risk appetite. Everyone will push the control of the risk appetite towards someone else.
  - e. Yes, but I would conclude it with one overall overview and a business case. I would also show a legend with controls. Eventually it is all about the way in which you present it. I my experience it is very good to summarize as much as possible in one presentation. In case of providing management information I would use less details. The overall overview is suited for this.

In total, everything is correct, but the implementation is very important.
6.
  - a. Quantitative approach. Quality of information and analysis is very important. As a guideline, the methodology is correct. The execution is very important. The question is how open you are towards information coming from different sources. Sometimes the best information comes from sources you would not expect. More research is needed towards the concrete implementation.
  - b. Visualizing the difference between “as is” and “to be” is very strong. The visualization is very nice, provided that the substantiation is good. I have my doubts about this and it is very difficult, but it is key.
7. I think various steps and concepts in the methodology are not new, but the linkage between concepts is. This is something we do not dare to do yet. The methodology serves as a proper guideline, but the implementation is difficult. It serves as a good starting point for discussion. Maybe this is the start of a design session. Surely added value to build on, but it will need some improvements before it can be sold.

#### Interview 5

1. Yes for sure. In this client case you see that a lot of effort is put in redesigning the process. Eventually the process has been redesign with the focus on two risks. But subsequently no integral view of the risks has been followed during redesigning the process. Afterwards, when the technology is developed after the redesigning, there arises a need that the business should be able to prove that all risks have been identified and the controls needed have been implemented. But actually that’s too late. This should have done during the redesign of the process.
2. Yes, as a methodology, for sure. But it falls or stand with the usage of it and the governance around it. In the steering you have to anchor that the risks and controls are properly identified. In terms of content you need

experts to make sure that you can properly assess this. It is important to know clearly who is going to use the methodology and where in the process.

3.
  - a. Yes, it is logically structured. When a “to be” situation already exists you have to perform a few steps retroactively.
  - b. Yes
  - c. I would surely use TOM for the requirements analysis. We have had a lot of discussion about BizDesign Architect. My opinion is that the methodology does not fit enough with the situation. Underlying connections between requirements do not come forward are not shown entirely properly now. This is where more gain can be acquired. *When looking at the whole:* I do not know all of it, but I think one should look at other risk categories also. When looking at the controls shift matrices I do wonder if the qualitative scale offers enough handhold. In terms of content I had expected that there would be more controls that are very high at the cost side, due to laws and regulations and the fees that you would otherwise receive from the authorities.
  - d. Yes, but we have had some discussions about the coloring code. I have made some suggestions to make it fit better to the real situation. I see now that the role of the financial assistant does not entirely show properly. This is an important movement which has to do with risk shift. Maybe the process has not been modelled on a detail level that is high enough for this. But looking at the visualization of the process etc. it is fine by me.
4. Yes, for sure.
5.
  - a. Yes, its fine when looking at the approach. However I do have some doubts about the usage of the tool, taking in mind this tool has some restrictions.
    - Personally, I think ARIS is a good tool. This tool enables you to model processes at different levels and to drill down to actors and the needed documents with the use of coloring codes and timestamps. This is a set of requirements that a good modelling tool should have. Input and output for every step should be modelled clearly.
  - b. I do not know if I can assess this entirely, since I am not a risk expert. I look at it from a business point of view.
    - I have some experience with it from the past in the form of linking price labels to the impact and working sometimes with a bucket of for example 1 to 2.5 million. What I notice is that there is still a feeling of high and low linked to it. Eventually a label is linked to this, but that has nothing to do with the actual impact. Often nothing is done with that amount of money in terms of resources. It is good to make people in the process aware of the extent of the impact. When you have determined that, I think it is sufficient to carry on with a qualitative scale.
  - c. As a methodology for sure, in terms on content I do not know if we have been entirely complete. But I would surely acknowledge it.
    - You should be able quantify the approach of assessing control costs in terms of time and cost I think. I think it is useful in relation to this client case to show the shift that occurs and that that saves money to the users and the others stakeholders. Many people still think that double checking by another employee is safer than an automated process.
  - d. Yes, for sure. But I think that in this client case it will be a big discussion who is eventually really accountable. The pressure from external and internal authorities is so high that the accountable personal is not always the one who can determine this.
  - e. Yes, it would even help more to show this in one picture and to add a legend of the controls. In order to provide more management information I would show the redesign decisions in one overview. I think that this helps. I would display the areas in the matrices by means of a diagonal border and by painting them green and red. Green is better than blue I think. The white areas are less clear I think.

6.
  - a. Possibly look at a quantitative analysis for the cost of controls. Tooling for the process modelling. The visualization of the controls shift as just discussed. Timing and governance of the methodology. I have for example not been involved in the risk analysis. This is what you see very often in practice at the customer. Involving the business side in the risk analysis and risk shift is very important.
  - b. The methodology is structured stepwise in a logical order and offers a lot more insight into the effect of redesign decisions you make. In practice a lot of designing is done based on what is better for the client and sometimes attention is also paid to the risks that emerge. Most of the time only a limited number of risks that have to be mitigated is focused on. But risks will also change and it is very useful to have an approach that enables you to pay attention to this during the redesign process. The power of this methodology is within the integration of the different concepts.
7. Yes I think so. I would use the body of thought behind it and not per se all exact steps within the methodology. For the exact execution of some tasks I would use the tools Deloitte already uses now. But the assessment and visualization of controls in both situation and looking at the shift of controls in terms of cost is very valuable. The methodology functions as a guideline and offers a good basis to develop further on towards a real approach that is also suitable to be used at clients. Added value for both Deloitte and the client.



