UNIVERSITEIT TWENTE.

MANAGING INFORMATION WITHIN THE THREE LINES OF DEFENSE TO ENSURE VALID AUDIT TRAILS

FINANCIAL SECTOR

A Practical Organizational Framework

COLOPHON

GRADUATION COMMITTEE

DR. M.E. IACOBS

BMS

IEBIS

UNIVERSITEIT TWENTE.

DR. M. DANEVA

EWI

SCS

UNIVERSITEIT TWENTE.

A. RAMKHELAWAN

IT RISK ASSURANCE

ADVISORY SERVICES

EY

N. HASPERHOVEN

IT RISK ASSURANCE

RISK

EY

DATE

19-06-2017

VERSION

1.57

STATUS

Final

PROJECT

Master Thesis Business Information Technology

AUTHOR(S)

Lukas Marinus Wielstra

MAILING ADDRESS

mailbox 217
7500 AE Enschede

WEBSITE

www.utwente.nl

PREFACE

This research represents the conclusion to my master study 'Business Information Technology' at the University of Twente. During my time at the University of Twente I learned a lot through studying and through extra activities within and around the university. I really enjoyed my time at the university as a student and I hope that I can apply the skills learned in the future in my daily job or other activities.

This research was conducted in cooperation with Ernst & Young Amsterdam within the IT Risk and Assurance department and several clients of Ernst & Young. The aim of this research is to develop an organizational framework that will support information management objectives and support internal audit operations.

First I would like to thank my University of Twente supervisors M.E. Iacob and M. Daneva for providing me with valuable feedback on my paper and overall support during the thesis process.

Secondly I would like to thank Ernst & Young for providing me with the opportunity to do my research in collaboration with them and their excessive network of clients. I would like to specially thank A. Ramkhelawan and N. Hasperhoven for actively helping me with understanding the problem statement and providing me with their expertise on the practical aspects of my paper. I would also like to thank K. Hozjan, other interviewees and discussion participants for taking the time to discuss my work in several sessions.

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

SUMMARY

Internal audit departments in the financial sector are struggling to acquire sufficient data with the right quality to perform the internal audit operations. On the other hand regulations and stakeholder requirements become increasingly strict, which forces companies to re-evaluate their internal audit function. The last financial crisis nearly a decade ago has increased the focus on assurance and compliance activities within companies. Year after year new regulations concerning corporate compliance to regulations have been deployed. Recently proposed regulations such as the GDPR [14] have put more emphasis for companies on knowing how their business processes function and on how data and information are used in the processes.

Most financial companies nowadays have structured their control mechanisms according to the three lines of defense framework of the Institute of Internal Auditors [27]. This framework, although providing a solid basis for control mechanisms and roles, does not provide companies with the right information management theory to ensure the third line of defense, or audit department, has all the needed data with the right quality to construct complete audit trails of business processes. This poses an increasing treat to financial companies. Therefore this research focuses on designing an organizational framework, based on the three lines of defense that improves information management within the three lines of defense to support internal audit operations. Concretely the following question is answered in this thesis:

> What is the appropriate framework for financial companies to govern information management within the three lines of defense to ensure complete audit trails in the third line of defense?

A number of literary domains play an important role in this paper and its artifact design, namely: Information management, risk management, governance, business process management, event data and process mining. These domains were combined in a research methodology to design the artifact of this paper available in appendix L.

The most important results of this research are:

- The combination of the literary domains in an action design science methodology [51] in order to develop the artifact of this paper.
- The development of design goals based on the literary relationships between the domains in accordance to the design science methodology and the operationalization of the design goals.
- The design of the artifact composed of: The “as-is” situation of the three lines of defense, representing the current situation. The “to-be” situation of the three lines of defense, focusing on improving information management within the three lines of defense to support internal audit operations. The migration plan, focusing on how a transition from the “as-is” situation to the “to-be” situation could be realized.
- The evaluation and validation of the artifact through several iterations of expert interviews and an expert discussion resulting in an alpha, beta and final version of the artifact.
- The artifact is generalizable to any company using the three lines of defense to structure control mechanisms using Bayesian logic [50] and therefore serves as the basis for a consultancy product for Ernst & Young. This research serves as an enrichment to their portfolio.
- The methodology provides a solid baseline for financial companies to restructure their three lines of defense and encourages a more data-driven internal audit approach.

TABLE OF CONTENT

INTRODUCTION

This chapter contains an introduction into the subject of this paper. In Chapter two the subject will be further elaborated upon and chapter three will contain the research proposal.

1. Introduction

The changing role of information technology in the business environment is nowadays one of the main drivers behind a company's asset management and business process development activities. As such traditional business processes have been interwoven with IT to increase efficiency and accuracy. As much as these business process enhancements have provided companies with enhanced ways of doing business, IT has also drastically complicated the nature and structure of companies. Economic events such as the recent financial crisis have proved that companies struggle to keep track of their business functioning and their assets. In the wake of the financial crisis, which left many business stakeholders affected, the focus towards governance activities have increased [39]. Internationally this has led to the development of the Sarbanes-Oxley act and the Basel acts. These acts turned even more attention towards governance activities [2] and have led to the development of several control frameworks and technologies. In the Netherlands several laws, such as the Wet Financieel Toezicht and the Wet Toezicht Accountingorganisaties [56], were revised. These revisions have drastically increased the power of controlling organizations such as the DNB and AFM. Even though the last financial crisis occurred almost a decade ago the emphasis on enhancing businesses control mechanisms and processes has not diminished, but rather increased. Recently the European Union has announced new regulations that aim at increasing data privacy, called the GDPR [14]. This law will be implemented in 2018, but the sanctions for companies that do not comply to this regulation are very severe. Sanction severity in turn forces companies to prepare data protection within their companies beforehand

The new regulations in combination with stakeholder expectancy drive companies to change the structure of their control processes by means of business process redesign. Aligning customer expectancy and compliance with control process performance often poses a challenge for companies [19]. Recently there have been developments towards automating parts of control processes, but automating control processes also poses a risk to a company in itself. Failures in automating control processes may threaten business continuity. As such it is vital that during automation all requirements derived from legislation are covered [19], [20].

Successes in automating control processes can drastically increase process performance and accuracy as well as save time and money. Automated processes also poses the computing capabilities to provide business intelligence by analyzing large datasets. Recent studies indicate that companies that focus on business information and analytics are twice as likely to be top performers [34], are on average 5% more productive and 6% more profitable [5], [38]. Increasing profitability and productivity as well as lowering costs of control processes might prove to be vital to the survival for some companies.

Ernst & Young consultants and auditors experience that some financial companies still struggle to keep up with enhancing their internal audit processes to the next level even though literature and best practices on the subject are widely available. When providing external audit activities for clients these problems to keep up with new techniques and best practices also has its effects on the work of the Ernst & Young auditors. Examples of problems arising from the inability to keep up with current practices are:

- Data needed for analysis activities is unavailable.
- Data needed for analysis activities is of poor quality.

Several clients of Ernst & Young have asked Ernst & Young IT Risk and Assurance for advice on this subject. For this reason this paper will dive deeper into the internal audit topic.

In order to develop an organizational framework that will help financial companies mature their internal audit processes a methodology has to be constructed. This methodology will be based on several questions proposed in this paper. These questions will cover several relevant theoretical topics as well as design aspects. This research aims to answer these questions by evaluating current best practices as well as theoretical and technological advancements. These aspects will be combined into a practical organizational framework. Keeping in mind that the practical organizational framework must help clients mature their internal audit processes to provide them with enhanced assurance capabilities. This research will provide valuable insights into the relations of internal audit processes, information management, compliance and data-driven audit automation. This paper will also provide Ernst & Young with a practical internal audit framework that helps them support and reform their clients operations.

2. Background

In this chapter some background information is presented that will help with understanding the problem statement concluding this chapter. This chapter will start with an analysis of the role of internal audit departments in financial companies. Furthermore we will analyze the relationship between business process management (BPM) and workflow management (WFM), technical aspects of different databases and the relationship between BPM, information management and internal control.

2.1. Internal Audit Function

The recent financial crisis has drastically increased the importance of governing internal controls in companies. Controls cover law and regulation requirements as well as serve as performance indicators. A well-known and widely applied framework to govern the functioning of the different control mechanisms inside a company is the three lines of defense model made by the Institute of Internal Auditors, or IIA [27]. Figure 1 provides a graphical overview of this model and its different lines of defense. The model builds upon the notion that the first line of defense owns and manages the risk, the second line oversees risk and the third line provides independent assurance. Respectively these functions are being performed by the operational department, risk department and internal audit department, or IA department. In some companies however the second and third line of defense and their respective functions are both performed by one entity, the IA/risk department [53]. The main activities of the IA department are: providing operational and business compliance to law and regulations and providing the company with correct reporting. Ideally

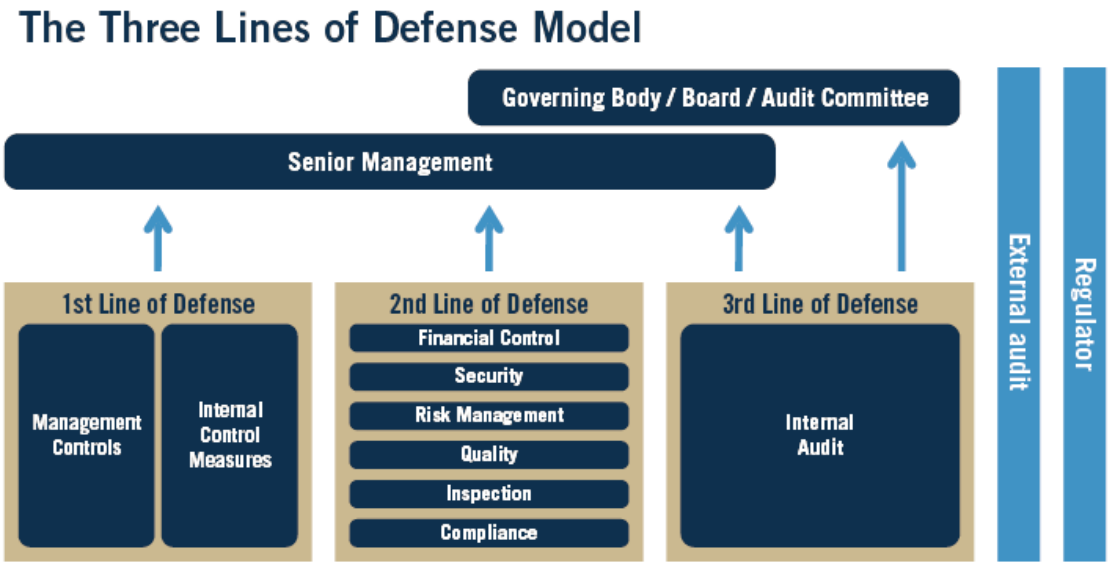


FIGURE 1. THREE LINES DEFENSE MODEL [27].

however the IA department should also focus on continuous business process improvement, but this is not a priority at the moment [44]. The problem statement will provide more insights into why continuous improvement is restricted at the moment.

2.2. Business Processes Management & Workflow Management

Before using the terms business process management, or BPM in this paper, and workflow management, or WFM, we will first go through a short analysis of their historic background. It is important to note that BPM and WFM are strongly related. WFM came up in the nineties and involves the automation of business processes and involves the information that is created during a process [58]. BPM involves supporting business processes using software, methods and techniques with the aim of controlling and analyzing the performance of these business processes [58]. Therefore it is possible to say that BPM encompasses WFM, but also involves controlling and analyzing performance [58]. Important to remember is that data stored during business processes is vital in the control functions of these processes and the overall business.

2.3. OLTP & OLAP Relation to Data Management

We will now explore the more technical aspect of data management by looking into the background of different database technologies and defining their advantages and disadvantages. Online transaction processing databases, or OLTP databases, and online analytics processing databases, or OLAP database, are two different kinds of databases that serve two different types of business needs. Within financial companies there are many systems that are used to register various data about various products and other business related subjects. OLTP databases are relational databases build for speed that support the business need of performing day to day activities of employees [8]. Shortcomings of OLTP databases are that it is very hard to do analysis on the data in the databases, which makes them less suited for performance control activities [8]. OLAP databases serve the need of gaining business intelligence by providing the opportunity to do analysis on them [8]. OLAP databases are preloaded with information from OLTP database and pre-construct different relations within the data to provide analysists with a direct view of data relations when they need them. Loading OLAP databases with OLTP information takes a lot of time and therefore it is hard to gain real-time insight in business information [8].

2.4. Business Process Management, Internal Control & Information Management

Compliance is primarily bound to managing three risk categories. These risks are: Operational risk, information technology risk and information risk. The first two risks are nowadays very well incorporated into corporate risk management, but information risk management is a relatively unexplored field that spans over parts of operational risk, It risk and other risk categories such as strategic risk, financial risk and compliance risk [24]. At the moment some of the Information risks are often managed by information security personnel and not by the risk department. From the theory behind BPM we can derive that correct information management is vital in the process of controlling and analyzing business process performance. Therefore information management can help companies improve upon their

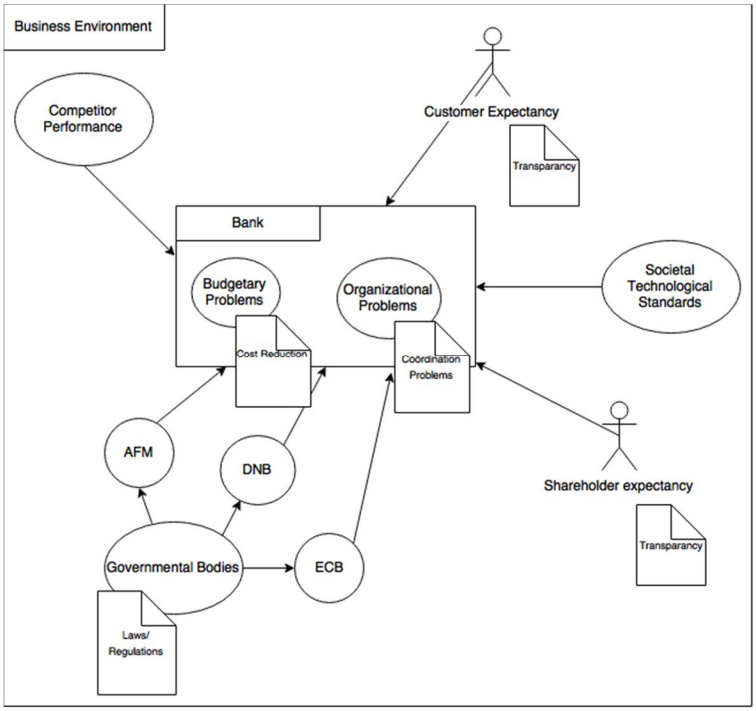


FIGURE 2. BUSINESS PROCESS MANAGEMENT STAKEHOLDERS & DRIVERS FOR A BANK

processes by making them more flexible, less costly, deliver better quality and reducing the processing time [47], [58]. It is important to note that BPM is driven by external and internal stakeholders and technological capabilities [40], [10]. Recent new drivers such as the GDPR, competitor performance and customer expectancy drive financial companies towards improving their information management and providing better compliance assurance as a whole. Furthermore it is noteworthy to state that companies that excel at information management and the governance of the risks that accompany information are in a better position to generate business intelligence from their big data [38]. Current technologies already allow for real-time business intelligence, which can support businesses greatly in their strategic operations and decision making. The process of information management starts at the data itself. From a high level point of view the data collection and retrieval process contains of two steps. Getting data into the company and getting data out [58]. This paper will focus on finding out how to govern the first step from the moment data enters the company to the moment it is used again for internal audit tasks. It will encompass data requirements and frameworks needed for correct information management.

2.5. Problem Statement

It is important to note that the problem of this paper is an information management problem within the three lines of defense, which results in an assurance problem in the third line of defense. Therefore the problem is a people, process and technology problem and spans over multiple layers of a financial company. We will look at the problem from a bottom-up approach, because the operational bottom of a company is the point where data enters the company. As such we will analyze the three lines of defense from line one to three accordingly. This paper focuses at improving information management within the three lines of defense to enhance internal audit performance.

When a customer has interaction with a financial company the correct operational department of the company will invoke and instance of the appropriate business process and proceeds to alter and add data to the appropriate IT systems in order to make sure the customers' needs are satisfied. It is important to note that one business process often spans multiple IT systems, so data from the business process instance is stored in multiple OLTP databases. Figure 3 provides a visual representation of an exemplary registration process. The employee then documents his or her actions performed conform the standards used within the operational department. The operational management of the department manages the risks owned by the department. This set of risks often does not contain many information risks however. The risk department of the company oversees the risks, but does often not include many information risks as said.

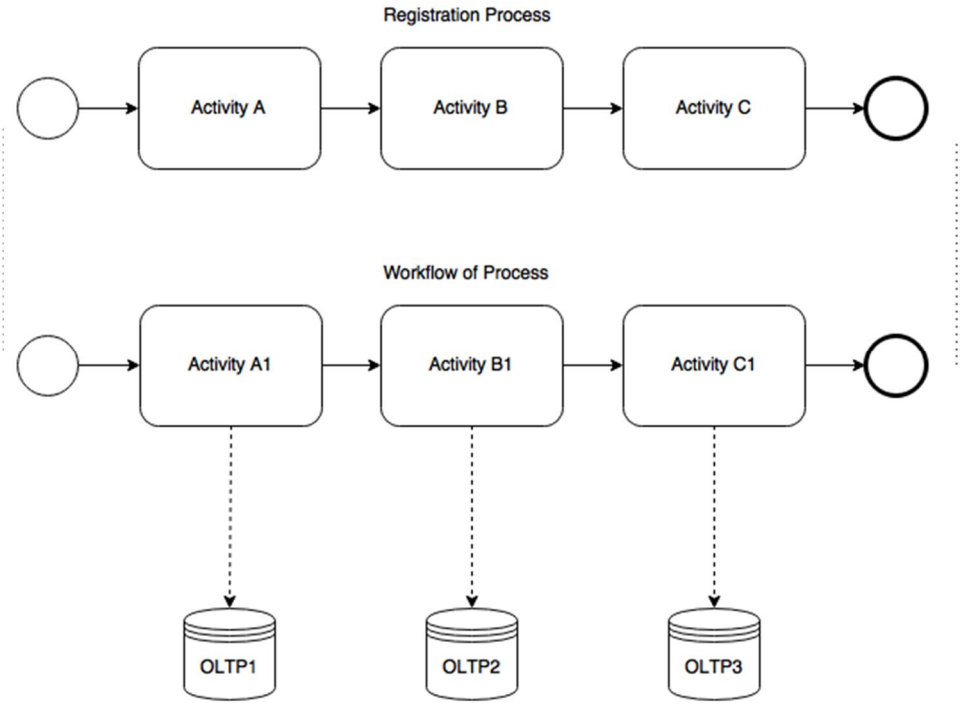


FIGURE 3. DATA STORAGE OF AN EXAMPLARY REGISTRATION PROCESS

The role of the internal audit department, is to control the work of the operations department employee as well as assessing the risk department's performance. The problem however is that during the business process instance invoked by the employee, data has been stored in different OLTP databases and the employee has only documented his or her activities to the standards of the operational department, without thinking about the complications for the IA department. The IA department now has a data quality and shortage problem that restricts them in their work [58]. The IA department now has to search in multiple OLTP databases to find evidence for the correctness of process handling. Figure 4 provides a visual representation of an analysis of the exemplary registration process.

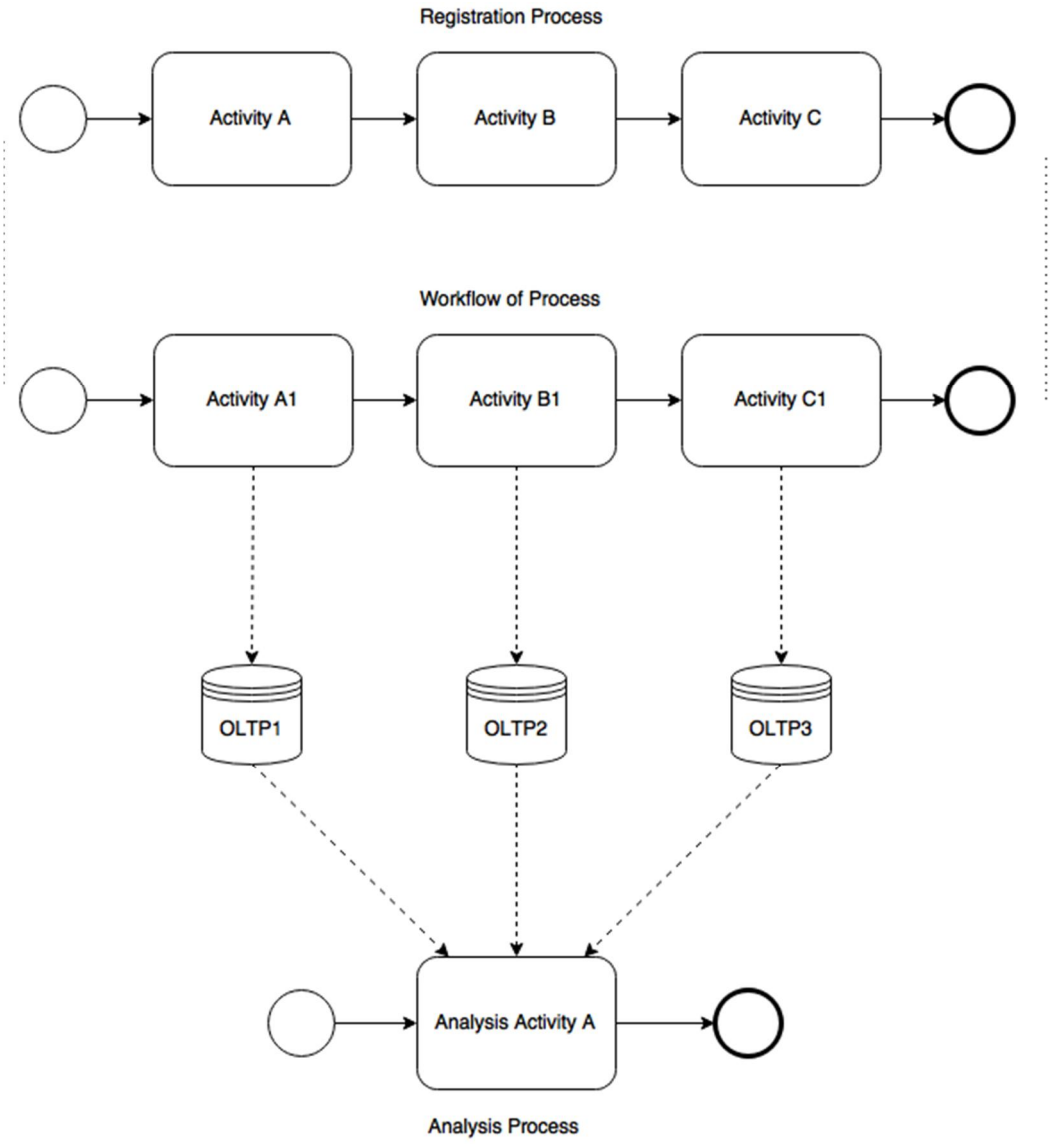


FIGURE 4. ANALYSIS OF AN EXAMPLARY REGISTRATION PROCESS

3. Research Proposal

This chapter explains the outline of the research paper. It will first explain the underlying theoretical framework in section 3.1. Section 3.2 focuses on explaining the empirical framework of this paper. In section 3.3 the scope of this paper will be elaborated upon. Section 3.4 will explain the main research question of this paper and the sub questions derived from the main question. Section 3.5 will explain the research relevance. In section 3.6 the research methodology of this research will be discussed. This chapter will conclude with the research overview.

3.1. Theoretical Framework

The theoretical framework will be based on the concepts introduced in chapter two of this paper. Namely Information management, BPM, OLAP, OLTP and their relationship with internal audit and continuous improvement. These concepts will be further elaborated upon in the literature review of chapter four.

3.2. Empirical Framework

Based on the background description of the previous chapter and the problem statement a conceptual theoretical framework of the current situation will be constructed. With help of experts in the field this conceptual framework can be validated and evaluated through multiple iterations. This repeating cycle will result in an improvement framework artifact as described in the action design science paper of Sein et al. [51].

3.3. Scope

This chapter will elaborate upon the scope of this paper as agreed upon with both the external Ernst & Young supervisors and the internal University of Twente supervisors.

As the focus of this paper is to establish a framework that will help manage information within the three lines of defense it is important that we first start at the theoretical basis of risk management and information management. Because of the limited time provided for finishing this paper we will focus on:

- Risk frameworks most often used by companies in the field.
- Usage of data within the audit functions of the IA department.
- Information management frameworks that can be used in business control processes.
- The three lines of defense model of the IIA.
- Internal IT and operational audit primarily.

Furthermore it is important to note that this paper focuses on unintentional errors in business processes and less on intentional errors, such as cybercrime. Reasons for this are that intentional errors often require extra investigation theory. Much of the work in this paper is however expected to also touch the cyber security management field.

Furthermore this paper will focus on exploring practical aspects of the theoretical topics used in this paper, such as the usage of event data files in internal control. This will include:

- Log file requirements.
- Theoretical frameworks for log file usage in control processes.
- Practical implementations for log file usage.

3.4. Research Questions

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

> What is the appropriate framework for financial companies to govern information management within the three lines of defense to ensure complete audit trails in the third line of defense?

This research questions, the scope and the problem statement assume three things:

- Financial company's systems of the "as-is" situation must be able to log process information in order to be able to use this in the "to-be" situation.
- There has to be a methodology to automate internal audit processes using process log files.
- There have to be practical options available to use log files for the purpose of audit processes.

In order to answer the research question, several sub questions have to be answered. The sub questions are as follows:

Risk Management & Information Management

1. What are the different corporate risk categories and how do they relate and differ?
2. What are well established risk frameworks?
3. How is information management related to risk?

Business Processes Management & Information Management

4. What is the relation between business processes and information management?
5. What information management theories are available that encompass business information derived from business processes?

Log Files & Information Management

6. What are the requirements for log files in order for them to be useful in internal audit?
7. Are any log file frameworks available that support the necessary requirements, so that practical usage is possible?
8. How can log files contribute to internal audit processes?
9. What practical applications are already available that use log files for audit purposes?

Design

10. Can we define a framework that helps financial companies with information management to support internal audit operations?
11. How can we evaluate the effectiveness of this framework on information management in the internal audit context?

3.5. Research Relevance

At the moment IA departments in financial companies are struggling to provide assurance for correct business process executions because business processes are executed in multiple systems within the financial company and data about these executions is hard to locate and use for audit purposes. In addition to this OLTP databases are not easily used for analysis tasks. Because of this struggle some errors or fraud attempts have not been noticed by internal audit departments, which has led to reputation damage at ABN Amro for example. In this example multiple employees fabricated signatures of customers to close dossiers [42]. The Institute of internal Auditors (IIA) has also stated the need for "whistle blowing programs" as well as the introduction of a compliance culture that fulfill the need for better IT control in financial companies in their Hot Topics for 2017 document [26].

This research is expected to have the following contribution to theory and practice:

- Extending theory about information management in the internal audit function.
- Extending theory and practical knowledge about the usage of event data files in internal audit control processes.
- Providing Ernst & Young with a framework that helps them in their advisory role to organize information management within the three lines of defense of their clients.

3.6. Research Methodology

This research contains several iteration steps, which will be elaborated upon briefly in this chapter. Figure 5 provides a visual representation of the steps in this paper.

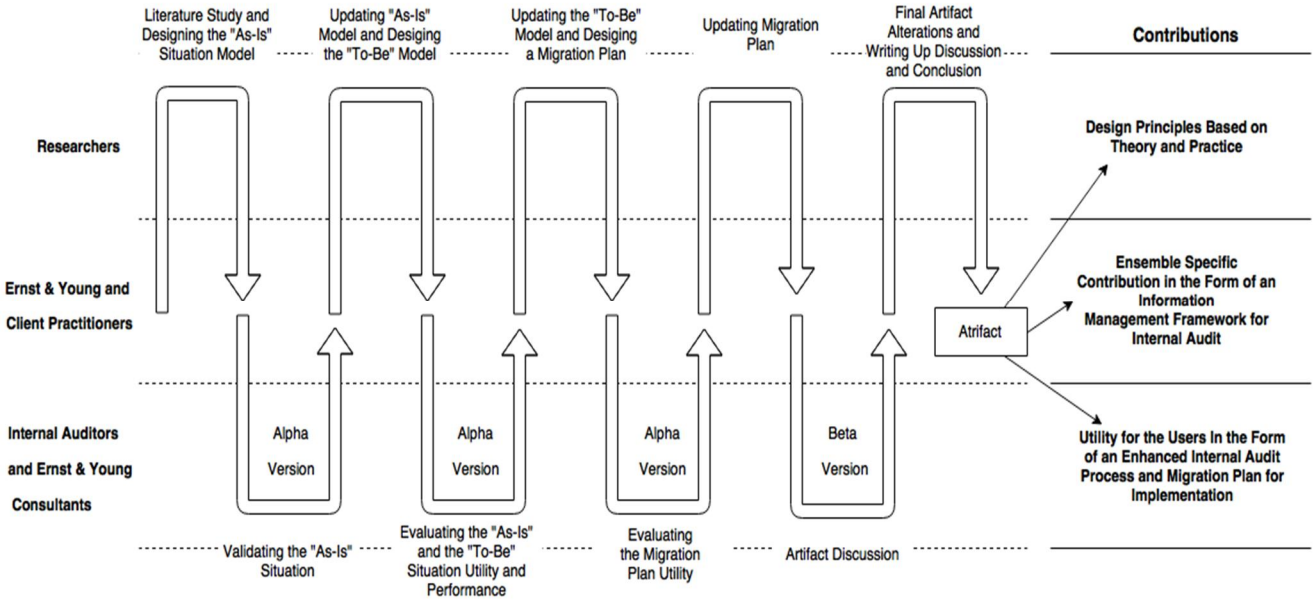


FIGURE 5. RESEARCH METHODOLOGY.

The first step in this research contains of a literature study towards the concepts introduced in the previous chapters and their links. In the literature study a combination of academic and practice literature will be used. The focus of this study is to provide frameworks and other literary topics, which will serve as a background for the artifact that we will create in this paper. In addition to this the conceptual model of the current situation way of working in internal audit will be designed. The second step in this paper will be to validate the conceptual “as-is” model designed in the first step. This will be done through means of expert interview with internal audit professionals. It is vital for this research that the “as-is” model is correct, because it will serve as a baseline for the “to-be” model designed in step three. In the third step the feedback on the “as-is” model will be integrated in the redesign. In addition to this a stakeholder driver analysis and a requirement analysis for the “to-be” situation will be conducted. Based on the outcome of the requirement analysis a “to-be” model will be designed. The fourth step will be a gap analysis between the “as-is” and “to-be” situations to determine if the “to-be” model will result in any information management performance increase and is tested positively to the technology acceptance model, or TAM [41]. In the fifth step the “to-be” model will be updated conform the feedback and a migration plan to reach the “to-be” state will be developed. The sixth step will be composed of a reevaluation of the updated “to-be” model and the evaluation of the migration plan using the TAM model again [41]. In the seventh step the migration model will be updated according to the feedback provided. In the eight step an Ernst & Young internal discussion will be conducted to validate the beta version of the artifact, consisting of the “as-is“ situation, the “to-be” situation and the migration plan. The final step consists of drawing up the results of this paper and presenting conclusions and discussions on the topic.

This research methodology is based on the theoretical approach of Sein et al. shown in figure 6 of the left hand side [51]. On the right hand side step two is presented in more detail as described in the Organizational-Dominant BIE model of the Sein et al. paper [51]. According to this methodology an action design research paper should cover all four steps of the model. The steps are as follows:

- Problem formulation
- Building, intervention and evaluation
- Reflection and learning

· Formalization of learning

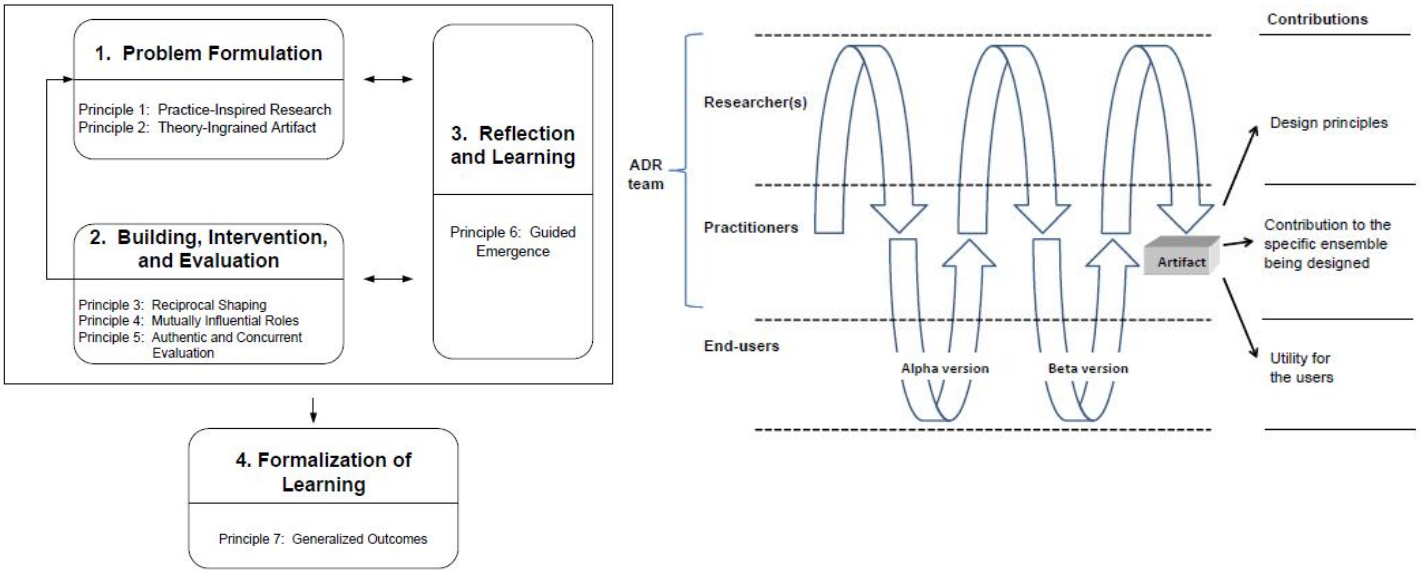


FIGURE 6. ACTION DESIGN RESEARCH METHODOLOGY (ADR) [51].

To demonstrate that all steps are being followed in this paper we will map our paper on the action design research methodology of Sein et al. shown in table 1.

TABLE 1. MAPPING OF THIS THESIS ON ADR

Sein et al. Methodology	Research Paper
Problem formulation	Problem statement formulation based on observations from Ernst & Young and based on theory on the subject.
Building, intervention and evaluation	Building of the “as-is”, “to-be” situations and the migration plan through several iterations and evaluating these models through expert interviews.
Reflection and learning	Development through direct input from the intentional users.
Formalization of learning	Development towards a generalized organizational framework to govern information management within the three lines of defense.

3.7. Research Overview

In order to answer the research question of this paper some sub questions have to be answered. In order to ensure complete coverage of all the sub questions we have constructed table 2 to track the progress and location of the answers to the sub questions.

This thesis will consist out of four parts. Part one is the research introduction. Part two consist of the information gathering from literature and practice. Part three consists of the design of the framework. Part four will cover the results and conclusion of this paper.

TABLE 2. RESEARCH OVERVIEW

Research Question	Answered In	Methodology	Outcome
Risk Management & Information Management			
What are the different corporate risk categories and how do they relate and differ?	Part 2 Literature study	Literature study	Six categories and they overlap.
What are well established risk frameworks?	Part 2 Literature study	Literature study	COBIT, COSO, ISO/IEC 27001.
How is information management related to risk?	Part 2 Literature study	Literature study	Control focus in risk and data focus in information management.
Business Process Management & Information Management			
What is the relation between business processes and information management?	Part 2 Literature study	Literature study	BAM covers the three columns and rows of the Maes framework.
What information management theories are available that encompass business information derived from business processes?	Part 2 Literature study	Literature study	IM Framework and KMC.
Log Files & Information Management			
What are the requirements for log files in order for them to be useful in internal audit?	Part 2 Literature study	Literature study	XES standard extension list.
Are any log file frameworks available that support the necessary requirements, so that practical usage is possible?	Part 2 Literature study	Literature study	MXML format and mining meta model.
How can log files contribute to internal audit processes?	Part 2 Literature study	Literature study	Process mining opens up a data driven control approach.
What practical applications are already available that use log files for control purposes?	Part 2 Literature study	Literature study	Process Mining tools and BAM Systems.
Design			
Can we define a framework that helps financial companies with information management to support internal audit operations?	Part 3 Design	Design	Figure 41 of this paper provides a framework and the information transfers within the framework.
How can we evaluate the effectiveness of this framework on information management in the internal audit context?	Part 3 Design	Design & Discussion	Interviews and discussion with Experts.

INFORMATION GATHERING

4. Literature Study Framework

This chapter provides an overview of the literature used in this paper and the method used to find the needed literature. A literature study is needed in order to provide insight in the theoretical context of the concepts introduced in the first part of this research. This literature study will first investigate the relationship between risk and information management, next the relationship between BPM and information management will be investigated and lastly the relationship between log files, information management and internal audit. Section 4.1 explains the strategy used to find literature for this thesis. 4.2 Explains in what way the papers have been analyzed.

Figure 7 explains in what order several relevant concepts to this paper will be investigated in the literature study and as such shows that our literature study will start with gaining knowledge about several high level concepts and will move towards more low level, practical concepts. First of all we will look into established risk categories and governance. Secondly we will combine this knowledge with current risk frameworks. The combination of risk categories and risk frameworks will give us insight into the relationship between risk and information management. We will further investigate established information management frameworks. Furthermore we will look into practical aspects of information management in the field of business processes management (BPM). Next we will investigate the relationship of log files, or event data, to information management in an attempt to clarify if they can be used in the design. Lastly we will look into any requirements for log files when using them for internal audit information audit purposes.

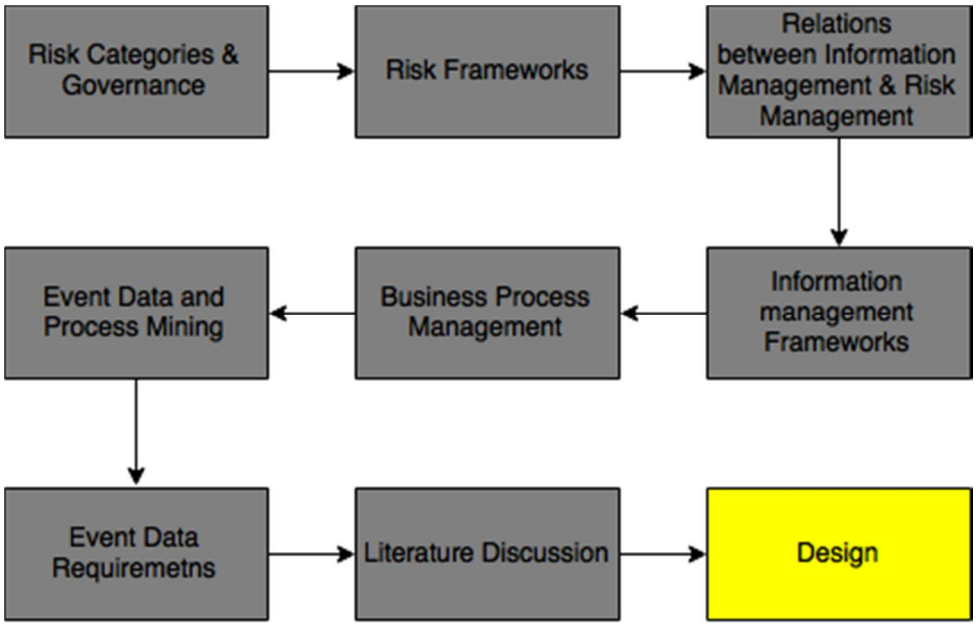


FIGURE 7. LITERATURE STUDY STEPS.

4.1. Literature Study Strategy

The literature review has been conducted in a semi-structured way. Key words relevant to the problem context provided by the supervisors and proposed by us have been used. The following search strategy has been used, which is inspired by the paper of Levy et al. [35].

- Key words: Important key words are used in search queries. These key words are either provided by interviews with supervisors or are taken from the research introduction of this paper. The key words are

either queried separately or relating concepts have been queried together. During the literature review new related concepts were introduced and were also used in the literature study queries. This approach is called the concept-centric approach [35].

- Relevant authors: Search queries containing important authors in the field of the concepts have been used. Some authors are publishing mainly on the concepts relevant to this paper and therefore their names are used to query for papers. This is called the author-centric approach [35].
- Finally the references of relevant papers have been analyzed to find additional relevant papers about the concepts.

The database used in this paper is Google Scholar, because it is a very large database which covers multiple relevant journals and conferences. The richness of the database fits the diversity of the concepts searched on in this literature review. In addition to this some articles were provided to me by Ernst & Young and some open source articles were acquired from the sites of the author institutions [28], [43], [54], [11], [12], [13].

4.2. Literature Study Way of Working

During the literature study a way of working was used by us in order to analyze vast amounts of papers and select only the relevant papers to our research questions and their relevant concepts. This way of working was based on several practical straight forward indicators that provided insight into the relevance of the paper. These indicators towards the relevance of the papers are as follows:

1. Relevance: The first twenty hits of a search query in google scholar were used to find relevant literature.
2. Title: Scanning the titles of papers indicates their relevance to our paper. These papers were further analyzed to validate their relevance to our research.
3. Abstract & Conclusion: Papers with a relevant title were further investigated by scanning their abstract and conclusion to ensure relevance to this paper.
4. Publication Year: No papers older than 2000 were used in this paper, with the exception of some core papers. The reason behind this is that the turnover time of IT is very high. In addition to this a lot of compliance regulations were added since 2008.
5. Number of citations: Since Information management is relatively unexplored a minimum of five citations is used to include papers.
6. Author names: Papers written by authors of other relevant literature are check substantially to find out if they are relevant.
7. Accessibility: For practical reasons only papers that are available to the University of Twente are used in the literature study.

The reason for using such a way of working is to make sure the literature study was conducted systematically and all papers were treated in the same way.

4.3. Practitioner's Literature

During interviews with Ernst & Young Nederland LLP employees and other experts in the field of internal audit some practitioner's literature was handed to me. These papers are not deemed as academic literature and therefore do not share the same quality standards. These papers were however relevant to this thesis, since the best practices described in this paper are used in practice and the artifact design of this paper will focus heavily on practice [13], [11], [12] .

5. Literature Study

In this chapter we will discover relevant topics to this paper's problem statement and questions. We will proceed with this as indicated in chapter 4 by starting at the high level abstract topics relevant to our thesis and working towards the low level concrete topics. As such we will start with analyzing risk and governance in section 5.1 and 5.2. We will then look into the definition of information management in section 5.3 and 5.4. In section 5.5 we investigate the relationship between business process management and information management. In section 5.6 we will conclude by investigating event data aspects relevant to our paper.

5.1. Governance, Risk & Risk Management

RISK & RISK MANAGEMENT

In the corporate environment the term governance, risk and compliance (GRC) is often used in the context of control processes and mechanisms. Although this term is widely used there is only few literature available on integrated approaches that combine these three aspects [45]. In order for us to gain insight into the relationships of these concepts we will first look into risk literature. According to Humphreys risk is the byproduct of uncertainties posed upon a company by the ever changing environment that surrounds the company [23]. As the business environment is most often beyond the control of a company's influence, so are the uncertainties that accompany it. In order to anticipate the impact of these uncertainties on the company, risks will be allocated to the uncertainties. A company will in turn aim at managing these risks in order to mitigate them. Because of the volume of risks to a company and the fact that the changing environment also changes risks and adds and subtracts risks from the company risk agenda, risk literature has aimed to categorize risks into six categories of risk. These risks are: Technology risk, operational risk, strategic risk, compliance risk, financial risk and information risk [24]. For this paper the relationship between the three risk categories information risk, technology risk and operational risk is most important. This relationship is shown in figure 8 [24]. Noticeable is that these risks share certain characteristics but have a completely different focus. ORM focuses on the business processes in a company, while TRM focuses on the systems used in those processes and IRM focuses on the information used and stored in these processes.

FIGURE 8. RISK CATEGORIES RELATIONSHIP [24].

Technological risks and operational risks are nowadays very much incorporated in business risk management agenda of the risk management departments that resemble the second line of defense of the Institute of Internal Auditors model [27]. However information risk is a relatively new field in both academic literature as well as business practice. As a result IRM is not treated as a separate discipline but is partly incorporated into the other risk categories. This does however also mean that it does not receive the same attention as the other risk categories [24], [12].

In order to answer the research questions of this paper we will further investigate the practice of risk management. To understand this however we must first accept that risk management is a multidisciplinary practice that covers Human behavior, IT system opportunities and limitations and process aspects of the tasks that are performed in the company [6], [24]. According to literature the main functions of the risk department are as shown in figure 9 [23], [45], [28].

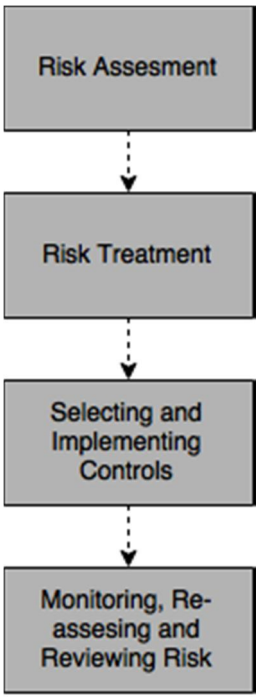


FIGURE 9. RISK MANAGEMENT [23].

Risk assessment is the practice of identifying the risk, registering them and calculating the risk level to the company. Risk level can be calculated as follows [23]:

- Risk level = exposure x Impact to company.

Risk treatment is the next step in risk management and involves the company's response to the identified risk. ISO/IEC 27001 distinguishes four types of responses namely [28]:

- Risk acceptance – accept the risk as it is.
- Risk aversion – Modify the process so the risk disappears.
- Risk treatment – implementing controls to reduce the risk.
- Risk transfer – Using insurance or contracting out the risk.

The third step is selecting and implementing controls to treat risks. The difficulty of this is choosing the right controls that cover the risk and implementing them in such a way that it enables you to control the risk. The last step involves monitoring the controls and risks. Re-assessing the risks is important because the environment in constantly changing.

GOVERNANCE

Governance focuses more on the human aspect of the business. The governance process is often invoked at the management layer of the company. The management of the company decides on the strategy of the company and decides what role IT plays in this strategy. Furthermore accountability for organizational changes is assigned to different people. The company strategy is communicated top-down to the operational management. The operational

management translates this strategy into policies and implements those policies in their department. Feedback from the implemented policies is send bottom-up so management can adjust accordingly [61].

When designing our artifact in the design phase of this paper we must remain aware of how the second line of defense is practically implemented and how this relates to the internal audit department [27]. In addition to this it is important to know how and in what direction information is shared within a company.

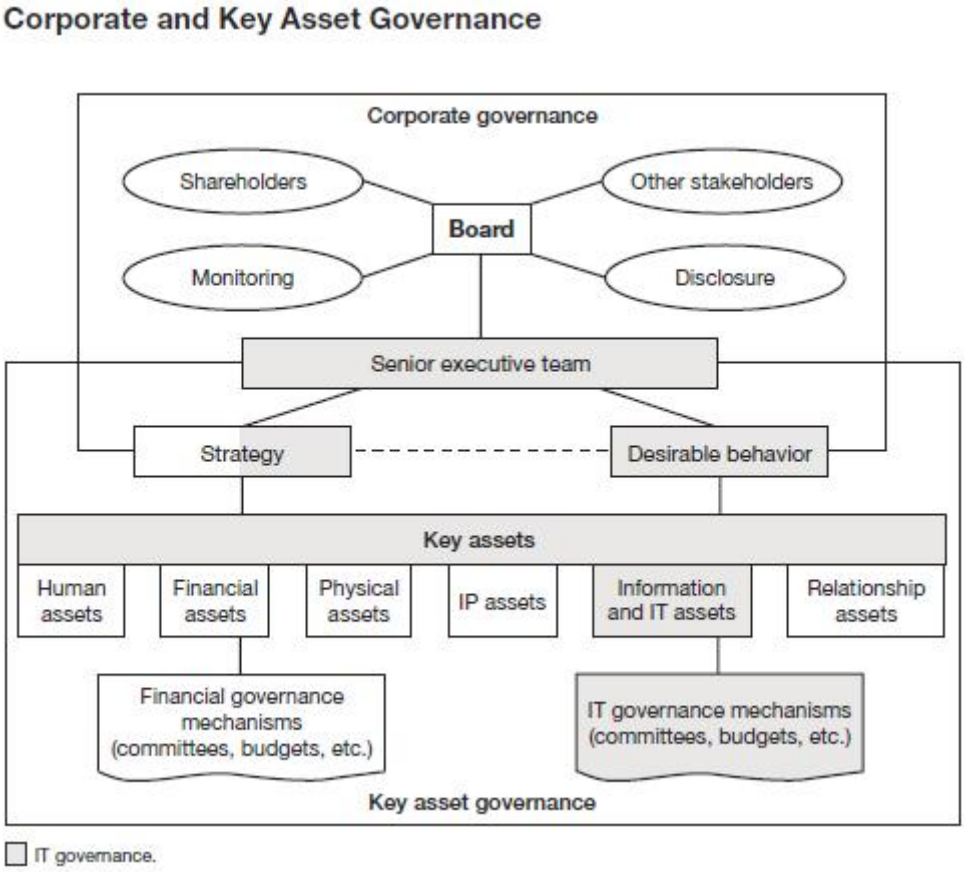


FIGURE 10. GOVERNANCE STRUCTURE [61].

5.2. Risk Frameworks

COSO INTERNAL CONTROL FRAMEWORK

As a response to the tighter government regulations of the Sarbanes-Oxley act some sector initiatives were taken to come up with a framework for organizational governance, risk management and internal control. The Committee of Sponsoring Organizations of the Treadway Commission framework, or COSO framework, is one of the result of these initiatives and is nowadays widely used in the industry. COSO explains internal control as follows and the framework is based on this notion:

"Internal control is a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance." [39].

FIGURE 11. COSO FRAMEWORK [7].

This business structure is exactly what Ernst & Young encounters at their clients and conforms to the three lines of defense model of the IIA [27]. The role of "other personnel, designed to provide reasonable assurance" is filled in by an IA department, operational management and risk department. The authors of the COSO model are aware that they use a very broad definition of internal control to satisfy all possible conditions of different industries in which the model can operate [7]. This however does mean that COSO is very high level and harder for practical implementations. COSO's basics consists out of three objectives which according to the framework can be achieved by performing well in the control components of the framework. The three objectives are explained as followed [7], [39]:

- Operating objective: These pertain to effectiveness and efficiency of the entity's operations.
- Reporting objective: These pertain to internal and external financial and non-financial reporting.
- Compliance objective: These pertain to adherence to laws and regulations to which the entity is subject.

COSO consists of five components explained as follows by COSO [7], [39]:

- Control environment: A set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.
- Risk assessment: Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.
- Control activities: Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
- Information and communication: Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management.
- Monitoring activities: Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning.

In an attempt to make the control components more concrete the components are divided into seventeen principles which are described in figure 12. The COSO components influence each other, where output information from one component can be input for another. The COSO process is iterative and multidirectional in usage. Internal control within a company starts at the top management of the company at the entity level. Management directions will be interpreted and implemented by divisions, operating units and lastly it will be interpreted and implemented on a functional level by individuals.

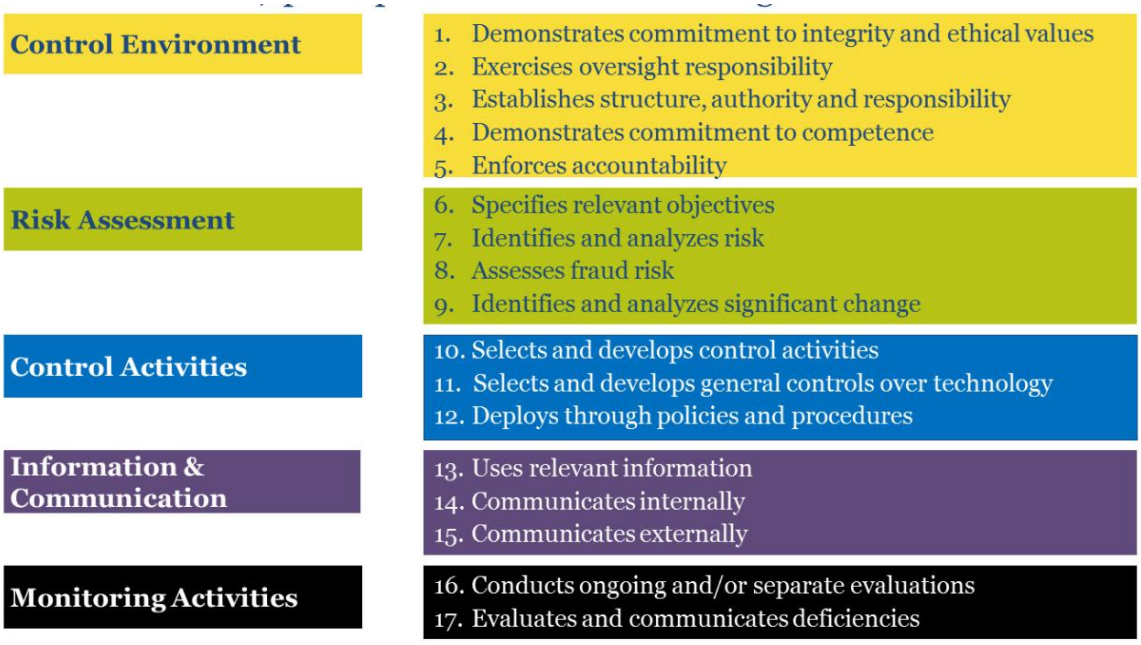


FIGURE 12. INTERNAL CONTROL PRINCIPLES [39].

COSO originally focused at external reporting in an effort to make companies compliant to external regulations but since 2013 the framework has been reworked. For this rework COSO also looked at the benefits of extending the framework to internal reporting to make companies more data-driven [39]. Internal auditing should perform control self-assessments (CSA) to evaluate their business performance in addition to external auditing. Depending on the nature of the control it might be possible to automate these CSA. According to COSO the combined strength of internal audit, external audit and enterprise risk management (ERM) processes will allow companies to achieve the strategic, operational, reporting and compliance objectives.

COBIT INTERNAL CONTROL FRAMEWORK

The Control Objectives for Information and related Technology, or COBIT, is an open standard widely used by companies in the field. COBIT is one of the more practical frameworks used by companies in aligning information technology with business goals. The framework itself puts emphasis on the business needs satisfied by the different control objectives [48]. COBIT is set-up to control IT within firms, shortly referred to as IT governance. Korac-Kakabadse et al. describe IT governance as follows:

"IT governance is the structure of relationships and processes to develop, direct and control IS/IT resources in order to achieve the enterprise's goals" [31].

COBIT is therefore based upon five principles as represented in figure 13. One of the core principles is that it aims to separate management from governance. This can of course only be achieved if COBIT helps fulfill all the stakeholder needs and therefore covers the organization from end-to-end. For this reason it provides a holistic approach encompassed in one framework [25].

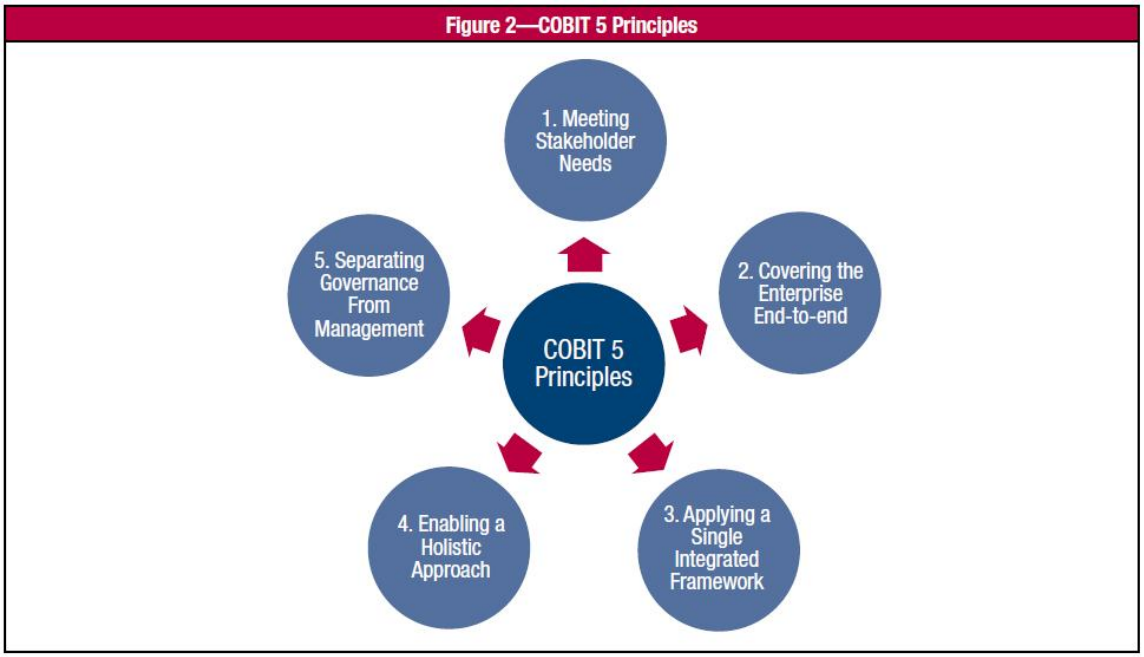


FIGURE 13. COBIT 5 PRINCIPLES [25].

In the COBIT framework IT-governance is divided into 32 processes, each with their own high level control objectives. These processes are distributed over four domains which are based on the standard plan-do-check-act (PDCA) cycle used in a number of frameworks. The domains are called as follows:

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

Distribution of the processes over the domains is illustrated in figure 14. Noticeable is that previous versions of COBIT 5 were much less focused on IT Governance and more focused on an IT process model framework and therefore lacked the focus on information security and quality management [52]. As the COBIT framework describes a more what-to-do approach towards IT governance it can be seen as an extension of the COSO model which is overall more high level.

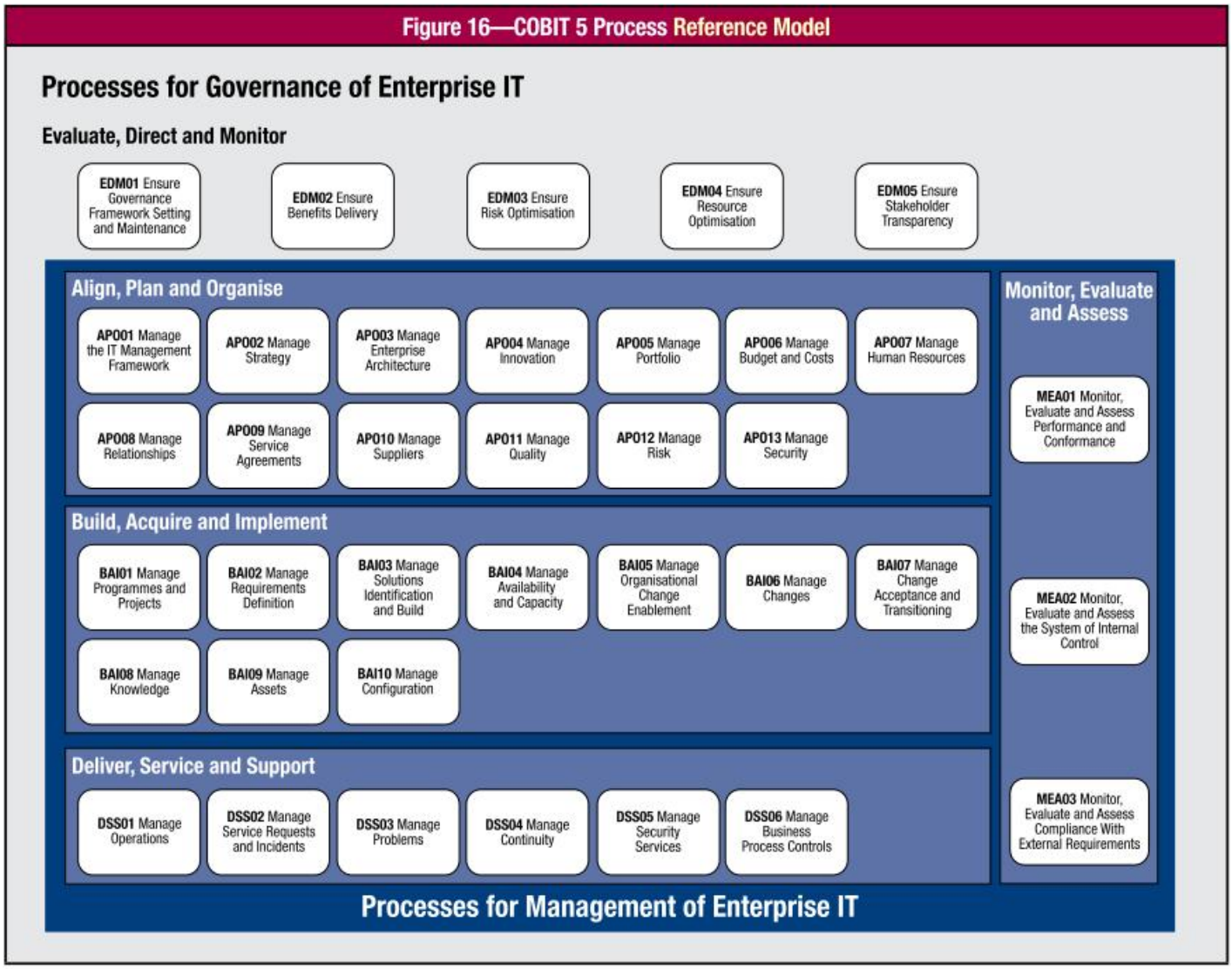


FIGURE 14. COBIT 5 FRAMEWORK [25].

ISO/IEC 27001

ISO/IEC27001 is a standard belonging to the family of ISO/IEC standards that are widely used in practice by companies from a wide variety of industries. This particular ISO/IEC focuses on information security management systems, or ISMS, and can therefore be regarded as important to the topic of our paper. ISO/IEC 27001 closely resembles the COBIT framework, but is more specialized on information security [52]. Even though ISO/IEC 27001 closely resembles COBIT and COBIT is widely used in practice ISO/IEC 27001 is not [17]. Within academic literature however the concepts of ISO/IEC 27001 are used a lot and therefore we will investigate into ISO/IEC 27001 in this paper [46], [17], [23], [52].

Identically to COBIT ISO/IEC 27001 is also based on a plan-do-check-act (PDCA) approach described in figure 15. Additionally ISO/IEC 27001 also prescribes a set of high level control domains described below [52]:

- Security Policy: Management commitment to information security policies.
- Organizational Information Security: Defining responsibilities towards information security and providing an overall coordination of security activities.
- Asset management: All critical assets are defined in this domain.

- Human Resource Security: User awareness and training.
- Physical Environmental Security: Physical access protocols.
- Communication and Operation Management: Domain involving the risk of failure and the resulting consequences.
- Access Control: Cyber access protocols.
- Information Security Incident Management: Security event reporting structure and responsibilities.
- Information System Acquisition, Development and Maintenance: Domain involving the loss and misuse of information in applications.
- Business Continuity Management: Domain involving the incident response structure and the procedures that enable business continuity.
- Compliance: Domain addressing the legal compliance and the establishment of business objectives.

ISO/IEC 27001 can be used as an addition to COBIT, but will overlap on most subjects [45].

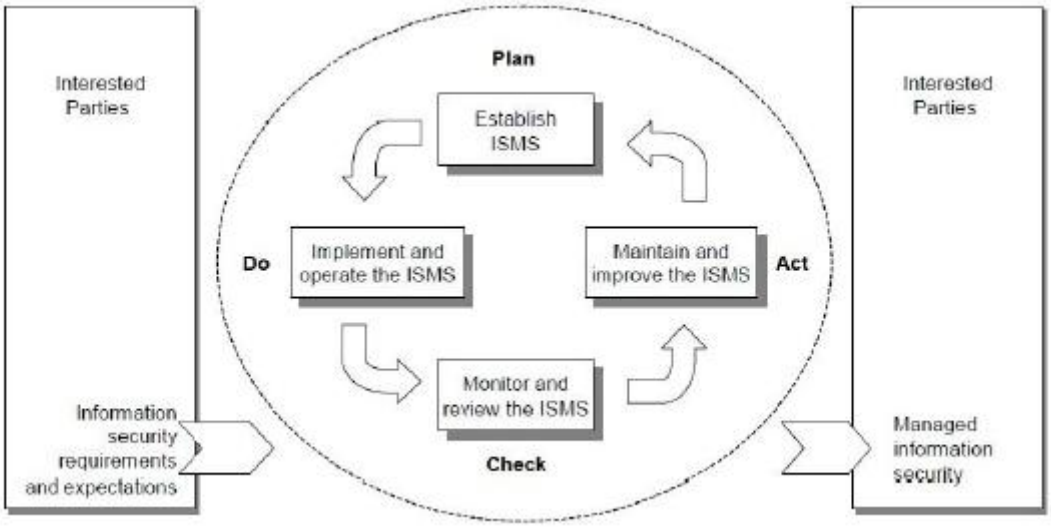


FIGURE 15. ISO/IEC 27001 CODE OF PRACTICE [52].

CONTROL FRAMEWORK OVERVIEW

COSO and COBIT are two risk governance frameworks that are used a lot in practice. Originally those frameworks did not focus much on information security and information management. There have been standards such as ISO/IEC 27001 that focused on these aspects, but were much less adopted due to factors such as the price of certification [17]. This has resulted in a corporate culture in which information security and management was not treated as a separate discipline and therefore semi neglected [17], [52]. After critics from the scientific community COBIT 4 was revised and expanded to COBIT 5 [55], [52]. COBIT 5 incorporates information security and management subjects and framework to establish a holistic IT governance framework. COBIT, although more practical than COSO, still proposes very high level controls and therefore companies might still struggle to implement information management and security in their business processes.

The nature of the three frameworks discussed in this paper provide us with more insight into the functioning of the first and second line of the three lines of defense model [27]. When designing the artifact of this paper we will have to apply this knowledge to support certain parts of the third line of defense.

5.3. Information Management & Risk Management

INFORMATION DEFINITION

In order for us to expand upon a literature analysis on the topic of Information management we will first briefly go into the definition of information used in this paper and the scientific community. In the field of philosophy the concepts of data, information, knowledge and wisdom are highly disputed [4]. This paper does not go into the relationship of these four concepts as this is out of scope for this project. Instead we will use the widely accepted hierarchical data, information, knowledge and wisdom framework, or DIKW framework, first proposed by Ackoff in 1989 [1]:

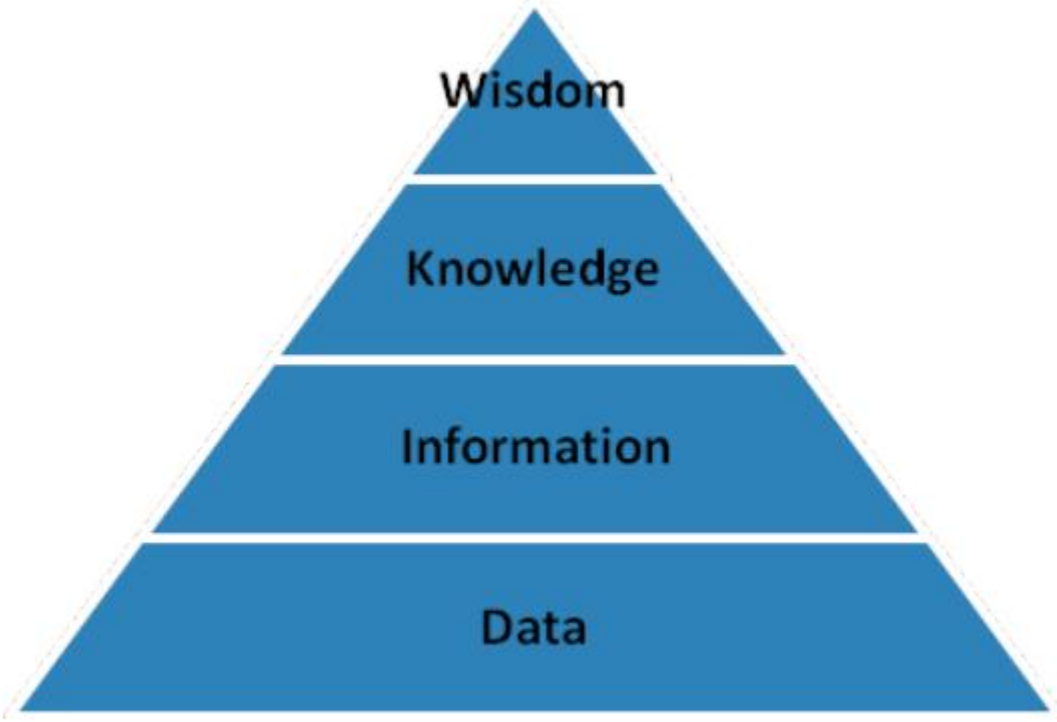


FIGURE 16. DATA, INFORMATION, KNOWLEDGE AND WISDOM FRAMEWORK [4].

In this model the four categories are described as follows:

- Data: Symbols.
- Information: Data that are processed and are perceived to be useful. Providing answers to 'who', 'what', 'where' and 'when' questions.
- Knowledge: Application of the information to gain insight into the 'how' questions.
- Wisdom: Evaluated understanding.

Because Ackoff predates the information technology age we will also use a modern addition of the terms from Laramee et al. [33]:

- Data: Computerized representation of models and attributes of real or simulated entities.
- Information: Data that represents the results of a computational process for assigning meaning to the data, or the transcripts of some meanings assigned by humans.
- Knowledge: Data that represents the results of a computer-simulated cognitive process or the transcripts of some knowledge acquired by humans.
- Wisdom: Evaluated understanding.

This means that when we talk in this paper about information we refer to data that has a meaning assigned to it and is perceived to be useful. The information can be used to answer 'who', 'what', 'where' and 'when' questions and can be applied to gain insight into the 'how' questions.

INFORMATION MANAGEMENT & RISK MANAGEMENT

Information is often seen in as "the lifeblood of an organization", offering advantages to those who excel at controlling it [5], [39], [37]. However Ernst & Young has experienced at their clients that managing information is very hard in practice. This is supported by recent literature about the topic [16], [37]. The term information management, or IM, is also disputed but in general it encompasses the relationship between business and ICT. The practice of IM is generally seen as a management task exceeding IT management [37]. At the highest level IM involves the acquisition of data from sources, the provision of data to stakeholders to fulfill their needs and the dispositioning of data by means of archiving or deletion. As such IM can be seen as a strategic alignment between the business strategy and the operations and between the business and IT [37]. We will elaborate more upon these alignment problems.

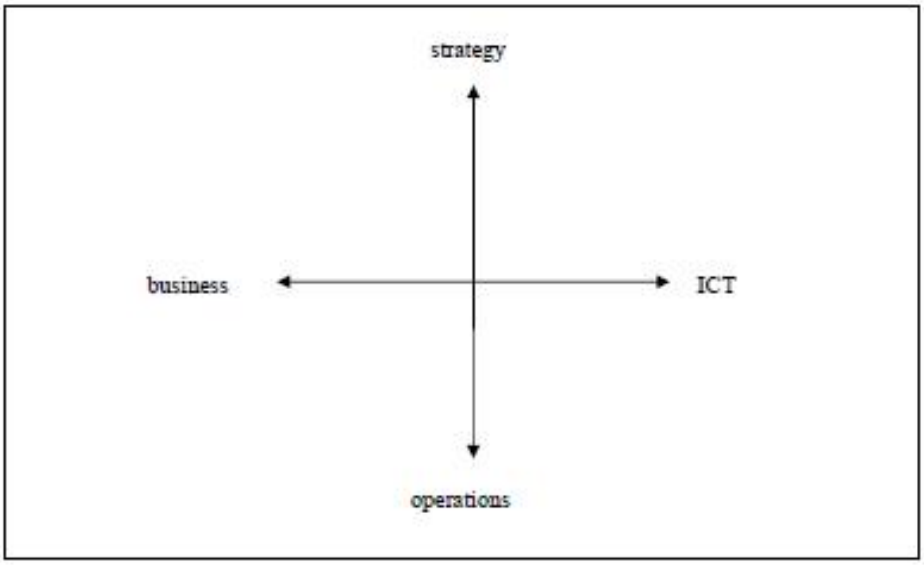


FIGURE 17 INFORMATION MANAGEMENT DOUBLE SPLIT [37].

Strategy – operations alignment:

- Employees will perform their operations and as such will acquire data in different systems. (Operations)
- Management involved with the business strategy will require feedback on their strategy and will as such require information from the different sources. (Strategy)

Business – ICT alignment:

- Success of the business relies upon good management and strategy. In order to adjust business and strategy to the environment bottom-up feedback is needed to justify changes. (Business)
- The business IT must be aligned with the business objectives in order to accommodate to the strategy. In addition to this feedback from the operations will mainly come from IT systems within the business. (ICT)

So how does information management relate to risk management? In section 5.1 and 5.2 we introduced the different kinds or risk categories and risk frameworks such as COBIT and ISO/IEC 27001. One of the more recent risk categories involves information (security) risks. Noticeable from this topic is that information (security) risk management is proposed by academic literature and practice as a people, process and technology problem [24], [18], [23], [46], [6]. The strategic alignment problems of IM is also a people, process and technology problem. Furthermore it is logically derivable that IM is complementary to IRM, meaning that is a company excels in information management it will also have better insight into information related risks and will excel at managing these risks. Let us further

explain some of the key aspects of the three components of these people, process and technology problems that relate to IT audit.

People:
In practice and in scientific literature there is a recognition that in overall information management and in information security processes humans are one of the weak links [6], [22], [23]. However if managed correctly humans can also be a valuable asset in those processes [6]. So what are crucial aspects in managing people in respect to information security and information management? Governance off course plays a vital role since all companies nowadays have a policies regarding information and security (ISP) and information sharing. In addition to this there have been attempts of academics to explain the behavior of employees towards following policies like ISP. Bulgurcu et al. use the theory of planned behavior in their paper to analyze employees' intention to comply with the ISP [6]. They found that attitude, normative beliefs and self-efficacy influenced the overall intention to comply significantly. Furthermore they found that the beliefs of employees about the outcome of their actions influenced their assessment of the consequences significantly, which in turn influenced their attitude. According to their paper information security awareness positively affected both attitude and outcome beliefs [6]. Full results are show in figure 18. Hu et al. performed a similar theory of planned behavior experiment and ended up with similar results [22]. All in all it is the nature of humans add additional complexity to policies and behavioral control. Knowing that creating awareness is vital in coordinating human resources towards a data-driven audit approach we will have to take this into account when developing the artifact.

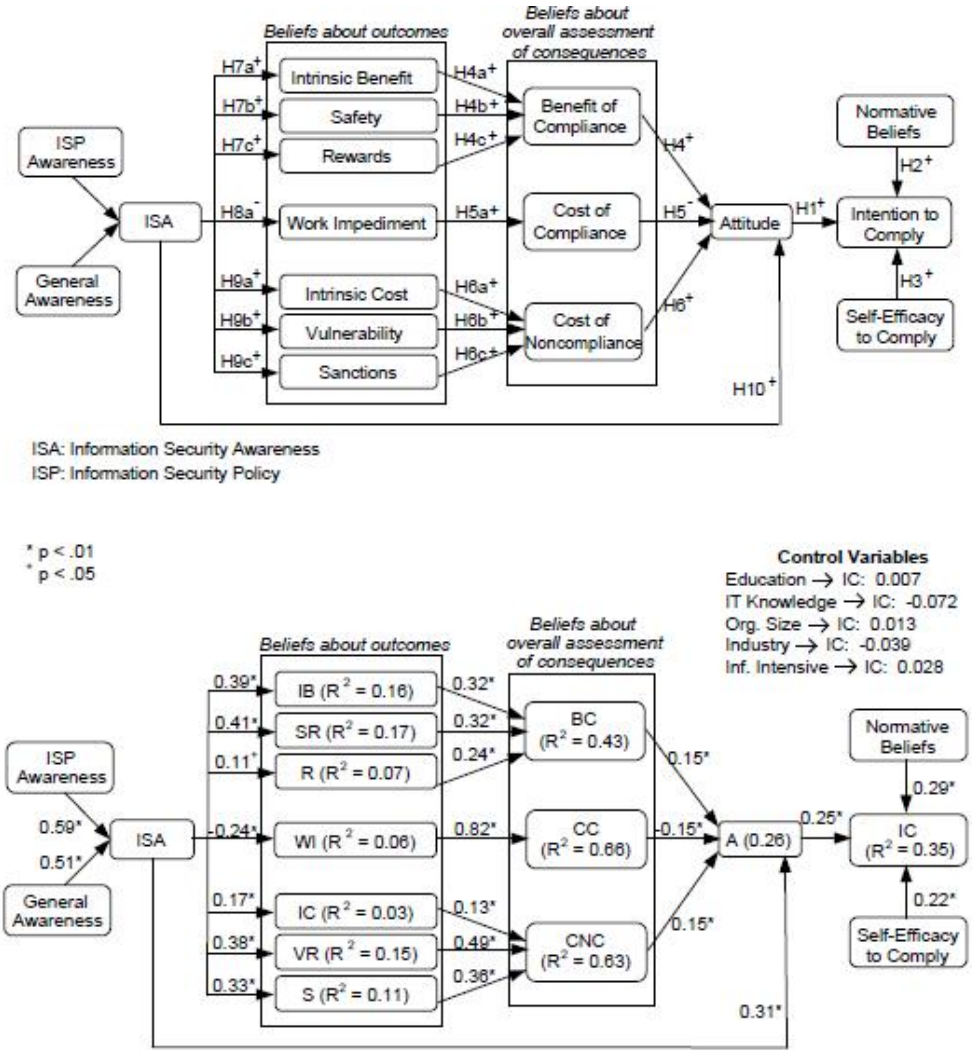


FIGURE 18. INFORMATION POLICY COMPLIANCE FACTORS [6].

Process:
Several process aspects are derivable from the notion that companies are conducting business via specified business processes. These business processes often involve multiple supporting IT systems. The correctness of the conducted business process instances must be verified, which implies that an IT audit trail of the business process instance can be made. As the disability to do this is one of the main aspects of the problem of this paper it is easy to see that IM also involves a process problem. One of the main aspects of the process problem is that segregation of duties must be ensured [23], [45]. At the basis of the segregation of duties problem is the notion of role based access control, or RBAC, which deals with access control in terms of roles assigned to job descriptions [9], [36].

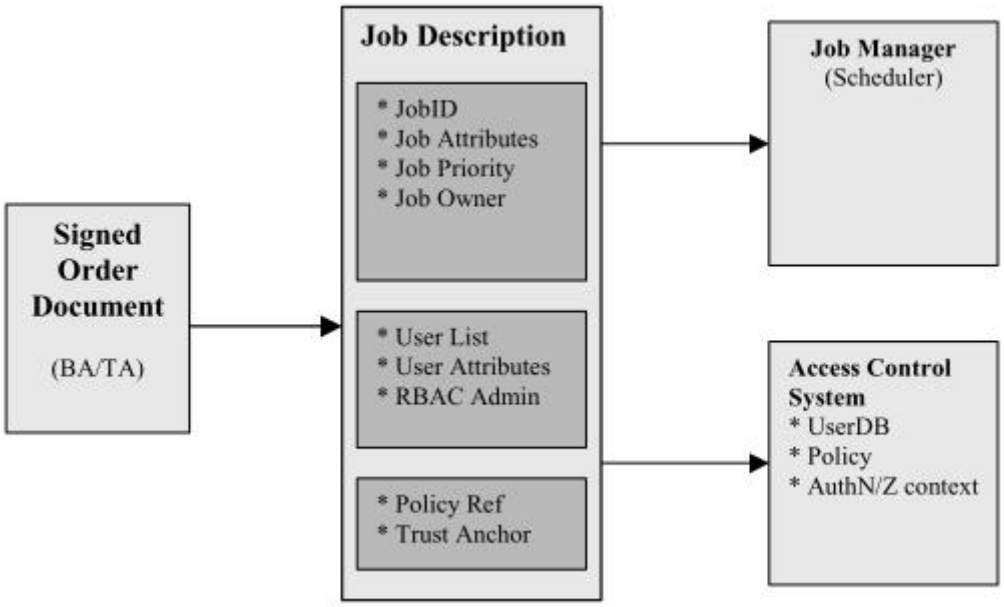


FIGURE 19. ROLE BASED ACCESS CONTROL [9].

Technology:
Lastly the IM problem resides in the technological capabilities of the company. As earlier stated the relational databases of the IT systems used in the different business processes are not easily used for analysis purposes and are therefore not often used for IT audit purposes [8]. For audit purposes event data from the systems are sometimes used. Nowadays there are no standards for IT audit log files which often results in files that contain noise or files that do not contain all information [57]. In section 5.5 and 5.6 we will go deeper into event data and their potential.

5.4. Information Management Frameworks

A lot of academic literature has dedicated attention towards the importance of good information management within businesses processes [58], [30]. However there is very little information about more practical frameworks that help businesses with achieving solid information management. In this paper we will use two high level IM related frameworks to help us in the construction of an organizational framework for the three lines of defense in financial companies that helps them deal with information management problems of the internal audit department.

The first of those frameworks is a very high level knowledge management cycle developed by Evans et al. as shown in figure 20 [15].

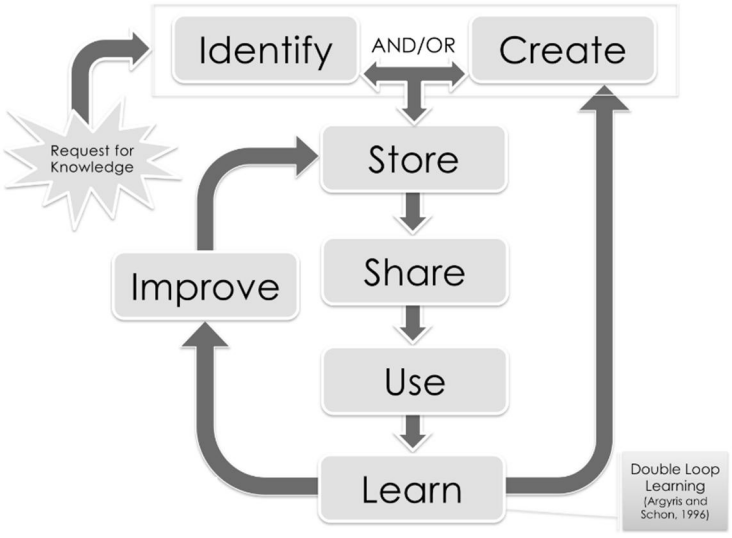


FIGURE 20. KNOWLEDGE MANAGEMENT CYCLE [15].

This framework starts with the notion that some stakeholder needs information to perform a certain tasks. This knowledge request results into the action to identify or create this knowledge in the company. The knowledge is then stored, shared and used for its purpose. Lastly the company will learn from this cycle and will improve the information or create new information that does serve the stakeholder request. Although this cycle is obvious and straightforward it is important to note one things, namely: The knowledge management cycle is invoked by a stakeholder and is therefore reactive and not proactive. Practically this implies that if the stakeholder request has not occurred once before the information request might take a long time to complete.

In addition to this framework this paper will use the information management framework developed by Maes as shown in figure 21 [37]. This framework builds upon the notion of the double split explained in the previous chapter.

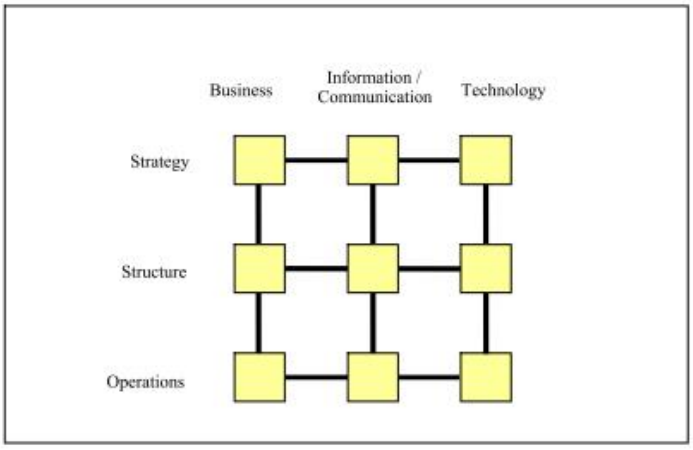


FIGURE 21. INFORMATION MANAGEMENT FRAMEWORK [37].

The IM model displays the three IM related issues on the y-axis, namely: Strategic, structural and operational issues. On the x-axis the information and communication processes and their supporting technology are related to general business aspects. When reading the x-axis from right to left you can see that it starts with the capture of data at the technological level, then the interpretation of this data at the information/communication level and then the usage of the information at the business level. Therefore you can assign the term data to the right column, information to the middle column and knowledge to the left column in accordance to the Ackoff DIKW framework [4], [37]. Additionally every column needs a different expertise, being: Domain expertise in the left column, information expertise in the middle column and technological expertise in the right column. According to Maes the left column (business) "constitutes the pragmatics of a given problem". The right column (technology) can be seen as "introducing a new syntax", which leaves the heart of IM, the middle column (Information), with a sense making problem. According to Maes this framework can be used to design more practical implementations for specific purposes, which we will do in this paper [37]. To broaden our view we will discover the relationship between information management and business process management in the next chapter.

5.5. Business Process Management

According to academic literature business process management involves four activities in a cycle. This cycle can be invoked at any of these activities depending on the context [58], [30]. Figure 22 shows the activities of BPM. Traditional workflow management excludes the diagnosis activity and solely focuses on the development of process

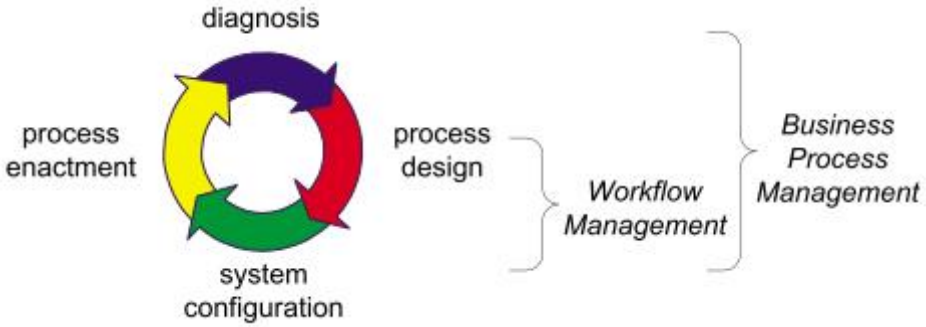


FIGURE 22. BUSINESS PROCESS MANAGEMENT CYCLE [58].

designs and the execution of these designs in their context. The whole focus of workflow management is therefore on the automation of business activities. Business process management does encompass the diagnosis step, which is basically a task that triggers the business to review their business activity automation. In modern society this step is becoming increasingly important as continuous process improvement with new techniques and technologies can save companies a lot of money. Furthermore new regulations have increased the need for businesses to understand their automation processes and protect the data generated in them.

The diagnosis step is where BPM meets information management and general data-driven audit tasks. Generally because monitoring a business' business process performance requires a company to manage the information about and from that specific business process. This is exactly what an audit trail should encompass and therefore from a BPM perspective the problem of our paper resides in the diagnosis step.

Recent literature from the BPM research community [59], [30], [60], have also acknowledged the problems in the diagnosis step and this different research topic is called business activity monitoring, or simply BAM. BAM academics note that in order to practically monitor business processes it is vital that log files are created during the process [30]. It is important to note that BAM is an iterative process that should occur at least once after deployment of the process and after every significant change in the process [30]. For audit purposes however we must also take into considering that next to process changes there are also people involved in the process who can be unpredictable. In a similar fashion the business environment is volatile. For our framework we have to take this into account. Another important thing to consider during diagnosis is what are you exactly trying to measure? The field of BPM is very much accustomed to using key performance indicators, or KPI's for establishing measurement objectives [30]. This means that at the start of the diagnosis step some KPI's are chosen, based on experience or previous acquired knowledge. The diagnosis step is then tailored in such a way that the KPI's are measured and the KPI objectives are met. Figure 23 shows that the monitoring model is influenced by business requirements and event definitions and the actual measuring is done using KPI's. When relating BPM, specifically BAM, with the information management frameworks discussed in section 5.4, we can see that business process management mainly covers the right and middle column of the information management framework of Maes [37], considering that the nature of the business process influences the production of data during the process and the interpretation of data in several stages of the business process as well as the interpretation of people who observe the process for auditing or improvement purposes. Results from BAM processes also cover the left column in which the information is used for business purposes. Of course the aim of BAM is to solve strategic, structural and operation problems, which represent the rows of the Maes framework.

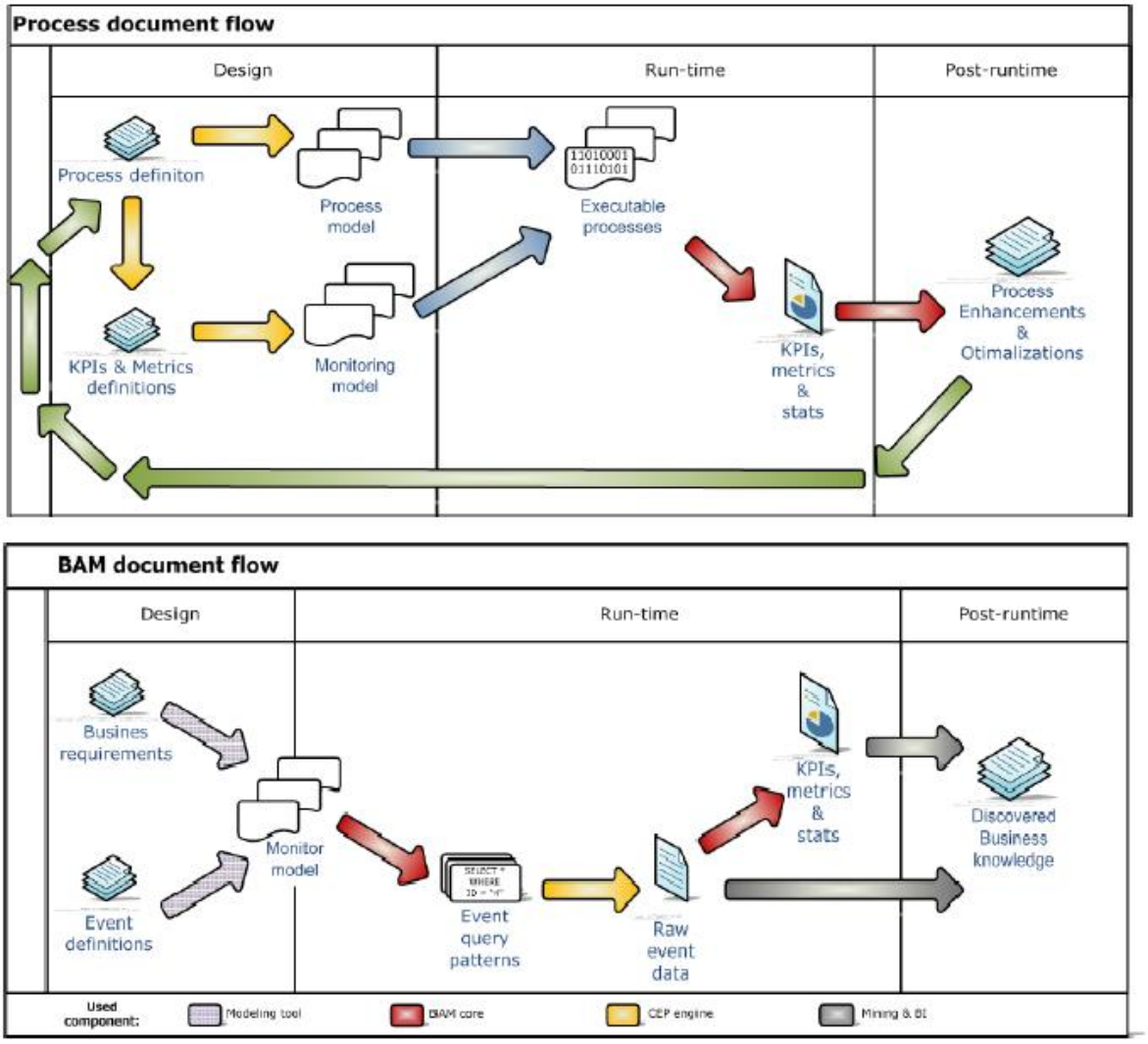


FIGURE 23. KPI'S IN THE DIAGNOSIS PHASE [30].

5.6. Event Data

PROCESS MINING

One of the big pillars behind the BAM principle discussed in section 5.5 is the usage of log files, also called event data, in process mining [3], [59]. Traditional IT audit focuses on system specifications and configurations and determines to what extend malicious activities are possible with these systems. This approach is very much a control based approach in the sense that the basis of the current audit function finds it origin in well adopted frameworks such as COBIT and COSO. These models treat business compliance as a function of controls covering multiple disciplines and departments. Our paper adds another dimension to audit by looking at audit from a data, or information perspective. The advantage of this is that business process data is treated as flowing between systems within the company in contrast to looking at every system independently. This perspective provides operational audits with IT, or data, aspects, which will generate some overlap between the two. The notion of separating information from information systems is the focus of multiple academic papers from multiple academic domains [52], [33], [15], [23], [59]. Using event data for business process evaluation and audit is called process mining. It is important to note that event data is often not the data generated in and transferred between the information systems of a company, but data about the data generated in the systems, which is documented and stored separately. Because of this we can speak about event data as metadata of the business process data. Figure 24 presents a visual representation of the metadata collection.

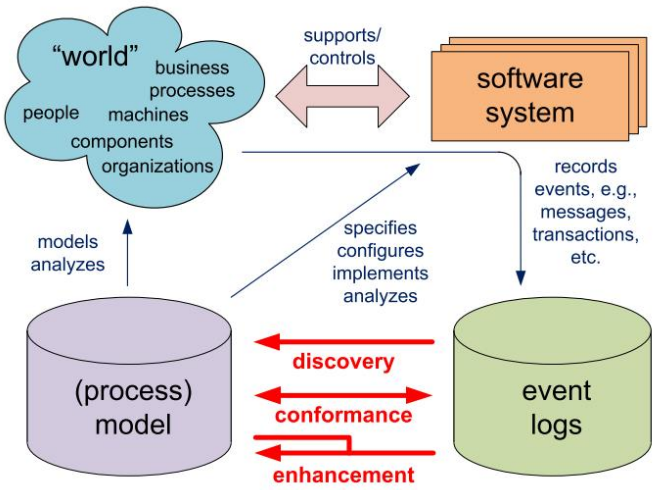


FIGURE 24. METADATA COLLECTION OF A BUSINESS PROCESS [59].

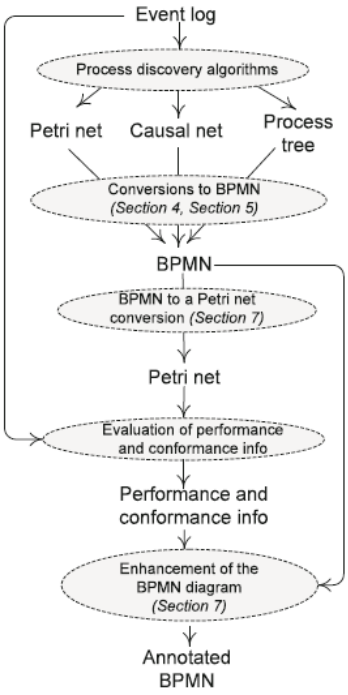


FIGURE 25. PROCESS MINING [29].

The paper of Van der Aalst et al. identifies three different process mining types being [59]:

- Discovery: Discover a process structure out of event data of the process.
- Conformance: Checking process performance with event data of the process.
- Enhancement: Using process event data of the current process with the aim of improving the process.

These three types are not mutually exclusive and build upon each other as shown in the paper of Kalenkova et al. [29]. Figure 25 shows how the different types extend each other. Van der Aalst et al. have constructed a lifecycle for business process mining that describes on a high level how a business process mining project should look like [59]. It starts off with a plan, in which domain knowledge and data availability knowledge have to be acquired. From this plan a set of questions and objectives are derived, as well as a high level understanding of what data has to be extracted in order fulfill the objectives. The next step is to construct a control flow model and connecting event data to this model.

The control flow model can be constructed using expert knowledge or present diagrams as well as using process discovery processes mining techniques. In step three several analysis are made with combinations of event data to estimate process performance, in order to answer additional questions. The last stage consists of operational support. In this step a combination of historical and real-time data is used to analyze and predict performance of the process in the future. The last step is only achievable if the process is stable and structured. Noticeable is that during the different steps of the model several questions will be answered and this insight can be used to redesign the model, to adjust the model, to intervene in the business or to support the business. Figure 26 provides a visual representation of the

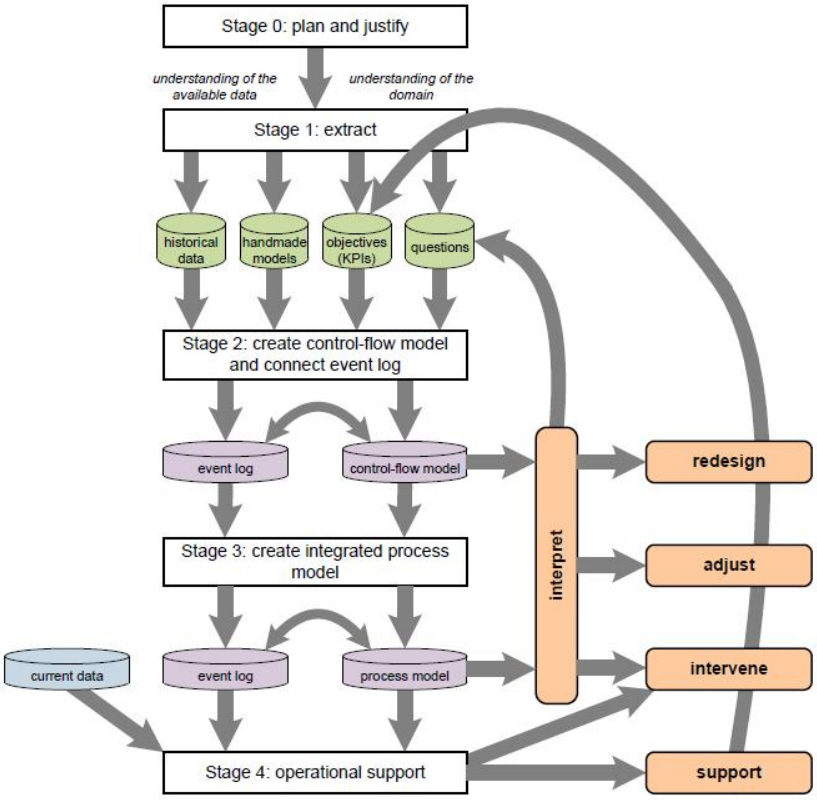


FIGURE 26. PROCESS MINING L* LIFE CYCLE MODEL [59].

model made by Van der Aalst et al [59].
When relating process mining to the information management framework of section 5.4 we can see that process mining as the practical implementation of BAM covers the same columns and rows as BAM, explained in section 5.5.

EVENT DATA REQUIREMENTS

This paper proposes a data-driven three lines of defense framework to help internal audit departments into a more structural and data-driven way of working. In order for this organizational framework to be generally applicable we need to define some event data requirements. In this section we will look into academic literature about this topic to find out if requirements for these purposes already exist.

Van Dongen et al. have dedicated a paper towards developing a metamodel for process mining data, which led to the development of MXML [60]. Even though MXML is now more or less replaced by the new standard XES this paper still provides us with some useful insights concerning process logs. According to their paper using process mining assumes three things regarding the structure of the logs, namely: [60]:

- Every event refers to one activity in the business process.
- Every event refers to a specific case.
- Events are totally ordered.

The IEEE has recently officially adopted XES to replace the MXML standard [60]. The new metamodel used is called extensible event stream, or XES, and is generally more flexible than the MXML meta model [21]. The basis behind this new metamodel is that every XES document has at its top level one log object containing all information related to one specific process. Every log contains an arbitrary number of trace objects, which indicate the process instances. Furthermore every trace contains an arbitrary number of event objects representing the activities of a business process. The log, trace and event objects are by itself empty and lack therefore any information. The information about the objects is stored in attributes, which all have a unique key string assigned to it [21]. For the purpose of maximizing flexibility the XES Meta model allows attributes to have child attributes or nested attributes. Figure 27 provides a detailed picture of the how the XES Meta model is designed.

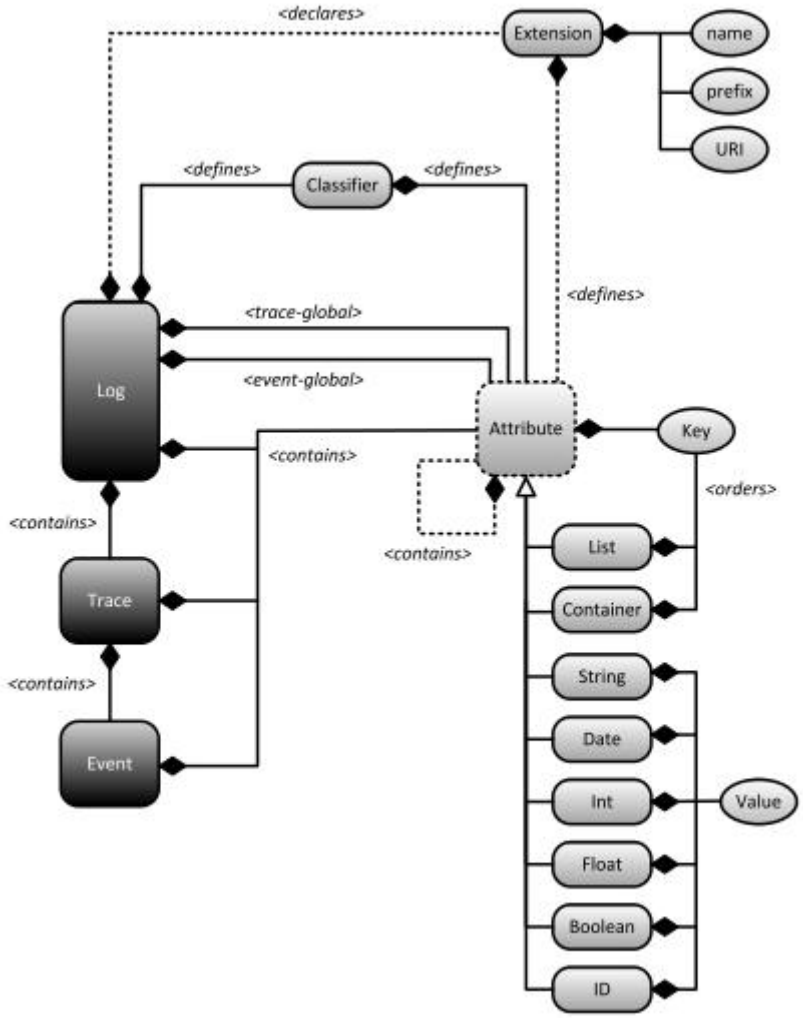


FIGURE 27. XES METAMODEL STANDARD STRUCTURE IN UML 2.0. [21].

The XES metamodel does not dictate which and how many attributes an object can have, but instead defines extensions. Extensions define which set of attributes are at least present on any of the three object levels and even on the nested attribute level. The XES standard furthermore incorporates several standard extensions which are deemed at least necessary. Our paper will use this baseline as requirements for the event data needed in this paper's artifact. The requirements are as follows:

- Concept extension: Attribute that stores the name of the element.
- Lifecycle extension: Attribute specifying the lifecycle transition the element is in (standard is the value used as standard).

- Organizational extension: Three attributes specifying for an event which actor has invoked, which role the actor has and what group it belongs to.
- Time extension: Attribute defining the exact date and time the event occurred.
- Semantic Extension: Attributes specifying references to model concepts in an ontology. The ontology concepts are specified with URI's.
- ID extension: Unique element ID.
- Cost extension: Attribute specifying the costs associated with an activity within the log.

One of the drawbacks of using a metamodel is that in order for the XES or MXML standards to work, you will often need a tool that is able to convert log files into the required format, which is indicated by Van Dongen et al. themselves in their paper [60]. Some additional issues that are indicated in their paper are related to the systems generating the log files. From their findings they were able to conclude that some very data-driven systems need to be specifically designed in a certain way in order to allow logging in such a way that it is possible to relate a single case to an audit trail entry. Furthermore they indicated that in some environments the audit trail entries had to be constructed out of multiple legacy system log files, which complicated the process [60].

6. Literature Review Discussion

This section will summarize the findings of the literature study and will also underline the connections between the different disciplines used in this paper, in relation to our research and artifact. The literature will function as a guideline for the construction of the three lines of defense organizational framework, which will be constructed in the next chapter. The problem statement provided to us by our Ernst & Young supervisors on behalf of their clients encompasses three domains: People, process and technology. Because the field of internal and external audit is practically very much interwoven with risk literature nowadays, we first looked into academic literature about governance risk and compliance (GRC) in order to answer research question one:

RQ1: *"What are the different corporate risk categories and how do they relate and differ?"*

We discovered six risk categories in literature: Technology risk, operational risk, strategic risk, compliance risk, financial risk and information risk [24]. Between these categories there is a lot of overlap. Our paper focuses on operational and IT audit, even though financial audit incorporates a lot of operational audit too nowadays. For this reason the combination of technology, operational and information risks categories are interesting. Noticeable is, that these risks overlap with each other [24]. According to academic literature the category of information risks has not really been practically adopted in contrast to the other two categories, which indicates to the origin of our thesis problem [24], [12]. In order to answer research question two we investigated which risk frameworks are available and are used in practice:

RQ2: *"What are well established risk frameworks?"*

Practically companies use several control based frameworks to assess risks to their company. Examples of well adopted risk frameworks are COSO, ISO/IEC 27001 and mainly COBIT [7], [25], [23]. Since COBIT 5.0 information risks have been incorporated better, but this revision of COBIT has happened in the last five years. Because we want to put an emphasis on providing audit trails of complete business processes and the data flowing in these processes from system to system, this paper looks at operational audit from a data/information perspective in addition to a control perspective. It is important to say that this does not mean that this paper discards control based audit methods, but rather adds another dimension to what is already there. Because we look at audit from an information perspective we have researched several academic papers in the field of information and data management to provide us with high level frameworks on which we can map our developments [37], [15], the same way as that risk frameworks can be mapped on high level risk literature. This in order to answer research question three:

RQ3: *"How is information management related to risk?"*

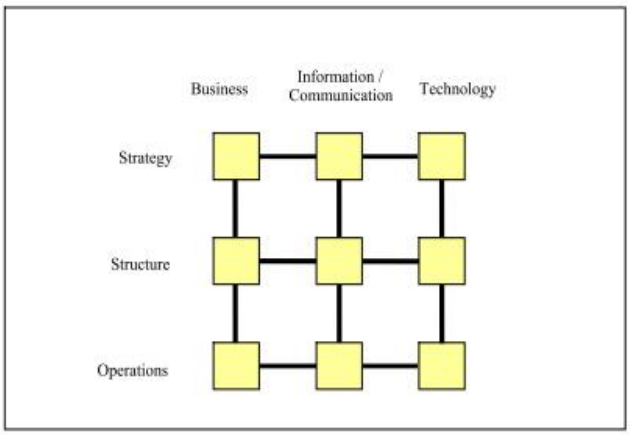


FIGURE 28. IM FRAMEWORK [37].

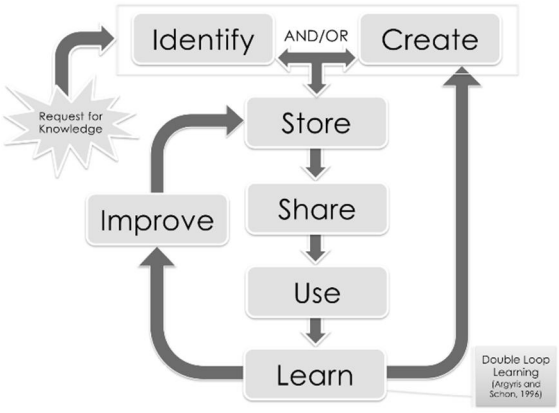


FIGURE 29. KMC [15].

Literature provided us with the knowledge management cycle, which is a high level framework for a data life cycle, explaining the transitions from data into information and information into knowledge, as shown in figure 29. We also discovered an information management (IM) framework, as shown in figure 28. This framework is encompasses the people, process and technology domains earlier described and combines that with the process of converting data to

information and putting information to use in order to solve several issues relating to strategy, structure and operations. These two frameworks also provide us with an answer to research question 5:

> RQ5: *"What information management theories are available that encompass business information derived from business processes?"*

The high level Information management framework [37] was used to map the other literature analyzed in this paper on it. One of the academic domains used in this paper is the domain of business process management (BPM), for the simple reason that it does also look at processes from a process perspective and a dataflow perspective [58], [30]. For the purpose of this paper and because of the role of internal auditors in a company we are mostly interested in the monitoring aspect of BPM. This subdomain of BPM is called business activity monitoring (BAM) and involves using event data to discover, audit and enhance business processes in order to improve business performance [30]. BAM can therefore easily be mapped on the IM framework, where the usage of event data fits into the technology column, the extraction of process information from this data fits into the information column and the application of the information to improve processes fits into the business column. The ability to map BAM on IM provides us with an answer to research question 4:

> RQ4: *"What is the relation between business processes and information management?"*

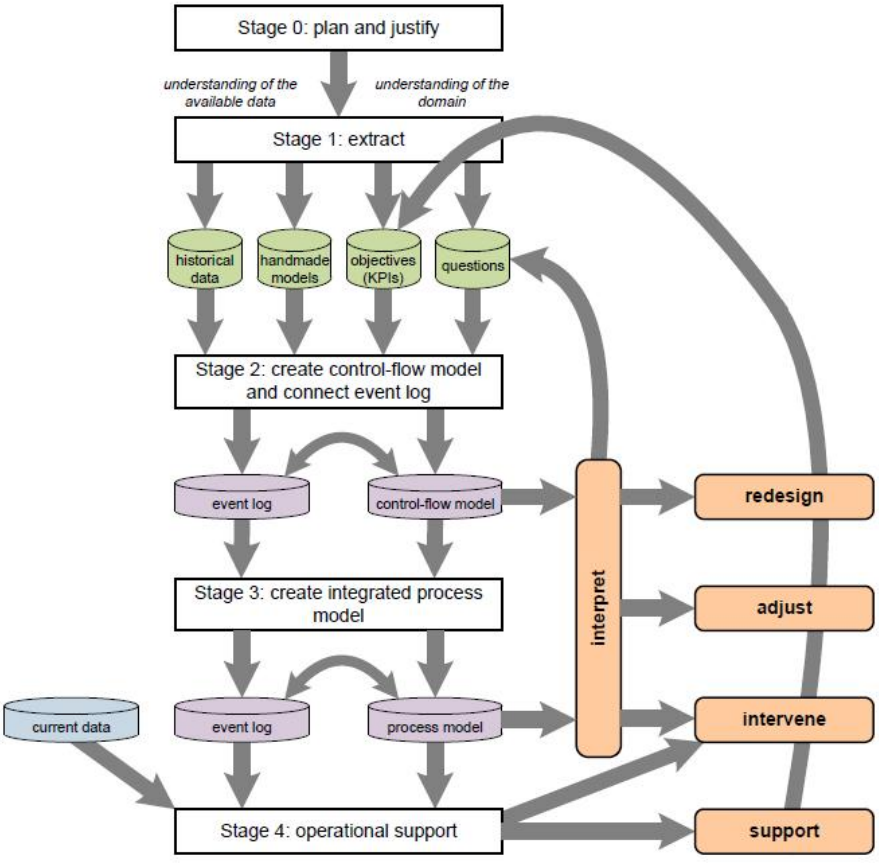


FIGURE 30. PROCESS MINING L* LIFE CYCLE MODEL [59].

In order for this paper to provide practical knowledge to practitioners in the field our framework will also need to encompass practical implementations of BAM. Therefore we have also looked into process mining, which has given insight in the establishment of objectives and KPI's prior to executing process mining. Furthermore literature has shown that in order for companies to enhance their business performance the combination of real-time data and historical data is needed. Van der Aalst et al. have combined this knowledge into a process mining life cycle model

shown in figure 30 [59]. The practice of process mining as explained by Van der Aalst et al. [59] and as shown in figure 30 provides us with an answer to research question nine:

RQ9: "What practical applications are already available that use log files for control purposes?"

Using event data in process mining makes the practitioner very dependable on the business environment and the company's systems. In an effort to make generalization possible academics have set up a mining data metamodel that can be used to convert different event data sources and formats into a single format XES file, called the XES standard. The requirements for event data are as follows according to literature [21]:

- Concept extension: Attribute that stores the name of the element.
- Lifecycle extension: Attribute specifying the lifecycle transition the element is in (standard is the value used as standard).
- Organizational extension: Three attributes specifying for an event which actor has invoked, which role the actor has and what group it belongs to.
- Time extension: Attribute defining the exact date and time the event occurred.
- Semantic Extension: Attributes specifying references to model concepts in an ontology. The ontology concepts are specified with URI's.
- ID extension: Unique element ID.
- Cost extension: Attribute specifying the costs associated with an activity within the log.

This list of requirements and the XES mining metamodel provides this research with an answer to research question six and seven:

RQ6: *"What are the requirements for log files in order for them to be useful in internal audit?"*

RQ7: "Are any log file frameworks available that support the necessary requirements, so that practical usage is possible?"

From the paper of Van Dongen et al. and prior papers of Van der Aalst [58], [57], [59], [60], we can derive that using log files in internal audit processes will result in providing a clearer picture of how business processes perform in real life, which cannot really be accomplished from the traditional control based audit approaches. This notion provides us with an answer to research question eight:

RQ8: *"How can log files contribute to internal audit processes?"*

We have discussed the process and technological aspects of the problem, but the people aspect is also important. According to literature a company's governance structure dictates its hierarchy. In addition to hierarchy a company also has an active set of rules, called policies, which dictate communication patterns based on the hierarchy. Policies are often imposed in a top-down manner and this means that managers might encounter resistance from employees [6], [61]. When regarding information security policies the adoption of these policies correlates with the amount of training provided to the employees in regard of information security. This human aspect must also be represented in the framework that we will create in the next part of this thesis.

DESIGN

7. Formulating Methodology Goals.

As argued multiple times in this paper, the main contribution of this research will come from the organizational framework created and evaluated in this research. This framework will have to encompass the connections between the literary topics identified in the literature study, as well as the observations of experts in the internal audit field. In this light we were able to determine multiple goals that the framework must accomplish based on the iterations of the research methodology of chapter 3.6. Each goal will cover additional links between literary topics and expert observations:

> G1: Determine the "as-is" situation of the three lines of defense model by combining expert observations and internal audit literature.

This paper argues that combining expert observations with literature about the current internal audit function will enable us to construct a model of the current situation of the internal audit function. This "as-is" situation can be used in establishing a "to-be" situation.

> G2: Determine the "to-be" situation of the three lines of defense model by combining knowledge about the "as-is" situation of the first and second line of defense with the requirements analysis of the third line of defense base on information management principles.

This paper argues that combining knowledge about the "as-is" situation of the first and second line of defense with the requirement analysis of the third line of defense, based on the literature study, will result in a possible "to-be" situation of the three lines of defense model that improves information management performance.

> G3: Assessing the impact of the "to-be" three lines of defense organizational framework on information management within the three lines of defense to support internal audit, by performing a GAP analysis between the "as-is" situation and the "to-be" situation.

We argue that if we evaluate and compare the information management performance of the "as-is" situation to the "to-be" situation, proposed in the framework that this paper will construct, that we can identify the added value of the framework constructed in this paper.

> G4: Providing a migration plan for the process, people and technology aspects of the artifact that addresses how to "to-be" situation can be reached.

We argue that providing a migration plan for the artifact will add to the applicability of the framework as well as improve its acceptation by practitioners. A methodology based on these four goals will provided us with the information to answer our paper's main question:

> What is the appropriate framework for financial companies to govern information management within the three lines of defense to ensure complete audit trails in the third line of defense?

The design of this methodology and the subsequent goal validation based on validation and evaluation interviews will prove if this is indeed the case.

8. Methodology

The methodology used in this paper, based on the Sein et al. methodology [51], will be further elaborated upon in this chapter. This methodology will serve as a guideline for assessing the impact of our information management organizational framework on the overall internal audit in a financial company. This is done through multiple sequential steps.

Each step consists of multiple tasks which require multiple skills, tools and techniques. These skills, tools and techniques are based on scientific literature and practice literature used by Ernst & Young. Experts within Ernst & Young and their clients were asked for best practice literature and insights to help solve multiple issues within the activities.

As stated in part one – introduction, this paper proposes a new systematical data-driven way of working for internal audit departments. This new way of working is built upon the existing three lines of defense model of the IIA [27]. This means that in order to evaluate our proposed framework it is vital that we provide a gap analysis that indicates the added value of our framework and the usability in comparison to the current way of working.

As stated before during the literature study we will approach developing the framework from three angles, being:

- People: Governance, training, theory of planned behavior
- Process: BPM, BAM, process mining, risk management
- Technology: Event data requirements, process mining, BAM

This means that the processes in this methodology must encompass aspects of all three domains. A similar approach is followed by Ernst & Young consultants [13]. The methodology steps that this paper follows, based on the design goals, are as follows:

1. Model the “as-is” situation: Creating a process model overview of the current situation of the three lines of defense.
2. Determine requirements for the “to-be” situation: Use literature and stakeholder knowledge to determine people, process and technology requirements for the “to-be” situation.
3. Model the “to-be” situation: Creating a process model overview of the “to-be” situation improving upon information management.
4. Perform a GAP analysis between “as-is” situation and the “to-be” situation to determine effectiveness of the framework in improving information management: Show off the added value of working with the framework.
5. Provide a migration plan to practitioners in order for them to implement the “to-be” situation in their companies.

In order to model the process models Business Process Modeling Notation 2.0, also called BPMN 2.0, is used [43]. The semantics of BPMN 2.0 can be found in appendix D. The reason for choosing this language is because BPMN is a widely used language that is both very flexible as well as extensive. It provides the possibility to model the different activities in a process model as well as model the information inputs for every activity. In order to model the stakeholder driver analysis, the requirement analysis and the migration plan the Archimate 3.0 language [54] will be used, as this language is widely used for these purposes and this language also provides flexibility, as well as an extensive set of semantics. The semantics of Archimate 3.0 can also be found in appendix D.

Figure 31 is based on the iterations described in the action design science methodology used in this paper and described in figure 5 of chapter 3.6 and displays the research model used in this chapter graphically.

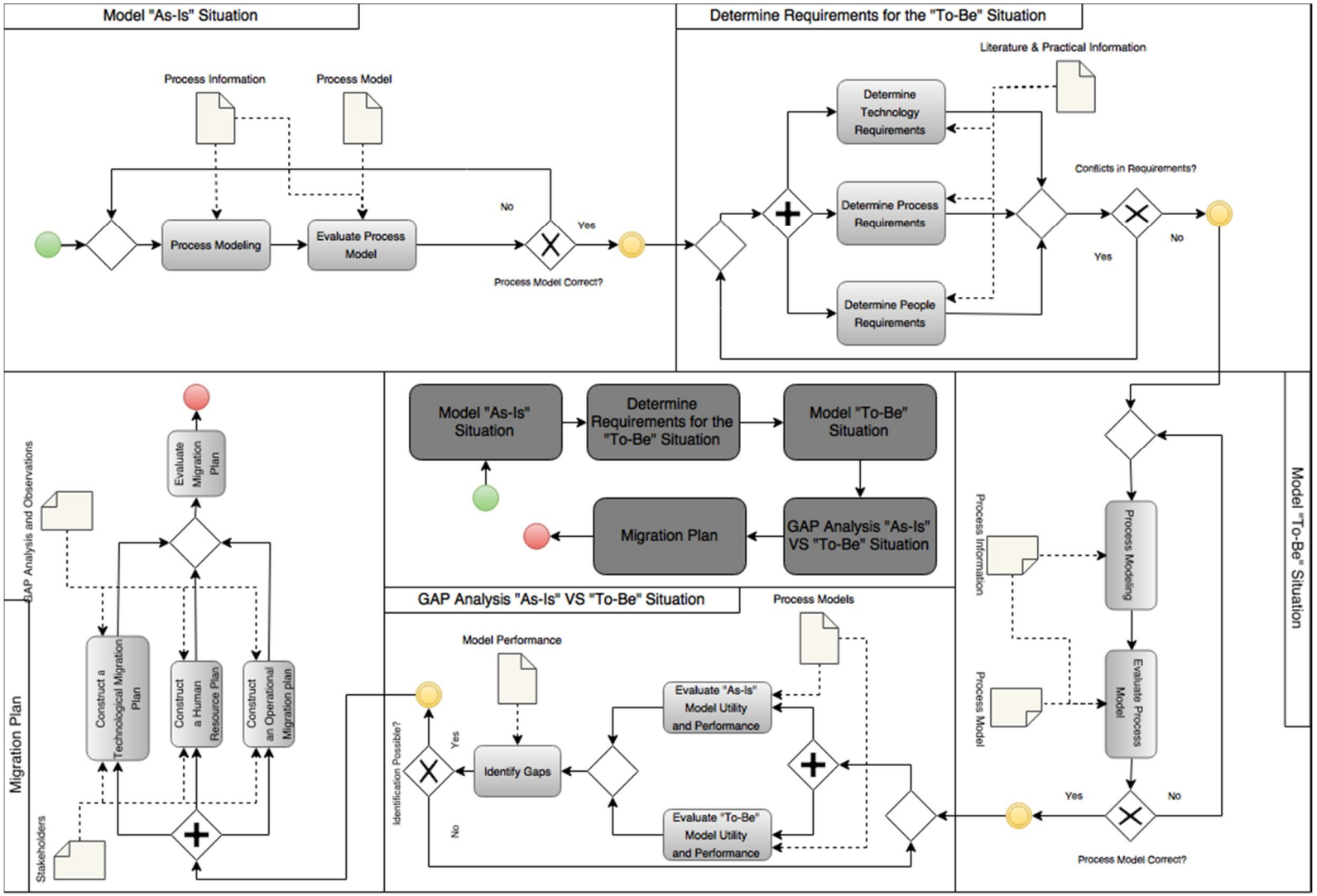


FIGURE 31. RESEARCH METHODOLOGY.

8.1. Model the 'As-Is" Situation

As described in the chapter 3.6 and in the research methodology of figure 31 we will start our first iteration by developing the current, or "as-is" situation, way of working within the three lines of defense for an organization that does not work data-driven at all. This "as-is" situation will be used as baseline throughout the development of the "to-be" model and the migration plan. The "as-is" model will provide us with valuable insights into the practical capabilities and the lack of some capabilities of the current way of working of internal audit. Expert observations and literature will also provide us with information about the considerations that have already been identified when establishing this "as-is" situation. When establishing the "to-be" situation in a later stage of this chapter we will also have the opportunity to compare the "to-be" model with the "as-is" situation in terms of expected information management performance and usability.

The research methodology of figure 31 proposes two actions that have to be performed in order to model and validate the "as-is" situation. The first of these actions focuses on the actual modeling of the "as-is" model and uses process information as an input as can be seen in figure 32. The second action focuses on validating the "as-is" situation model by means of expert interviews and will use the process model and process information of the first action as input. The "as-is" process model will be developed in the language of BPMN 2.0 [43].

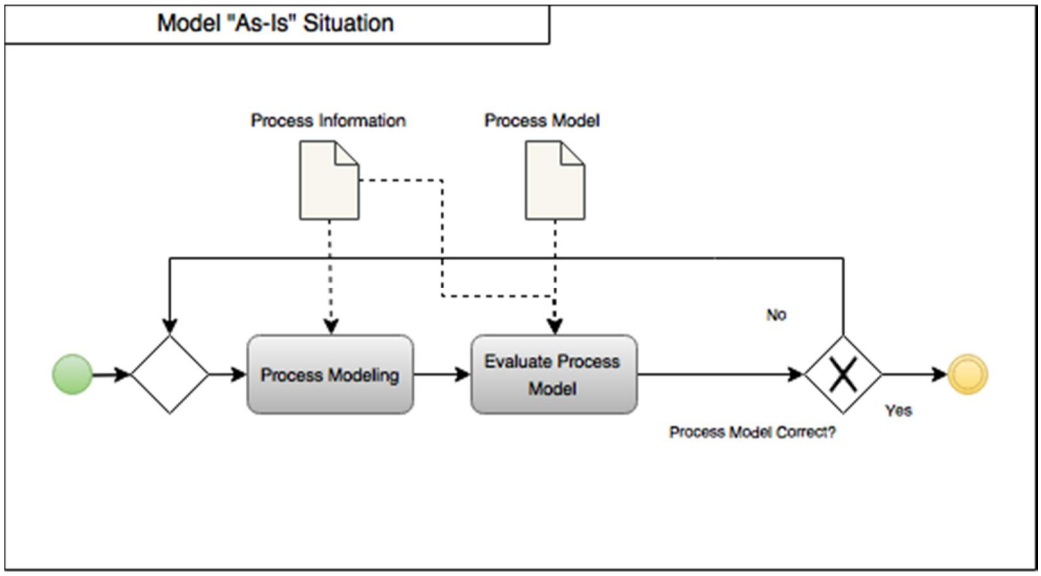


FIGURE 32. MODELING THE AS-IS SITUATION

PROCESS MODELING

In order to start modeling the "as-is" situation we first have to gather sufficient information about the current situation. From theory [27] we learned about the theoretical model that encompasses the three lines of defense, but in order to make sure the model will represent the actual situation in companies we will have to consult experts in the field about the day-to-day practices that they observe or perform. This is important because high level frameworks like the three lines of defense are often not followed completely in practice or altered slightly to conform to the business. We will first summarize the information from the literature study relevant to the model. The IIA paper [27] explains that every line has their own role in a company. We will describe these roles in this chapter to clarify our design choices in the "as-is" model.

According to the IIA's *"The Three Lines of Defense in Effective Risk Management and Control"* paper [27] the first line of defense, or the operational department, has three mayor responsibilities. The first of these is that the operational department owns the risks of a company. This means that risks identified by the second line of defense will have to be counter measured in order to accommodate the organizations risk appetite. In order to identify if these countermeasures have reduced a risk sufficiently some control will have to be implemented and tracked by the first

line of defense. Intended is, that the first line of defense provides independent assurance reporting to the senior management.

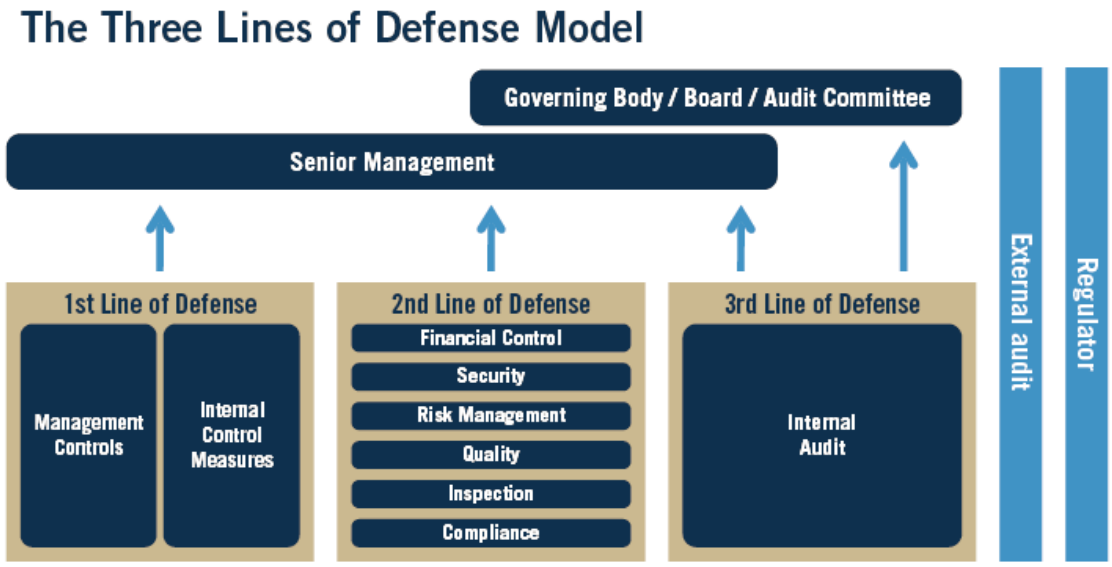


FIGURE 33. THREE LINES OF DEFENSE MODEL [27].

The second line of defense, or risk department, is mainly involved in identifying risks to the organization, based on certain risk frameworks like COBIT [25] and COSO [7], that we described in the literature study. In addition to this the risk department also has to determine the company's risk appetite, based on the organizational strategy. Risks to the company also have to be monitored to provide independent assurance from the first line of defense. This is done by developing controls and monitoring these controls. Risk management reporting to the senior management fulfills two critical roles. It provides input for management policies and alerts operation management to emerging issues. The second line of defense is also responsible for providing risk trainings and guidance when needed [27].

In the *"The Three Lines of Defense in Effective Risk Management and Control"* paper of the IIA [27] the role of third line of defense, or internal audit department, is explained less clearly. Since this model is also widely used by companies we expect that this is also one of the reasons that companies struggle to organize the internal audit department successfully in a data-driven way. The main function of the third line of defense is, that the internal audit is independent from the company and is therefore able to report directly to the top management as well as the senior management. In order to gain more insight into the activities of the third line we will conduct an exploratory interview with an Ernst & Young expert of the internal audit function. The interview structure and a summarization of the results can be found in appendix E. The interview resulted in the following key points:

- Every year a list of objectives is set up by the governing bodies of the company.
- The list of objectives is based on what the governing bodies deem important that year and will differ from year to year.
- The list of objectives is used by the internal audit department to audit relevant processes.

With the key points of the literature and the expert interview the conceptual alpha version model in figure 34 of the "as-is" situation could be made.

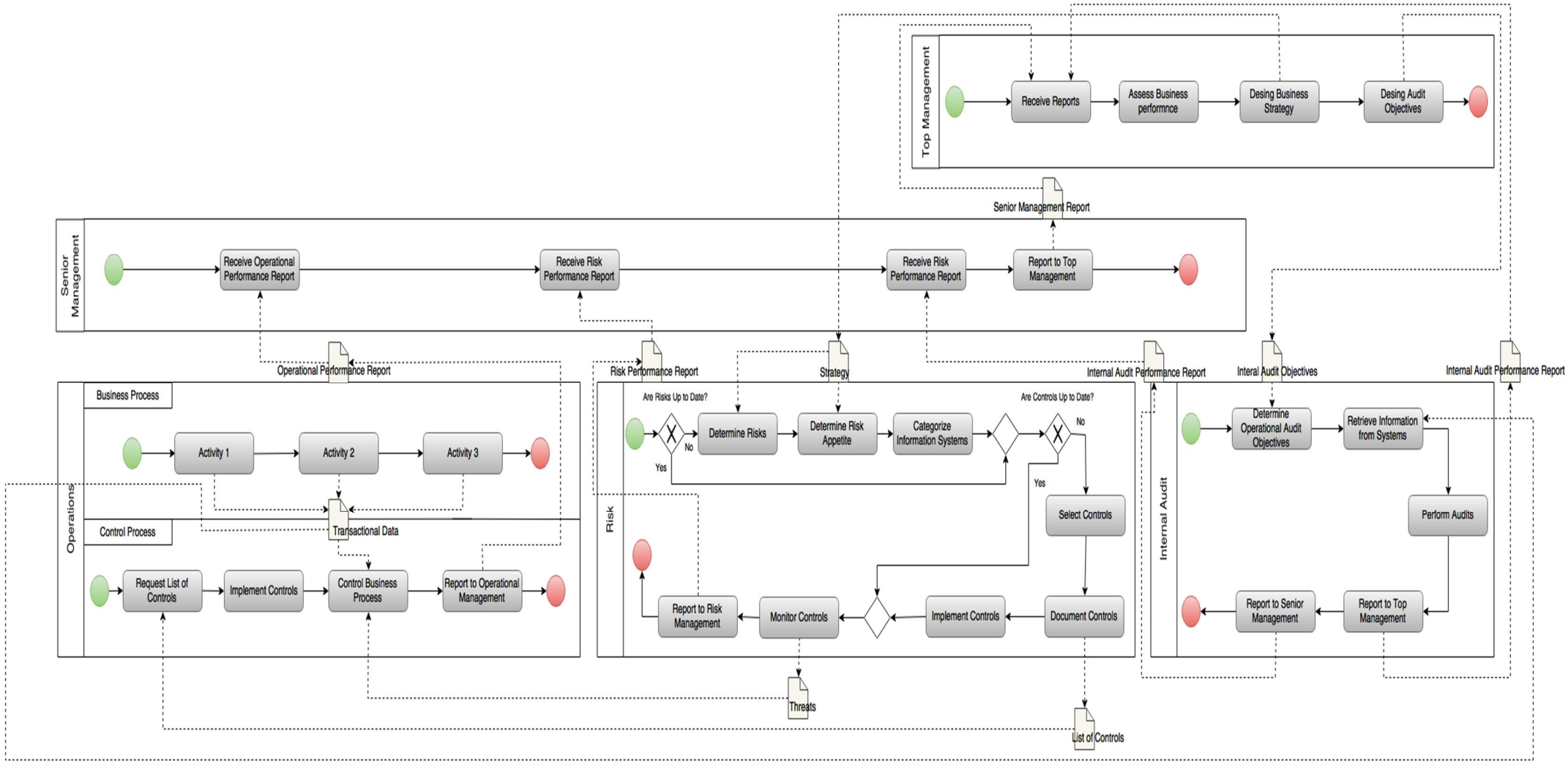


FIGURE 34. AS-IS SITUATION THREE LINES OF DEFENSE (ALPHA VERSION).

Model explaination:
The first line of defense consists of the operations department, who check every business process instance on correctness via a control process. In this control process the operations department is dependent on information from the risk department, such as an up to date list of controls and a list of current threats. The control process uses transactional data stored by the different systems used in a business process to evaluate if a business process has been completed correctly. The first line of defense reports to the senior managament.

The second line of defense consists of the risk department of a company and is responsible for selecting business relevant controls for business relevant risks. Relevant risks and risk appetite are based upon the strategy of the firm. Based on the identified risks several controls can be selected and implemented. The residual tasks of the risk department are to monitor the risks and report to the senior management.

The third line of defense consists of the internal audit department. The funtion of this deparment is to provide individual assurance of the business. The internal audit department receives multiple audit objectives from the top management and determines their own operational audit targets, based on these objectives. In order to do the operational audits several datasets from relevant information systems will be requested and used. These datasets are however not constrcuted for the purpose of audit and will therefore not always provide the information needed to succesfully audit a business process. Findings are both reported to the senior management and the top managament directly.

EVANLUATE PROCESS MODEL

In order to validate if the “as-is” model represents the reality of internal audit in companies that are not yet operating in a data-driven way we will perform two expert interviews with an Ernst and Young expert of the internal audit field and with an expert of a client of Ernst Young. The structure and the result of these interviews can be found in appendix F.

Both of the experts interviewed indicated that the function of the first line of defense was not modelled completely correct. They indicated that the first line of defense does not only use controls developed by the risk department to monitor risks to the company, but mostly use their own set of risk controls. In addition to this both experts indicated that the third line of defense was also not modeled completely correct. In the conceptual model the internal audit department receives the annual internal audit obejctives from the top management of the organzation. In reality this is not the case. The internal audit depatrment develops their own internal audit objectives based on reports from the first and second line of defense. These internal audit objesctives are only approved or disapproved by the top management, based on what they perceive as important. Furthermore both interviewees indicated that an additional action needs to be added to the internal audit function which covers the design of internal audit controls used during audits. For clarification reasons the interviewees pointed out that the “perform audit” action should be split into three actions covering the three different types of audits performed by an internal audit department.

In figure 35 these errors have been corrected. Figure 35 therefore serves as the validated baseline for the construction of the “to-be” situation and the migration model and as this paper’s beta version.

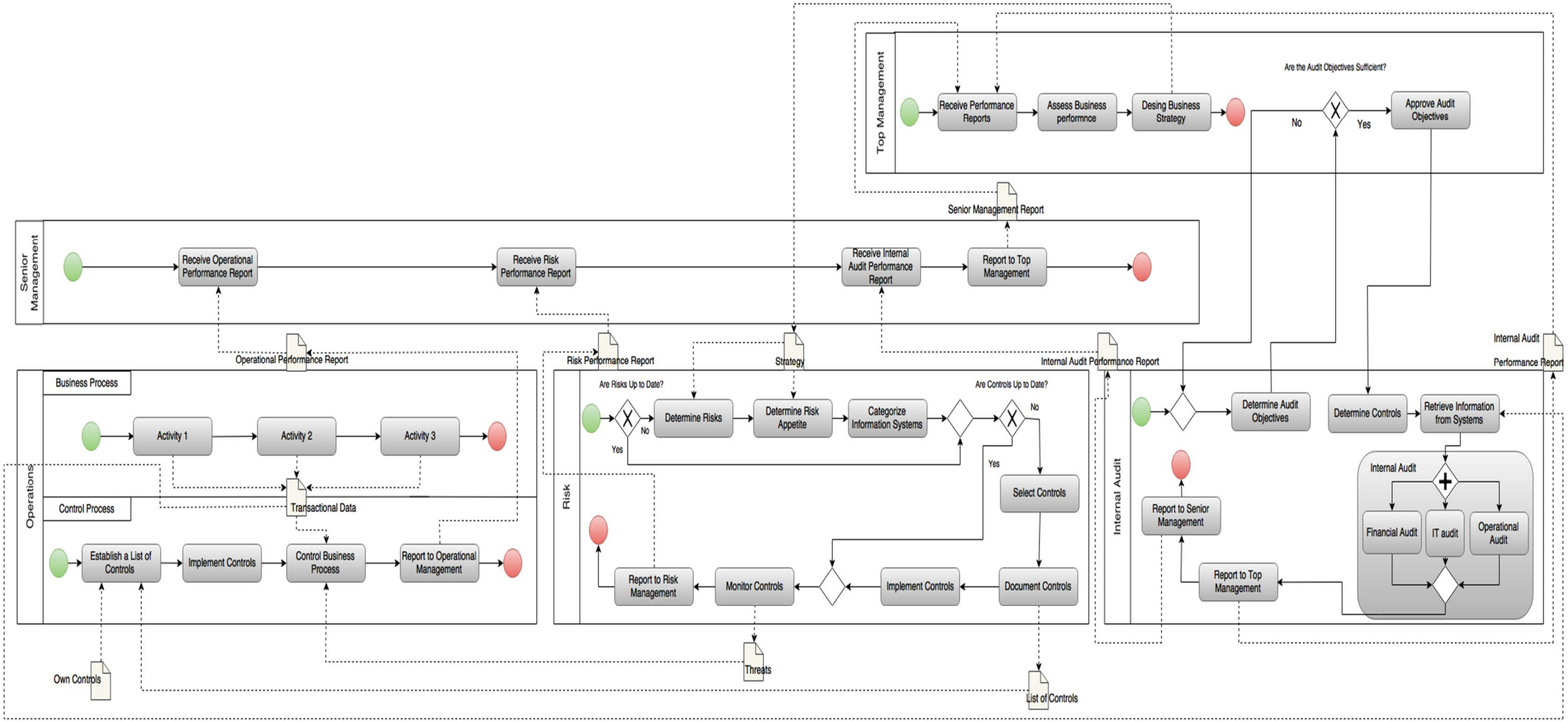


FIGURE 35. AS-IS SITUATION THREE LINES OF DEFENSE (BETA VERSION).

8.2. Determine Requirements for the “To-Be” Situation

The second iteration of this action design science paper evolves around the development of a “to-be” model and performing a gap analysis on the “as-is” and “to-be” model to determine information management performance differences and model usability. In order to start modeling the “to-be” situation however we will first have to perform a requirement analysis to determine what the requirements for the “to-be” model are. The requirements determined in this chapter are based partially on the literature study and partially on the previous expert interviews as can be seen in figure 36.

The research methodology of figure 31 proposes three parallel actions for this step in the research methodology. These actions are based on collecting a complete set of requirements based on the technological, human and process aspects of the problem statement. The requirement analysis will be modeled in the Archimate 3.0 language [54]. The first step in the analysis will be to construct a stakeholder and driver analysis. The result of the stakeholder and driver analysis serves as input in the requirement analysis.

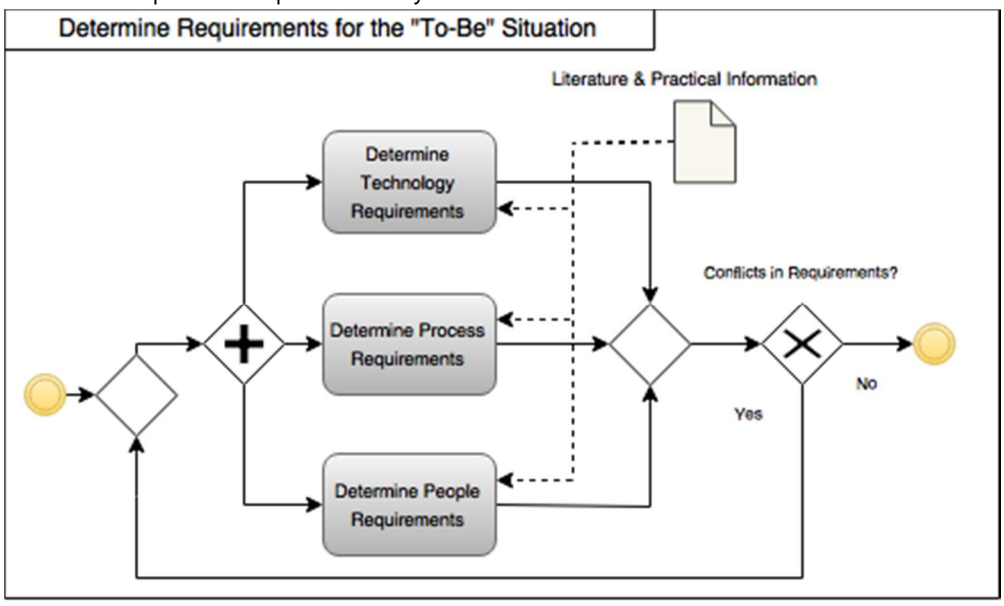


FIGURE 36. DETERMINE THE “TO-BE” SITUATION REQUIREMENTS.

In order to identify stakeholders relevant to any financial company in the three lines of defense process context we will have to make sure the stakeholders are generalized, but still understandable and relevant. Furthermore it is important to note that a company can have internal and external stakeholders. From literature [27], [40], [7], [25], and exploratory expert interviews we derived that from our context’s point of view we can identify two categories of external stakeholders relevant to our paper. The first of these stakeholder categories is called “financial company external stakeholders” in our stakeholder and driver analysis of figure 37. External stakeholders of a financial company are comprised of several separately identifiable groups of people that are mainly interested in the reliability of the financial company. Unethical company behavior will hurt these external stakeholders’ trust of the company or will even hurt them financially. The second external stakeholder group is called “financial sector regulators” in our model of figure 37. This group is comprised of several governing and controlling entities of the financial market that are mainly interested in the company’s compliance to the national and international law and regulations. In the Dutch financial market this group is mainly comprised of the DNB, AFM, ETA, EBA and the Dutch government. For the case of this paper we identified three internal stakeholders most relevant to the problem of this thesis. The three internal stakeholders represent the three lines of defense in the internal control function of a financial company. The operational department, the risk department and the internal audit department are mainly interested in providing assurance to the company. Therefore we identified assurance as the main driver for the three internal stakeholders. Based on the identified external and internal stakeholders and their main drivers the top layer of the model of figure 37 could be designed.

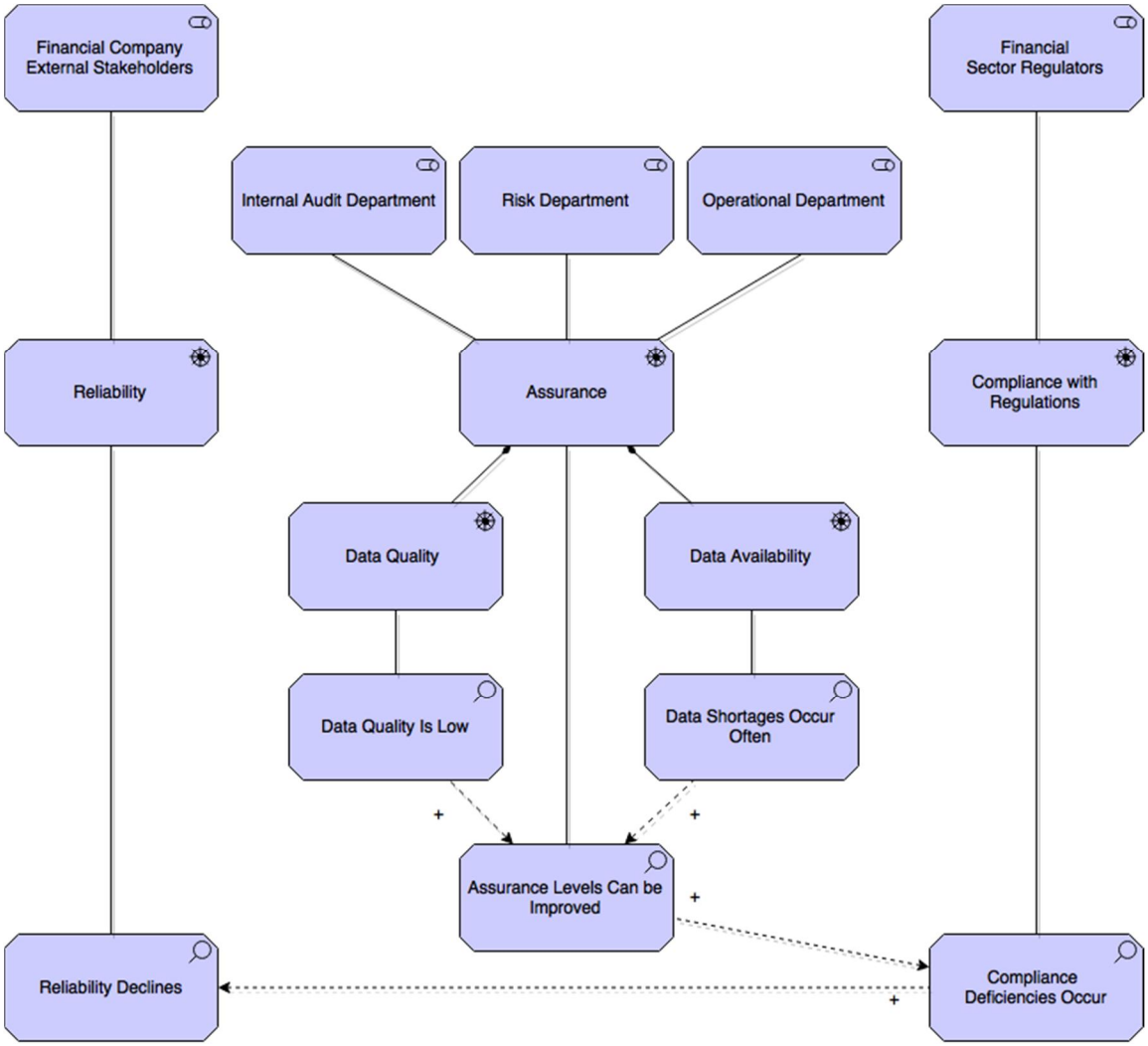


FIGURE 37. ARCHIMATE 3.0 STAKEHOLDER & DRIVER ANALYSIS.

From exploratory interviews with experts of Ernst & Young and their clients we could derive that the main assurance driver behind the redesign of the current assurance process of the three lines of defense and especially the internal audit function can be subdivided into the “data quality” and “data availability” drivers. As described in the problem statement and the research questions of this paper companies are often willing to make a transition to a more data-driven audit process, but their current organizational and IT infrastructure does not allow for such a process at this moment. In the literature study of this paper and in exploratory interviews with Ernst & Young experts we found sufficient evidence for the sub drivers “data quality” and “data availability” [59], [30], [21]. Recent observations of experts within Ernst & Young and clients of Ernst & Young indicate that at the moment data capture within company systems is insufficient to establish complete audit trails. Expert observations also indicate that current data capture, if present, is often not conform the data need of the three lines of defense. Both of these expert observations are modeled in figure 37 as “data quality is low” and “data shortages occur often”. Poor data quality and low data availability both influence the observation that the current assurance level can be improved. Because the assurance level is currently too low some compliance deficiencies occur as can be seen in recent news reports about some companies in the Dutch financial sector [42]. These news reports in turn influence the perceived reliability of the company negatively.

The underlying goal of redesigning the current three lines of defense process situation will therefore be on improving the assurance level provided by the three lines of defense through means of data-driven audit. The desired outcomes of this redesign are that the technological capabilities level, the process performance level and the people skill level of the three lines of defense will be enhanced as stated before in this paper. Exploratory interviews with experts as well

as literature [59], [21], [29] analyzed in the literature study part of this paper provided us with several desired sub-outcomes, their priorities, requirements and constraints. Figure 38 provides a graphical overview of the relations between the semantical notations.

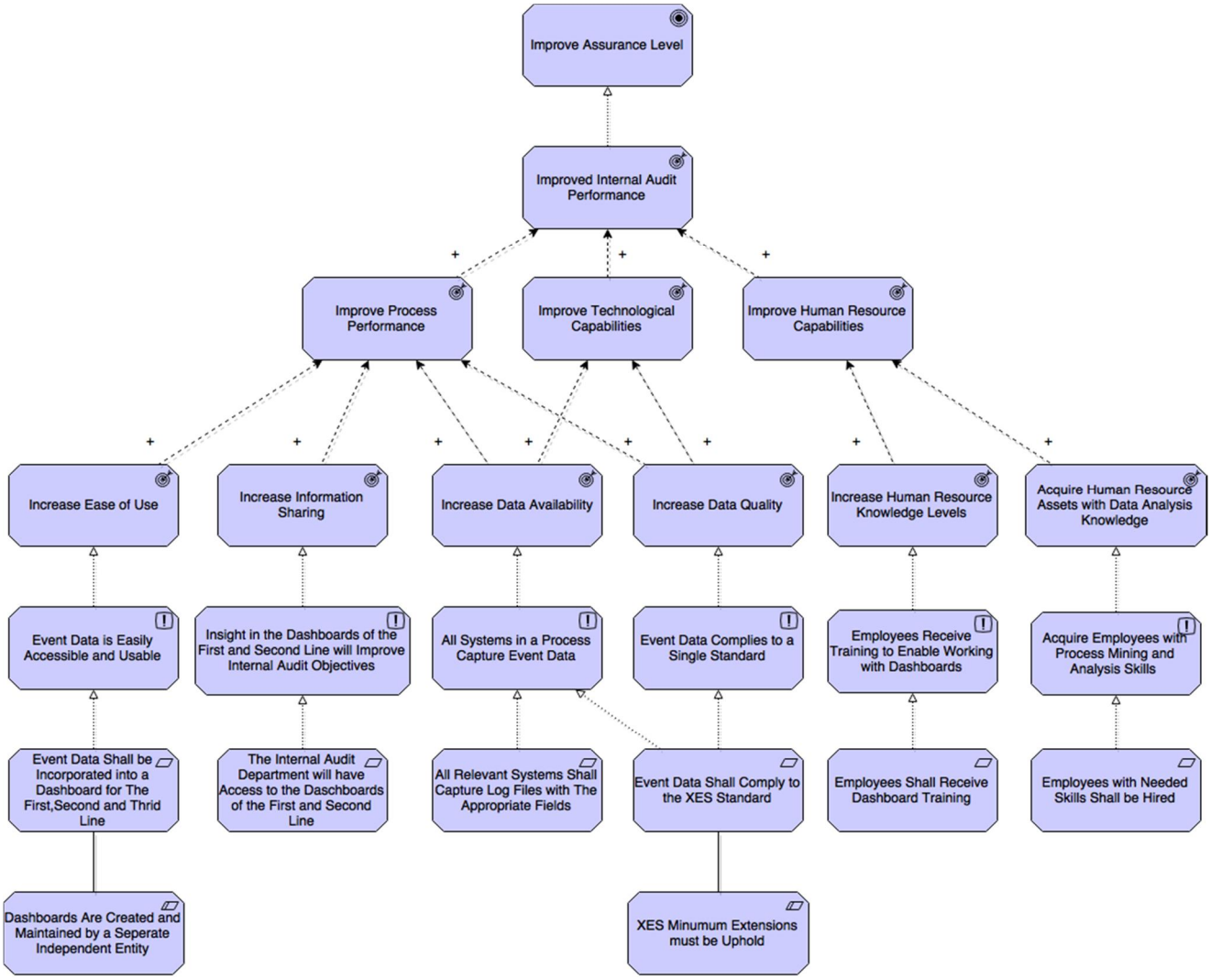


FIGURE 38. ARCHIMATE 3.0 REQUIREMENT ANALYSIS.

TECHNOLOGICAL REQUIREMENTS

One of the main issues with the current situation is that data needed for IT audits and operational audits are often either not available or qualitative not sufficient. In order to solve this issue we investigated into the field of process mining and business process activity monitoring in the literature study. Conversations with experts at Ernst & Young have also indicated that process mining can add additional quality and accuracy to assurance processes. In the literature study we identified a set of XES standard extension which we will propose as requirements for event data used in process mining in this paper. The requirements translate as follows:

- Each audit trail entry should contain a concept extension field, describing the names of the elements.
- Each audit trail entry should contain a lifecycle extension field, describing the lifecycle transition of an element.
- Each audit trail entry should contain an organizational extension field, describing the actor, role and group of the invoking person.
- Each audit trail should contain a time extension field, describing the date and time the event occurred.

- Each audit trail should contain a semantic extension field, describing to which higher level entity the entity refers.
- Each audit trail should contain an ID extension field, describing its unique ID code.
- Each audit trail should contain a cost extension field, describing the cost and cost drivers associated with the entity.

Because the usage of event data is relatively new to a lot of organizations in the financial sector we will have to include the capture of this data in the "to-be" model separately from the transactional data that is stored in during the execution of business process instances. In addition to the capture of this event data, the data should also be used for audit purposes within the three lines of defense. We argue in this paper, based on literature [24], [7], [30], that the development of event data-driven dashboards can provide the three lines of defense with a graphical overview useful for analysis purposes.

PROCESS REQUIREMENTS

Process requirements for the "to-be" situation evolve mainly around the addition of event data-driven dashboards to the processes of the three lines of defense. For this reason the systems of the business processes executed by the operational department, or first line of defense, will have to be enabled to capture event data. This event data will be represented in the "to-be" situation separately from the transactional data captured in the business processes of the operational department. In order to provide practitioners with a graphical representation of this data we argue that dashboards should be constructed and maintained based on KPI's communicated from the lines of defense. The baseline for the development of the dashboards should be the knowledge management cycle of the literature study [15]. These dashboards should be accessible by all lines of defense and external parties. The dashboards will speed up data collection for all parties in de three lines of defense model and will help support internal audits. The operational department can use the operational dashboard to monitor implemented controls for the risks identified by the second line of defense. The risk department can use the risk dashboard to better determine risks to the company and the risk appetite. In addition to this the dashboards can help the risk department with the monitoring of risk controls. The internal audit department can use the dashboards of the first and second line of defense to more accurately establish internal audit objectives instead of base the objectives on first and second line reporting. Information latency will be less likely to be an issue in internal audit this way. The internal audit dashboard can support the internal audit department with monitoring internal audit controls based on the internal audit objectives.

PEOPLE REQUIREMENTS

People requirements are based on the training required for employees of the company to raise their data and information awareness as well as elevate their skills in analysis tasks. It also encompasses the acquisition of human resources with certain skills needed in the "to-be" situation. Companies willing to make a transition to a more data-driven way of performing audit processes will have to train their IT departments in developing dashboards that are fed with event data from the relevant systems in the organization as well as train them in enabling the capture of the event data from the systems. New employees with the required skills can also be acquired. The three lines of defense will have to make a transition towards working with event data-driven dashboards and performing analysis tasks based on this. Enabling this will also require training or acquisition of several new employees with the right skills.

CONFLICTING REQUIREMENTS

The main conflict that could arise from the different requirement categories is that the first and second line of defense are supposed to work independently from the third line of defense. For this reason we must take into account that event data is collected objectively. The dashboards build on the event data should visualize relevant information for the practitioners from the different departments. This means that dashboards for the risk department should encompass risk department controls, operations should have access to a dashboard containing also their own controls and internal audit should have access to a dashboards containing their controls. For this reason an independent entity should create the dashboards. Following this reasoning means that the current requirements will not result in a conflict.

8.3. Model the “To-Be” Situation

To continue the second iteration we will have to develop the model of the “to-be” situation as can be seen in the research methodology of figure 31. The basis of this model is already described in the “as-is” situation of section 8.1. The requirements of section 8.2. Provide a baseline for the redesign to the “to-be” situation. Figure 39 provides us with an overview of actions that have to be taken in order to model the “to-be” situation. We will start by developing the “to-be” model in BPMN 2.0, based on the requirements proposed in section 8.2 and expert opinions. The second step will be to evaluate if the “to-be” model incorporates all the requirements proposed in section 8.2.

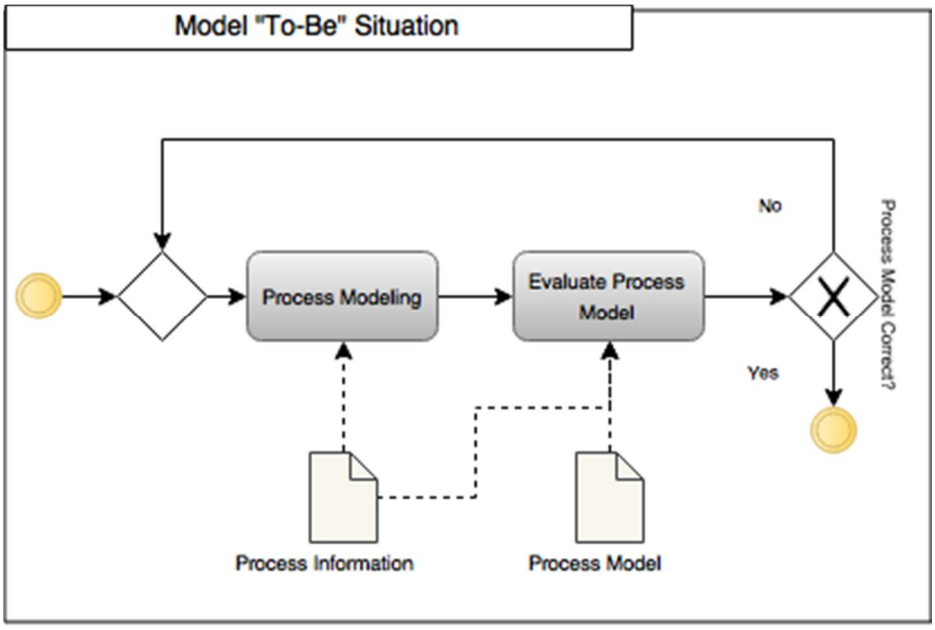


FIGURE 39. MODELING THE TO-BE SITUATION.

PROCESS MODELING

In comparison to the “as-is” situation the “to-be” situation will be based more heavily on IT in order to better support data-driven internal audits. For this reason an extra swim lane called “IT department” is added to the “as-is” three lines of defense model. This IT department is often a companywide department and therefore spans all three lines of defense. The IT department is mainly responsible for implementing the event data capture within the systems of the company’s business processes, according to the XES requirements proposed in this paper. This process is visible in the technology pool of figure 41. The process involves categorizing the business processes of the company, categorizing the IT systems used in these processes, determining the event data requirements for these systems and the implementation of the event data capture in the systems.

In addition to this the IT department will be responsible for developing and maintaining the event data-driven dashboards for the three lines of defense, as described in the process pool of figure 41. The operational dashboard will be fed with event data from the business processes of the company and will be designed around the list of controls used by the first line of defense to control the business. The operational dashboard can provide support for the business monitoring activities of the first line of defense. The risk department dashboard will also be fed with event data from the business processes and will be designed around the controls identified by the risk department to monitor risks. The risk dashboard can be used to support monitoring the risk controls by the risk department. The internal audit department will have the ability to use the dashboards of the first and second line of defense to establish internal audit objectives. Previously reports of the first and second line of defense provided the information for these objectives, but using dashboards will reduce the information latency between the three lines. The IT department will also develop an internal audit dashboard based on the list of controls used by the internal audit department to perform internal audits.

Because many organizations in the financial sector do not have experience with data and process analysis, cases with skill deficiencies will occur. For this reason the “to-be” situation model also encompasses a people pool. This people pool proposes that the three lines of defense as well as the IT department will be provided training. Next to training companies can also decide to hire additional skilled employees. IT department training should precede the training phase of the employees of the three lines of defense according to our model. Our reasoning is that IT department event data implementations in systems and developed event data-driven dashboards can serve as input of the training of the three lines of defense employees. The migration plan of section 8.5 will go deeper into these aspects of training. The implementation of the requirements of section 8.2 and our design choices have led to the model of figure 41, which will serve as the conceptual alpha version “to-be“ situation model.

During the development of the “to-be” situation we had to make sure that in addition to the mostly theoretical requirements of this paper we had to take practice literature into account. As practice literature baseline for the “to-be” model we used a recent Ernst & Young study about the adoption of analytics in internal audit [11].This paper evolves mainly around the model of figure 40, describing the added value of analytics in different stages of the internal audit process. This model can be divided into four analytical aspects of the internal audit:

- Define analytics: Define what data is important for the IA department to analyses during audits.
- Produce analytics: Capture the relevant data.
- Consume analytics: Analyze data based on internal audit controls to support audits.
- Govern analytics: Making sure the previous three steps are incorporated into the IA process as a package deal.

Our “to-be” information management model combines all of these four stages to provide a complete organizational framework. In our “to-be” model of figure 41 event data is combined with department specific controls into dashboards for the first and second line of defense. These dashboards provide a solid basis for the internal audit department to define the IA strategy and annual objectives. Event data capture based on the XES minimum requirements proposed in this paper provide a technological baseline for the production of event data. Furthermore this paper combines people, process and technology aspects to provide a holistic framework. The internal audit dashboard developed by the IT department in collaboration with the internal audit department provides a solid basis for the internal audit department to consume department specific important data. Governance of analytics is one of the main focus points of our framework and is accomplished when a migration from the “as-is” situation to the “to-be” situation is finalized.

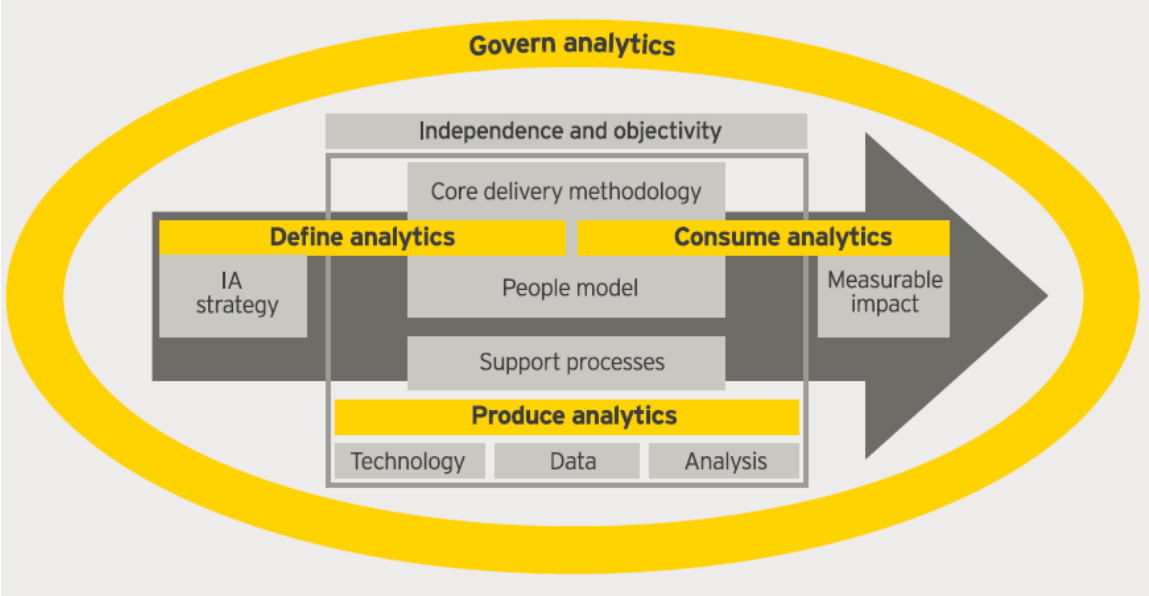
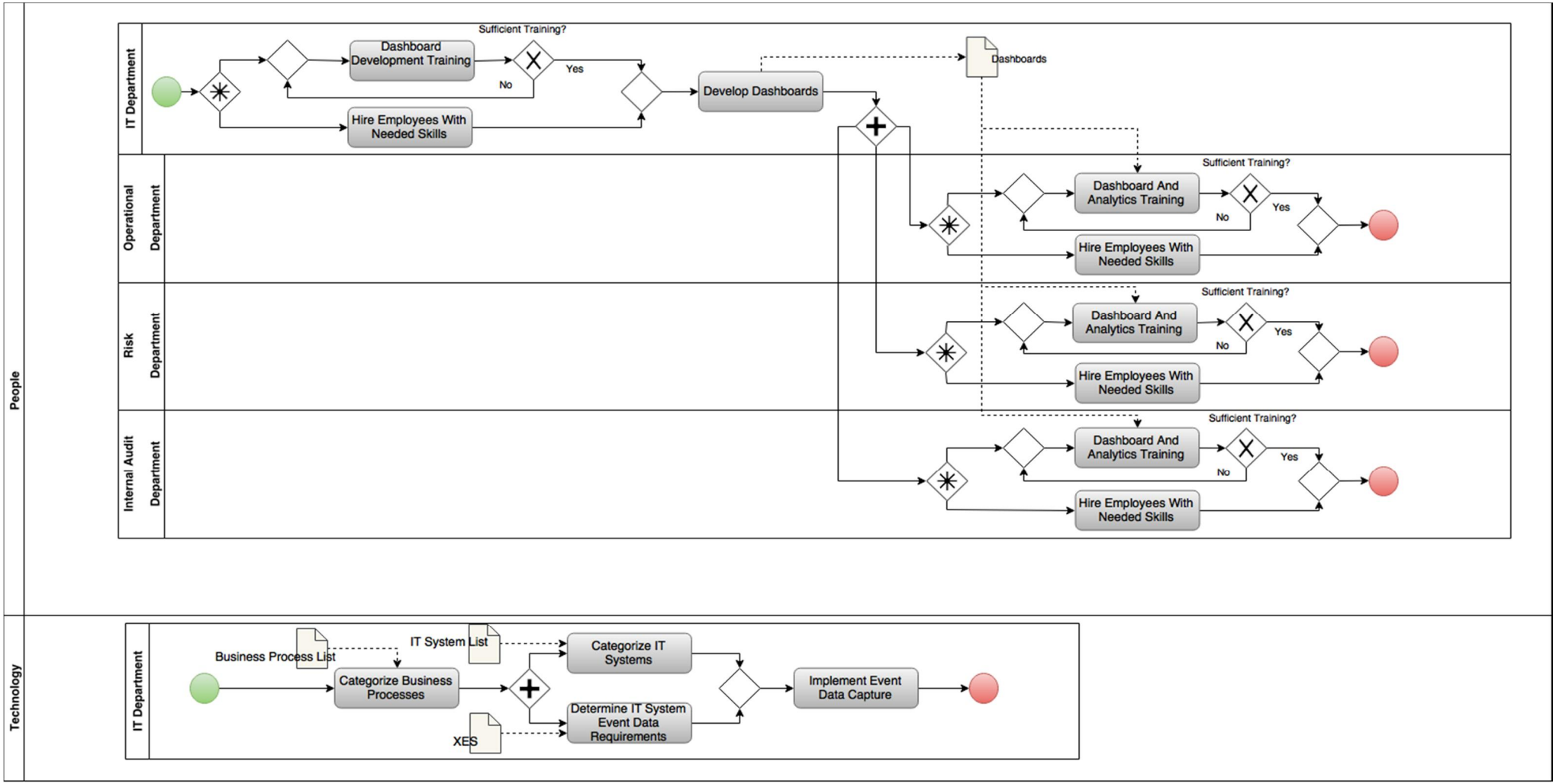


FIGURE 40. ERNST & YOUNG IA ANALYTICS MODEL [11].


People
IT Department
Dashboard Development Training
Sufficient Training?
Yes
No
Hire Employees With Needed Skills
Develop Dashboards
Dashboards
Operational Department
Risk Department
Internal Audit Department
Dashboard And Analytics Training
Sufficient Training?
Yes
No
Hire Employees With Needed Skills
Technology
IT Department
Business Process List
Categorize Business Processes
IT System List
Categorize IT Systems
Determine IT System Event Data Requirements
XES
Implement Event Data Capture

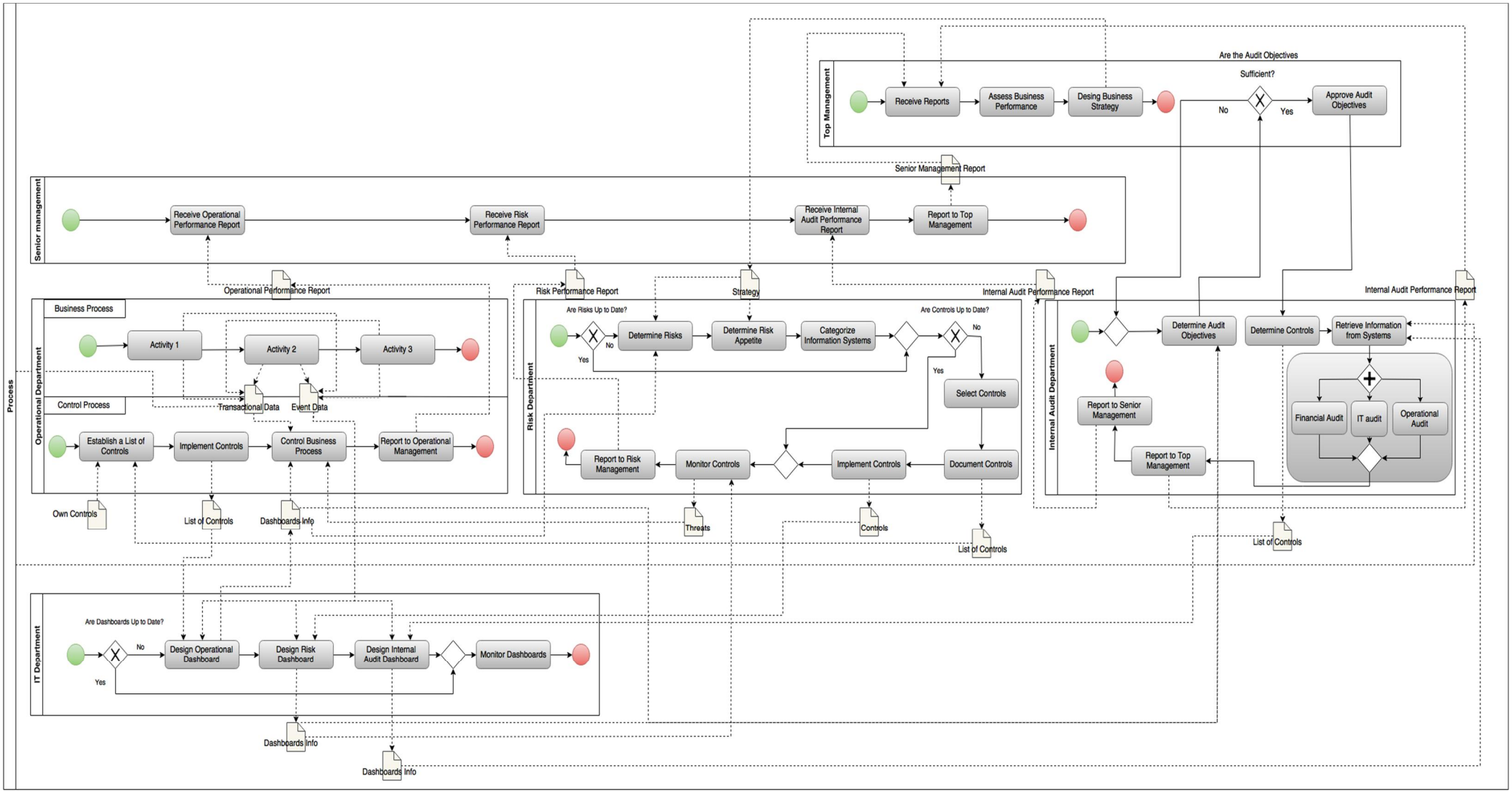


FIGURE 41. TO-BE SITUATION THREE LINES OF DEFENSE (ALPHA & BETA VERSION).

EVALUATE PROCESS MODEL

The focus of this process model evaluation is to check if all process requirements of section 8.2 are accounted for in the "to-be" process model and if the model can be mapped on the IM framework of Maes [37].This evaluation will also look into some of the design decisions that we made while constructing the process model. In section 8.4 a gap analysis between the "as-is" and "to-be" situation will be performed in order to identify if experts perceive the "to-be" situation to deliver better information performances than the "as-is" situation and to determine if usability will go up.

The Strength of BPMN 2.0 is in the easily understandable visualization of processes and data transfers. Therefore we believed that the construction of the "to-be" process model in BPMN 2.0 will aid our information management performance and utility expert interviews in section 8.4. Our choice of semantics however also provided us with some design restrictions, which led to the creation of three separate pools for the technology, people and process requirements.

The technological requirements, which are based on the creation of event data are mainly visible in the technology pool. The actions in this pool require the IT department to implement event data capture in the company's systems according to the XES minimal requirements proposed in this paper. The actual capture and usage of event data is visible in the process pool. Business processes invoked by the operations department result in event data logs stored by the systems used in these processes.

The process requirements are shown the easiest in BPMN 2.0 as it is a process based language. The process requirements are represented in the bottom process pool. The requirements are implemented as follows:

- The event data flow is shown as originating from the different activities of a process model and is fed to the different dashboards created in the model.
- All lines of defense have access to their specific dashboards designed to accommodate their needs. External parties are not modeled in the model, but can have access to all dashboards if needed.
- The dashboards are created and maintained by a separate entity.
- The operational dashboard can provide indications for risks in the company. The risk dashboard helps the risk department with monitoring controls.
- Internal audit objectives can be determined using the dashboards of the operational and risk departments as well as their own insights. The internal audit dashboard provides information for the audits that have to be performed.

The people requirements are represented in the top pool called people. The activities described in this pool indicate that training and acquisition of employees must occur in order to support the skill level of the redesigned process model and to raise people awareness about the redesign. Furthermore the people pool indicates that it is smart to first train the IT department in making dashboards if this is needed and then use the dashboards in the training of the three lines of defense employees.

In the literature study discussion of chapter eleven we were able to map all relevant literature for this paper on the information management framework of Maes [37]. A correct "to-be" model based on the literature, which focuses on solving information management problems, should therefore also be mappable on the IM framework. The implemented requirements of section 8.2 are based on people, process and technology and therefore cover the x-axis of the IM framework: Technological, information/communication and business. Furthermore our "to-be" model focuses on solving the problems of the y-axis: Operational, strategic and structural. It does this by supporting the business through means of capturing data in the business systems, providing data analysis to generate information about the business processes and supporting internal audits to create knowledge about the business.

With the construction of the "to-be" model we can now argue that we have provided an answer to research question ten of this paper:

> RQ10*: "Can we define a framework that helps financial companies with information management to support internal audit operations?"*

8.4. Gap Analysis

In order to finalize the second iteration of the research methodology of figure 31 of this paper we will have to perform a gap analysis to evaluate if the “to-be” situation will increase the three lines of defense information management performance and if the “to-be” process is more easily usable in comparison to the “as-is” situation. Due to the time constraints imposed on this thesis the gap analysis will be based on expert interviews conducted among experts within Ernst & Young and clients of Ernst & Young. As shown in figure 42 of this paper we will have to perform three actions in order to complete the gap analysis. The first two parallel actions are based on performing two expert interviews in order to evaluate the “as-is” and “to-be” situation utility and performance. The third step is to identify the gaps between the two situations. Based on the identified gaps we will be able to construct a migration plan in section 8.5 of this chapter.

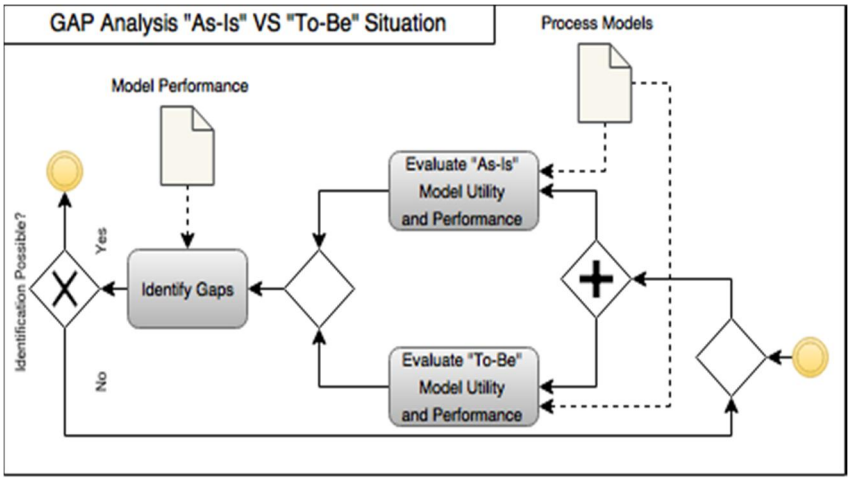


FIGURE 42. GAP ANALYSIS STRUCTURE.

EVALUATING “AS-IS” MODEL UTILITY AND INFORMATION MANAGEMENT PERFORMANCE

Evaluation of the information management performance of the current way of executing internal audits will be done through means of interviews with two experts with a different background. One Ernst & Young expert, with experience in data-driven audit methods, will be interviewed and an expert of a client of Ernst & Young will be interviewed, who is not familiar with data-driven audit methods. During this interview problems and benefits of the “as-is” situation will be identified. The interview structure and results are available in appendix G.

The interviewees indicated that in the current situation of the three lines of defense model there are problems arising from information shortages. These shortages occur because there are no agreements on how the sharing and capture of information should work in practice. In the current situation some tools or reports are used to gain insight in what the other lines have found. The problem with this is that the intended user of these reports is often the senior or top management and not another line of defense. In addition to this some findings will not be reported because of strategic reasons. Since these reports do form the basis of the establishment of internal audit objectives this often will mean that those objectives are not accurate and are based on older information. A data-driven approach of internal audit is not often used, since the basics in terms of technological capabilities and human resource capabilities for data and process mining are often not available. The main technological implication is present in the capture of event data. Event data is either qualitative not sufficient or not present at all. No event data standards are followed presently in almost all companies in the financial sector.

EVALUATING “TO-BE” MODEL UTILITY AND INFORMATION MANAGEMENT PERFORMANCE

In order to compare the information management performance and utility of the “to-be” situation organizational framework of this paper to the current “as-is” way of working we will perform an interview with practitioners to evaluate the “to-be” process model of figure 41. This interview will determine if performance will go up due to the artifact created in this paper and will evaluate the “to-be” model usability. This expert interview is conducted among the same

two experts as the “as-is” model utility and information management performance interview to make sure both backgrounds are represented and all gaps are identified. The interview structure and results can be found in appendix H.

The interviewees indicated that in the “to-be” situation the addition of event data incorporated into dashboards will provide real-time insight and will probably improve the overall audit accuracy. This new approach will also make the auditing more data-driven. The establishment of annual audit objectives will improve if the dashboards of the first and second line of defense are developed in such a way that the third line of defense can use them for the purpose of developing annual audit objectives. The interviewees did not believe that their jobs would become easier, but a more data-driven approach would decrease the time needed to perform certain audits. Training will be needed to elevate the data and process mining skill level of the three lines of defense employees. The Interviewees believed that problems will arise when trying to implement XES event data capture in the systems of a company. The organizational and cost extensions will be hardest to implement. Both interviewees did however believe that a successful event data capture implementation will help in doing more and more specific analysis for audit purposes. The interviews with the experts did not result in any redesign cases for the “to-be” model. Therefore the model of figure 41 represents the validated “to-be” model and as this paper’s beta version.

IDENTIFYING GAPS

In section 8.5 we will construct a migration plan, which will cover the transition from the “as-is” situation to the “to-be” situation and model this transition in Archimate 3.0. In order for us to do this we will have to clearly identify the gaps between the “as-is” and “to-be” situation. From the interviews we conducted we were able to derive that one of the big challenges of a transition is to implement the technological infrastructure behind the “to-be” model. Both interviewees indicated that it will be challenging to implement all XES minimum requirements as proposed in this paper. In addition to this it will be challenging to construct event data-driven dashboards that are relevant to the different lines of defense. Overcoming the overall technical infrastructure can therefore be seen as one of the big gaps between the two situations. The other big gap that we can identify is based around the organizational aspects of the “to-be” situation. A transition to the “to-be” situation will require a company to redesign the three lines of defense working processes to a situation in which the event data-driven dashboards are used for different tasks within the three lines of defense. As this organizational transition is primarily based on human action and reaction the interviewees believed that problems could arise in the organization transition due to a lack in training and governance. This will obviously mean that employees responsible for the technical transition and the three lines of defense activities will require sufficient training to make sure they acquire the right data and analysis skills. In addition to this clear policies should be developed concerning the “to-be” situation way of working. These policies should be delivered in the company from a top-down perspective to make sure process and data awareness is elevated at all employees.

8.5. Migration Plan

The third and last iteration of the research methodology of this paper, as shown in figure 31, will start with the development of a migration plan in Archimate 3.0 [54]. This migration plan deals with the transition from the "as-is" situation to the "to-be" situation. The migration plan will deal with the gaps identified in section 8.4 of this chapter. As shown in figure 43 we will have to perform four activities to design a complete migration plan. The first three parallel activities focus on designing a migration model that is complete in addressing people, process and technology gaps between the "to-be" and "as-is" situation. The last activity will focus on evaluating the usability and advantages of the migration plan among three experts within Ernst & young and their clients.

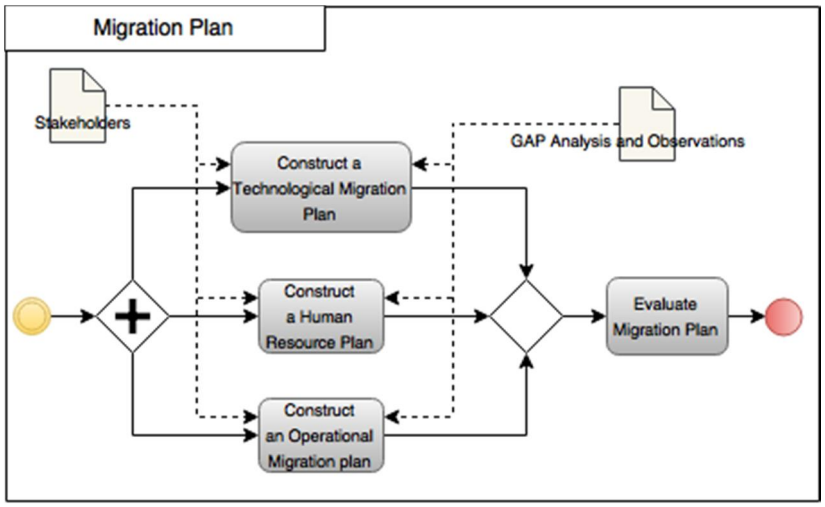


FIGURE 43. MIGRATION PLAN DEVELOPMENT.

In order to make sure all important aspects of a transition migration are represented in the migration plan constructed in this chapter we will use the gaps identified in section 8.4 and combine them with the relevant critical success factors (CSF) identified in the paper *"Investigating success factors in enterprise application integration: a case-driven analysis"* by Lam [32]. Even though the artifact of this paper is based around data and process mining technologies and therefore does not necessarily constitute to an enterprise application, the case of this paper does resemble an enterprise application integration (EAI) case in terms of technological, human and process challenges. Some examples of this are [32]:

- Both this paper's case and EAI involve activities associated with integration of existing information systems.
- Both this paper's case and EAI require upfront strategic planning on which systems are to be integrated.
- Both this paper's case and EAI impact multiple information systems in a company.
- Both this paper's case and EAI span divisional boundaries, which complicates designating project owners and identifying the stakeholders.
- Both this paper's case and EAI lack established practitioner methodologies for migration.

Furthermore Lam says the following about the usage of critical success factors:

"However, CSF studies are still valuable for making sense out of problems where there are many potential factors influencing the outcome, and where the researcher hopes to make a set of practical recommendations based on the most influential factors." [32]

The establishment of the "to-be" situation, as proposed in this paper, is certainly identifiable as a problem where many factors influence the outcome, and where we as researchers are aiming to make practical recommendations based on the influential factors in this section of the research.

TECHNOLOGICAL MIGRATION

The implementation of the "to-be" model proposed in this paper implies several technical changes and integrations. During the planning stage of the transition a technical architectural plan should be constructed, which is based around determining key systems and process in an organization as well as preparing an event data capture plan based on the data need of the three lines of defense. The data capture plan should contain a tool selection strategy for data mining, process mining and the implementation of event data capture in the systems of the organization. By developing these plans experts will prepare for integration problems in legacy systems as well as prepare a technology migration time planning, which are two of the CSF's determined by Lam's paper [32]. The technical architectural plan should be based on the XES minimum requirements described in this paper, as this ensured the third, common data standards, CSF described by Lam [32]. The technical architectural plan should also include a list of mature tools that will be used for data and process mining activities in the finalizing steps of the migration, which are the fourth and fifth technical CSF described by Lam in his paper [32].

The road map, which is also created in the planning stage of the migration should developed based on the findings of the technical architectural plan as well as the human resource training plan and organizational transition plan, which will be discussed in the next two sections. During the actual transition phases to a data mining organization and a process mining organizations respectively the technical architectural plan should serve as a guide for the implementing experts.

HUMAN RESOURCE MIGRATION

The human resource migration deals with human opinions about the project. According to Lam's paper it is vital to make sure all stakeholders of the project and the top management of the organization are on board as the transition to the "to-be" situation will influence the way of working within the three lines of defense a lot and will often require the top management of an organization to invest a lot of money. Stakeholder and top management commitment and overcoming resistance to change serve therefore as the sixth, seventh and eight CSF according to Lam's paper [32]. Prior to the initiation of the transition these commitments to the transition should be clear and should remain clear during the project. One of the main aspects off overcoming resistance to change is to actively educate employees of the three lines of defense in data and process mining technologies important to their role in the company as well as making sure the "to-be" situation will fit the organization specific structure and culture. For this reason a human resource training plan should be constructed in the planning stage of the transition. This plan will deal with the eighth, ninth and tenth CSF, resistance to change, organizational and cultural fit and employee skill level fit respectively [32].

OPERATIONAL MIGRATION

In this section we will look at the operational aspects of the migration. The main deliverable from this perspective is the organizational transition plan and the roadmap, which are also constructed in the early planning stage of the migration. In the organizational transition plan the overall integration strategy, which is the eleventh CSF, should be clarified. This strategy will include aspects of how the three lines of defense processes will change towards data and process analysis processes and what business processes will be first to change towards this. Employee awareness of their role in the organization is important here. By developing this strategy it will be possible for employees of the three lines of defense to start with data and process analysis techniques respectively on business processes which are already implemented for this purpose during the timespan of the whole transition. These early analysis will provide implementing experts with monitoring feedback and will serve as a testing ground, which represent the twelfth and thirteenth CSF of the paper of Lam [32]. Developing a roadmap that will incorporate the technical architectural plan, the human resource training plan and the organizational transition plan will ensure that all activities of the migration are planned ahead of time and will provide a realistic schedule, which is the last CSF identified by Lam [32].

Table three provides an overview of how we have mapped the critical success factors, used in the construction of the migration planning model, on the information management split of the paper of Maes [37] and on the identified gaps between the "as-is" and "to-be" situation of section 8.4.

TABLE 3. CRITICAL SUCESS FACTOR MAPPING ON INFORMATION MANAGEMENT AND IDENTIFIED GAPS.

Technological	Critical Succes Factor	Gap Identified	Maes IM Framework	IM related Topic	Deliverable
CSF 1	Technological Migration Time Planning	Techincal Infrastructure	Business - ICT Allignment	BPM and Data/Process Mining	Techincal Architectural Plan
CSF 2	Legacy System Planning	Techincal Infrastructure	Business - ICT Allignment	BPM and Data/Process Mining	Techincal Architectural Plan
CSF 3	Common Data Standards	Techincal Infrastructure	Strategy - Operations Allignement and Business - ICT Allignment	Data/Process Mining	Techincal Architectural Plan
CSF 4	Using Mature Tools	Techincal Infrastructure	Business - ICT Allignment	Data/Process Mining and BAM	Techincal Architectural Plan
CSF 5	Using the Right Tools	Techincal Infrastructure	Business - ICT Allignment	Data/Process Mining and BAM	Techincal Architectural Plan
Human					
CSF 6	Top Management Commitment	Organizational infrastructure	Strategy - Operations Allignement	Governance and Risk Management	Letter of Commitment
CSF 7	Stakeholder Commitment	Organizational infrastructure	Strategy - Operations Allignement	Governance and Risk Management	Letter of Commitment
CSF 8	Overcomming Resistance to Change	Organizational infrastructure	Strategy - Operations Allignement	Governance and Risk Management	Letter of Commitment
CS 9	Organizational and Cultural Fit	Organizational infrastructure	Business - ICT Allignment	Governance and Risk Management	Training
CSF 10	Empoyee Skill Level	Organizational infrastructure	Business - ICT Allignment	Governance	Training
Operational					
CSF 11	Proper Migration Approach	Organizational infrastructure	Strategy - Operations Allignement	Governance and Risk Management	Organizational Transition plan
CSF 12	Monitoring and Feedback	Organizational and Technical infrastructure	Strategy - Operations Allignement and Business - ICT Allignment	BAM	Training on implemented business processes
CSF 13	Adequate Testing Plan	Organizational and Technical infrastructure	Strategy - Operations Allignement and Business - ICT Allignment	Data/Process Mining and BAM	Training on implemented business processes
CSF 14	Realistic Project Plan and Schedule	Organizational infrastructure	Strategy - Operations Allignement	Governance and Risk Management	Organizational Transition plan

Figure 44 provides a graphical overview of the complete migration plan in Archimate 3.0 combining the technical, human resource and operational aspects of the transition. Figure 44 serves as the alpha version migration plan of this paper.

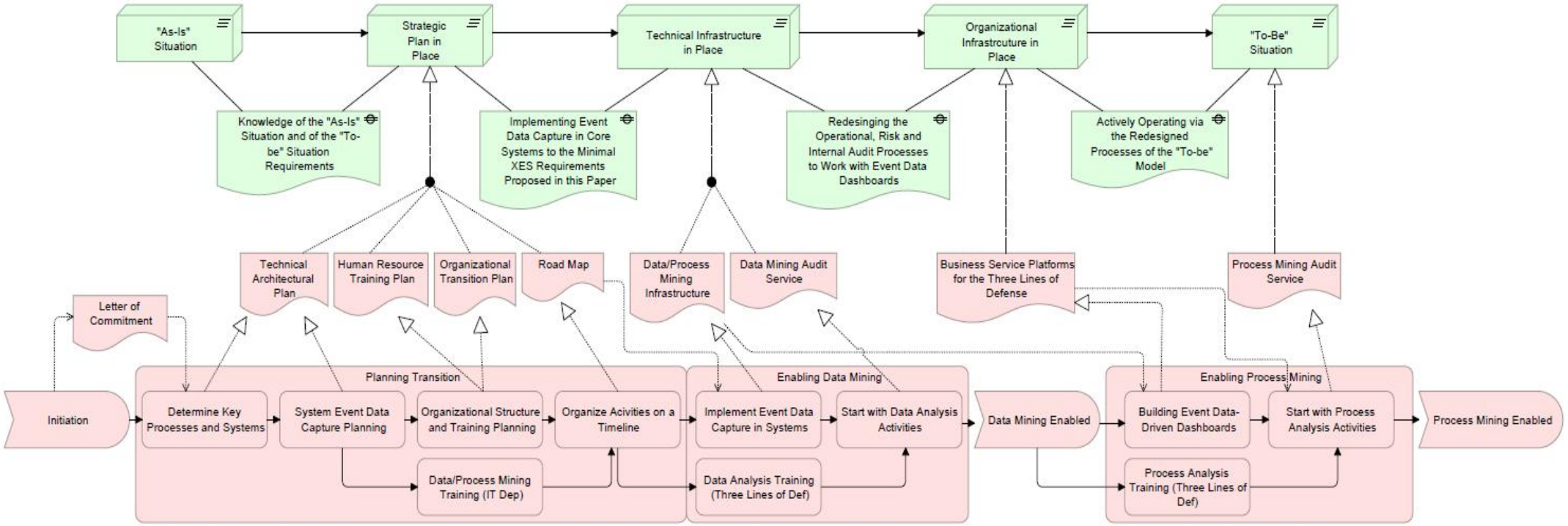


FIGURE 44. MIGRATION PLAN (ALPHA VERSION).

EVALUATION OF THE MIGRATION PLAN

In order to evaluate the utility of the proposed migration plan of figure 44 in this thesis we will conduct several interviews with experts from Ernst & Young and clients of Ernst & Young. This interview will determine if the proposed migration plan will provide a usable template for practitioners to manage the transition from the “as-is” situation to the “to-be” model in their organization. Practitioners will also be asked if they think that following the migration plan proposed in this paper will help their organizations maximize the “to-be” process information management performance. One Ernst & Young expert will be interviewed for this interview as well as two client experts from companies with different data-driven IA maturity. The interview structure and results can be found in appendix I.

The interviewees indicated that overall the conceptual migration plan model of figure 44 provided a good overview of how a transition from the “as-is” to the “to-be” situation of this thesis will look like. All interviewees indicated that this model also provided a good practical baseline for experts that are starting up such a transition. Regarding the deliverables in the migration plan model one of the interviewees indicated that in the strategic plan plateau of the model she would have expected a policy and tool selection strategy deliverable. We indicated that this is one of the aspects of the technical architectural plan and the organizational transition plan, but we understood that this was not clear from the interviewee’s point of view. In the validated beta version model of figure 45 we have chosen not to add separate deliverables for these aspects in the migration plan beta version of figure 45, but we have instead chosen to describe the deliverables separately in table 4. Another expert indicated that it is smart to add a business case deliverable for the strategic plan plateau. From this business case the letter of commitment, representing the commitment of the stakeholders, can be derived better. We agreed to this and have added this in figure 45. Two experts indicated that the process was to linear and should include feedback loops in the lowest level of the model. Feedback loops have been added in the model of figure 45. All experts indicated that the training activities in the model are very important and combining this with a feedback loop to the implanting team will make sure the project results will be better. In addition to this all experts indicated that stakeholder commitment to the project prior to the start of implementation is of vital importance. Two experts expected that the information management performance of the “to-be” situation would be better when following this migration plan in contrast to working without a plan. One of the experts thought it would only decrease the implementation time, but would not result in better information management performance. All experts indicated that it is smart to start with the key business processes and systems as indicated in the migration plan. However two experts indicated that they would probably do a pilot on an easy to implement system first. Our University of Twente supervisors indicated that during the migration process it would be vital to track if the CSF’s are accounted for. These monitoring activities have also been added to the beta version migration plan model of figure 45.

The migration plan model of figure 45 Therefore serves as the validated beta version migration model in this paper.

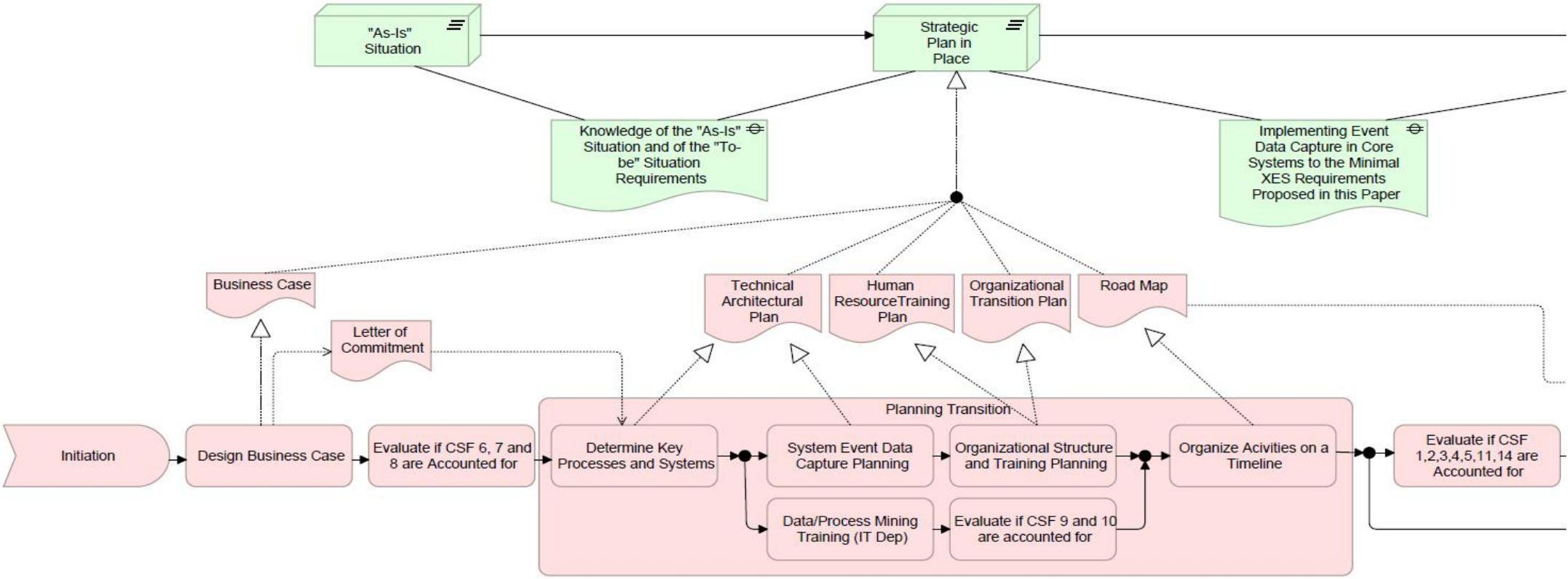


FIGURE 45. MIGRATION PLAN (BETA VERSION)

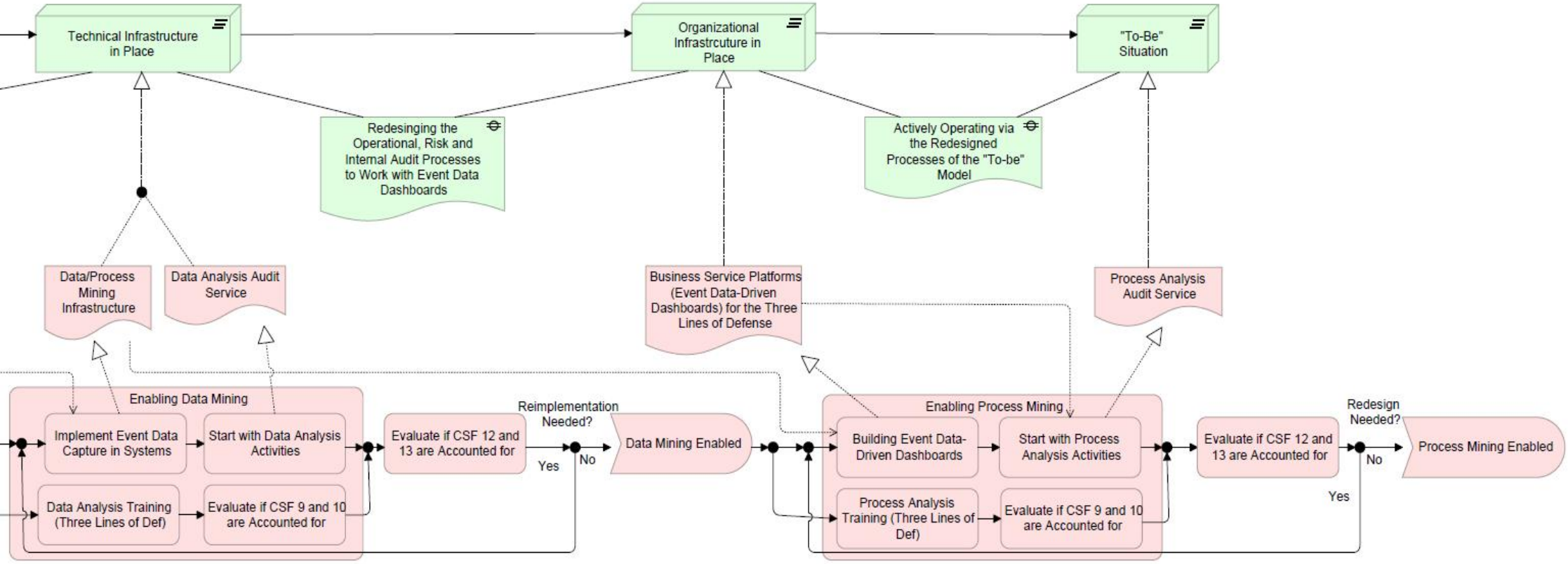

Technical Infrastructure in Place
Organizational Infrastrcuture in Place
"To-Be" Situation
Redesinging the Operational, Risk and Internal Audit Processes to Work with Event Data Dashboards
Actively Operating via the Redesigned Processes of the "To-be" Model
Data/Process Mining Infrastructure
Data Analysis Audit Service
Business Service Platforms (Event Data-Driven Dashboards) for the Three Lines of Defense
Process Analysis Audit Service
Enabling Data Mining
Implement Event Data Capture in Systems
Start with Data Analysis Activities
Data Analysis Training (Three Lines of Def)
Evaluate if CSF 9 and 10 are Accounted for
Evaluate if CSF 12 and 13 are Accounted for
Reimplementation Needed?
Yes
No
Data Mining Enabled
Enabling Process Mining
Building Event Data-Driven Dashboards
Start with Process Analysis Activities
Process Analysis Training (Three Lines of Def)
Evaluate if CSF 9 and 10 are Accounted for
Evaluate if CSF 12 and 13 are Accounted for
Redesign Needed?
Yes
No
Process Mining Enabled

Table 4 provides a more detailed description of the different deliverables described in the migration plan of figure 45 of this paper.

TABLE 4. DETAILED MIGRATION PLAN DELIVERABLE OVERVIEW

Migration Plan Deliverable	Input	Activity	Tools & Techniques	Output
1. Business Case	• List of stakeholders • Prediction of cost and benefit over time • List of critical systems and processes • Transtion goals	• Cost-benefit analysis • Listing of corporate skills and capabilities	• Financial analysis and prediction techinques • Sensitivity analysis	• Detailed business case
2. Letter of Commitment	• List of stakeholders	• Mediation and securing commitment	• Discussion based on the business case	• Letter of commitment
3. Technical Architectural Plan	• Three lines of defense data need based on XES • List of critical systems and processes	• Determine strategy for event data capture • Determine strategy for data/process mining tool selection • Selection of data/process mining vendors	• Strategy development tools and techniques • Selection strategy	• List of data/process mining tool vendors • Event data capture plan • Technical architectural plan
4. Human Resource Training Plan	• List of stakeholders • List of essential data and process mining courses and trainings	• Developing a strategy to maintain stakeholder commitment throughout the project • Matching employees with relevant and essential trainings	• Strategy development tools and techniques	• Clear stakeholder commitment throughout the project • Human resource training plan
5. Organizational Transition Plan	• To-be model gap analysis • Technical architectural plan	• Determine policies relevant to the to-be situation • Determine when to start with data and process analysis activities and on which processes and systems	• Strategy development tools and techniques • Policy development techniques	• To-be situation policy list • Organizational transition plan
6. Road Map	• Technical architectural plan • Human resource training plan • Organizational transition plan	• Planning of activities on a timeline	• Planning tools and techniques	• Road map including time planning
7. Data/Process Mining Infrastructure	• Technical architectural plan	• Enabling event data capture in the business systems to accommodate three lines of defense data need	• Event data capture tools and techniques	• Infrastructure based on the three lines of defense data need and the XES standard
8. Data Analysis Audit Service	• Datasets of event data capture enabled systems • Skilled employees • To-be situation model	• Working via the to-be situation model using data sets from systems that the have event data capture enabled	• Data analysis tools and techniques	• Data analysis based internal audit
9. Business Service Platforms	• Event data • Line of defense sepcific controls	• Develop event data-driven dashboards for the three lines of defense	• Dashboard development tools and techniques	• Event data-driven dashboards for the three lines of defense
10. Process Analysis Audit Service	• Event data driven dashboard information • Skilled employees • To-be situation model	• Working via the to-be situation model using event data-driven dashboards for analysis activities	• Process analysis tools and techniques	• Process analysis based internal audit

DISCUSSION AND CONCLUSION

9. Discussion

In this chapter the results of this thesis will be discussed. This is done based on the action design science methodology used in this paper [51], the design goals proposed in this paper and based on a final artifact discussion with experts. In the final artifact discussion three experts from Ernst & Young were presented with the beta version of the artifact constructed in this paper and were presented with the design methodology used in this paper. All of the experts were actively involved in the previous validation iterations and therefore already posed substantial knowledge about the artifact prior to the discussion. An overview of the discussion structure and results can be found in appendix K.

In section 9.1 the relevance of this research and its artifact are discussed in relation to the main research question proposed in this paper. Discussing the research goals will provide insight into the completeness of the artifact and its ability to satisfy answering the main research question of this thesis. Section 9.2 will go deeper into the model of the "as-is" situation as described in goal one of the artifact design. In section 9.3 the goal of designing a "to-be" situation that improves upon information management and its relating concepts will be discussed. In section 9.4 the third goal of assessing the information management gaps between the "as-is" and "to-be" situation will be discussed. Section 9.5 will go deeper into the migration plan proposed in this paper and will discuss if goal four of the artifact design of this paper is achieved. In section 9.6 the future potential of the artifact of this action design science paper will be discussed.

9.1. Research Relevance and Methodology Goals

The problem statement of this thesis, based on initial conversations with Ernst & Young experts, indicated that there is a rising need for better information management within the three lines of defense to support internal audit operations. Meaning that within the three lines of defense there should be more focus on the usage of process data and there should be more focus on the conversion of data to information and eventually to knowledge. The rising need of better information management mainly comes from the increasing set of control requirements that companies in the financial sector have to accommodate to.

In the literature study of our paper we have combined several subjects related to information management to form a basis of our "to-be" situation design process. With this basis we have described several design goals that our design process should achieve. Our paper design methodology has been based on the Organizational-Dominant BIE model described in the paper of Sein et al. [51]. Through multiple iterations of expert interviews we have validated the "as-is" and "to-be" situation as well as the migration plan. In the interviews experts indicated that the "to-be" model is expected to improve information management within the three lines of defense as well as help the internal audit structure of companies mature to a more data-driven process. We can argue that the combination of literary topics in this paper and the artifact design based on this contribute to the scientific community.

In the final artifact discussion the internal experts of Ernst & Young were asked about the research relevance of this thesis in respect to using the artifact in practice. All experts pointed out that this research was highly relevant to the consultancy domain, since the information management problem within the three lines of defense is a reoccurring problem in most of the clients of Ernst & Young. The goals of our artifact design as proposed in chapter seven were therefore also seen as relevant by the discussion participants. The experts indicated that although this paper has a solid literary basis for the design itself the research will benefit from an actual implementation of the artifact to prove its worth to financial companies.

9.2. "As-Is" Situation Results

To start the design phase of this paper we first had to design a clear picture of how the current situation of the three lines of defense within companies in the financial market looks like at the moment. The first goal of the design phase of this paper focuses on this aspect:

G1: Determine the "as-is" situation of the three lines of defense model by combining expert observations and internal audit literature.

This goal was achieved by following three lines of defense literature and conducting an exploratory interview with an expert of the field. "As-is" model validation interviews resulted in the validated beta version of the model. The main advantage of modeling the "as-is" situation is in the overview of process activities that it provides. In contrast to the three lines of defense model of the IIA [27], which provides only an abstract overview of responsibilities of the three lines of defense, our "as-is" model provides detailed activities per line and models the data transfers between lines. This provides a clearer picture on which we could design a "to-be" model and also provided a baseline situation for subsequent interviews about our proposed changes.

During the final discussion experts indicated that the "as-is" model designed in this paper provides a good overview of how the three lines of defense work in practice. All three experts indicated that the relationship between information management and the "as-is" model is not directly clear from the model solely, because the model is based on the process language BPMN 2.0. This means that without the paper's context it would be hard for Ernst & Young Experts to convince companies that information management can be improved within the three lines of defense of their companies. All discussion participants did indicate that they believed that information management could certainly be improved in the "as-is" situation however. Experts also indicated that in the beta version of the "as-is" model a connection between the reporting of the first and second line and the audit activities of the third line was missing. The experts also pointed out that the naming of the operations department, the risk department and the internal audit department in the model should be changed to first, second and third line to mimic the Three Lines of Defense model of the IIA [27] These final corrections have been added to the final artifact as shown in appendix L.

9.3. "To-Be" situation Results

The second design goal proposed in this paper's design phase evolved around the development of the "to-be" situation and the requirement analysis prior to doing this. The eventual goal of the "to-be model was to improve information management within the three lines of defense to support internal audit functioning. The second design goal translated as follows:

G2: Determine the "to-be" situation of the three lines of defense model by combining knowledge about the "as-is" situation of the first and second line of defense with the requirements analysis of the third line of defense base on information management principles.

This goal was achieved by conducting a literature based requirement analysis towards the requirements of the "to-be" situation and the sequential design of the "to-be" situation based on these requirements. Practice information obtained from the "as-is" exploratory and validation interviews was also incorporated in the requirement analysis. During the requirement analysis the most important stakeholders and their drivers were identified. These drivers eventually led to the requirement list incorporated in the 'to-be" situation model. The model of the "to-be situation was re-evaluated in order to describe how all requirements were implemented. The "to-be" situation was also mapped on the IM framework of Maes [37] to show that the "to-be" situation theoretically proposed an improvement to the information management within the three lines of defense. This improvement was further validated by conducting expert interviews. The interviews also focused on the TAM aspects used in this paper: Perceived ease of use, the perceived usefulness, the attitude towards using and the behavioral intention to use [41].

In the final discussion experts also indicated that the "to-be" model was an improvement compared to the "as-is" model in terms of information management. The inclusion of event data made sure the data quality problem and data shortage problem were solved for relevant controls. The expert participants of the discussion were all positive about using the "to-be" model in future relevant client assignments, because they believed it would have a positive effect on client companies. Initially most of the experts believed that employees of the three lines of defense would have a hard time to adjust to the more data-driven approach of the "to-be" model, but training would make sure the employees would be able to work via the "to-be" data-driven system. Just as with the "as-is" situation the discussion experts indicated that the naming of the operational department, the risk department and the internal audit department should be changed to the first, second and third line to explain the reference to the IIA Three Lines of Defense model [27]. Development of the dashboards would be a first line of defense task in practice according to the experts, so the IT

department name should therefore also be changed to first line of defense. According to the discussion experts this would still ensure segregation of duties between the lines of defense. These corrections have been added in the final artifact of appendix L.

9.4. Gap Analysis Results

In order to assess if the "to-be" situation would lead to better information management performance and in order to determine the utilization of the "to-be" model in comparison to the "as-is" situation a gap analysis was performed. For this gap analysis the third design goal was determined:

> G3: Assessing the impact of the "to-be" three lines of defense organizational framework on information management within the three lines of defense to support internal audit, by performing a GAP analysis between the "as-is" situation and the "to-be" situation.

This goal was achieved by performing two interviews with experts going deeper into the utilization differences between the "as-is" and 'to-be" situation and the expected performance differences between information management in the two situations. The interviewees of the gap analysis interview indicated that because of the incorporation of analytics into the three lines of defense, the conversion of data to information and information to knowledge as explained in the IM framework of Maes [37] would be easier to do and would provide more accurate results. Because of the information management improvements the experts expected that the communication between the three lines of defense would also improve and overall audit results would improve too. Because experts expected improvements from a "to-be" situation implementation they were also positive about working via the "to-be" situation in their day-to-day jobs. Questions regarding the "perceived usefulness, the "attitude towards using" and the "behavioral intention to use" were therefore positively answered by the experts [41]. The interviewees however did not think that working via the "to-be" situation would make their day-to-day jobs easier or harder and therefore the last aspect of TAM, "perceived ease of use" was answered neither positive nor negative [41].

The experts in the final discussion of this paper pointed out that the mayor technical and organization gaps that were identified in the gap analysis of this paper were correct. Certainly in respect to the technical aspects of the "to-be" situation the XES event data logging and the creation of good event data-driven dashboards will be hard to overcome. Overcoming the organizational gap in terms of changing the way of working of employees of the three lines of defense towards the more data-driven way of the "to-be" situation will depend a lot on the company's internal structure and culture according to the experts. The willingness of stakeholders to change the three lines of defense in their companies towards the "to-be" situation of our paper will be affected by the gaps we identified in this paper according to the experts. All experts however believed that the gaps will not deter stakeholders from implementing the "to-be" situation completely. Working towards a more data-driven way of internal audit is according to the experts inevitable, since competitors will also move in this direction and more and more strict regulations force companies in this direction. Experts also believed that the information management performance improvement indicated in our paper will provide companies with enough added value to justify the expenses from changing to the "to-be" situation of the three lines of defense.

9.5. Migration Plan Results

The last design goal of this paper focused on how companies in the financial sector could make a transition form an "as-is" situation to a "to-be" situation. The gaps between the "as-is" and "to-be" situation regarding information management, technical infrastructure and organizational infrastructure identified in this paper were used as a basis for the migration plan. The last goal translated as follows:

> G4: Providing a migration plan for the process, people and technology aspects of the artifact that addresses how to "to-be" situation can be reached.

This goal was achieved by designing a migration plan in Archimate 3.0 and by conducting an evaluation interview with experts based on the properties of the migration plan model. During the interviews the experts indicated that although the migration plan model was certainly practically useful, an actual "to-be" situation implementation would depend heavily on the company's internal structure. The main limitations to our artifact will be discussed in the conclusion of this paper, but the results regarding the "perceived ease of use" and the "perceived usefulness" of the migration model

turned out more negative, because experts expected several complications during a transition. The "attitude towards using" and the "behavioral intention to use" results were, although overall positive, also negatively influenced, because experts expected complications during a transition. This is however to be expected considering the structure of TAM in the paper of Morris et al. [41]. Two of three experts indicated that the expected information management performance improvement of the "to-be" situation in respect to the "as-is' situation would be better when using the migration plan for a transition, while the other expert only expected a deceased transition time as result of following the migration plan model.

During the validation discussion of the beta version of the artifact of our paper experts pointed out that above all it was important that a transition towards the "to-be" situation of this paper should be done systematically. The expert thought that the migration plan posed an excellent systematical method in that respect and had the potential to maximize "to-be" information management performance. All experts agreed that the migration plan was certainly practically useful as a baseline for managing a transition to the "to-be" situation. Per company the aspects of the migration plan should be to be made more concrete to be relevant for the individual transition of a single company's three lines of defense way of working. All experts indicated that they would be willing to use the migration plan in practice in future assignments relevant to this thesis. The migration plan did not have to be corrected according to the experts, since it was already complete. The final artifact version can be found in appendix L.

In this paper we conducted serval interviews in the design phase of this paper and a discussion in this chapter based on the action design science cycle used in this thesis [51]. These interviews and the discussion led to the development of the alpha version, beta version and final artifact of this paper. We believe the results of the interviews and the discussion, based on TAM [41] and the IM and KMC frameworks [37], [15], provide an answer to the final research question of this paper:

> RQ11: *"How can we evaluate the effectiveness of this framework on information management in the internal audit context?"*

We have argued that the action design science methodology used for this paper and the design goals of this paper could be used to formulate an answer to the main question of this paper:

> What is the appropriate framework for financial companies to govern information management within the three lines of defense to ensure complete audit trails in the third line of defense?

We have identified that there is a need to improve information management within the three lines of defense to support internal audit objectives. All experts in the final artifact validation discussion as well as the prior interviews told us that the design goals used in this paper provide a well-structured approach to tackle the problem of this thesis. Subsequently all four design goals were acknowledged to be relevant and achieved by experts in the discussion. This means our action design science based methodology, developed in this paper, is adequate as a baseline to design a framework that improves information management within the three lines of defense. As such our methodology is able to provide an answer to our main research question. The answer to the main research question will be discussed in the conclusion of this paper.

9.6. Future Potential

As the artifact of this paper is in essence a scientific based consultancy product its main potential is also based around this field of work. Experts from Ernst & Young indicated in several interviews that the artifact designed in this paper can form a basis for new consultancy jobs in the financial market. This paper's artifact will of course have to be tailored to the company structure of the client company. What this means is that per company the practical implementation of the three lines of defense can, and probably will, slightly differ from the IIA [27] literature based model of the Three Lines of Defense. The migration plan model will also have to be made more concrete based on the internal structure of the client company. During the interviews with Ernst & Young and client experts it was also acknowledged that every company might have a slightly different implementation of the three lines of defense compared to the scientific standard used as a baseline in this paper. When used correctly by consultants in an implementation, the artifact of this paper will of course also provide the internal audit within companies with increased information management performance and therefore this can also be seen as a future potential of this thesis research.

The final discussion provided similar results as the interviews. Experts indicated that they believed the artifacts usefulness was primarily in the domain of three lines of defense consultancy. All experts indicated that the artifact of this paper was likely to be used within Ernst & Young in future assignments focusing on the three lines of defense and specifically the third line of defense, in financial companies. In addition all experts agreed that the artifact of this paper provided an answer to the information management problem that was provided to me at the start of this master thesis.

10. Conclusion

In this chapter we conclude this thesis. Based on the literature study, the action design science methodology used in this paper and the validation and evaluation interviews and discussion conducted in this paper, we are now able to formulate an answer to the main question of this thesis:

> What is the appropriate framework for financial companies to govern information management within the three lines of defense to ensure complete audit trails in the third line of defense?

In order to provide a complete answer the answers to the sub questions of this thesis are shortly revisited in section 10.1. Further suggestions for future research in this area are discussed in section 10.2 as well as several limitations of the research of this paper. In section 10.3 both the contribution to theory and practice of this research are discussed.

10.1. Research Questions

This paper uses several sub questions in order to answer the main research question. The sub questions are answered in several parts of this paper. Question one to nine are answered in the literature study of this paper. The design phase and discussion of this paper provided definitive answer to sub questions ten and eleven. The literature study explored connections between relevant topics to our paper. This provided the backbone of our design phase in which the explored connections were utilized. The discussion provided a final evaluation of the artifact of this paper.

GOVERNANCE, RISK MANAGEMENT & INFORMATION MANAGEMENT

As it was clear to us that the subject of this paper was based heavily around the business controlling departments we had to investigate deeper into the corporate risk management and governance domain and its relationship with information management. This subsection will discuss the answers provided on research questions one, two and three:

1. What are the different corporate risk categories and how do they relate and differ?
2. What are well established risk frameworks?
3. How is information management related to risk?

In section 5.1, 5.2 and 5.3 of chapter five of the literature study risk management and its relation with information management has been discussed.

Risk management, according to several literary papers used in this thesis [45], [23], [24], is the practice of identifying risks to the company based on the external environment of a company and the internal situation of a company. Risk management is one of the main activities of the risk department, or second line of defense [27], in a company. The identification of risks takes place in the risk assessment phase of figure 46. The next step in the risk management process is to determine risk appetite dependent on the company's strategy. Based on the risk appetite the risk has to be treated as shown in figure 46. According to literature [28] there are four types of responses to treat identified risks:

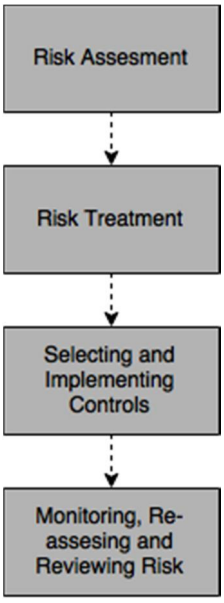


FIGURE 46. RISK MANAGEMENT [23].

- Risk acceptance – accept the risk as it is.
- Risk aversion – Modify the process so the risk disappears.
- Risk treatment – implementing controls to reduce the risk.
- Risk transfer – Using insurance or contracting out the risk.

The third step of risk management involves selecting and implementing controls for the identified risks. The implementation of controls is often done by the operational department, or first line of defense [27], of a company. The last step in risk management is to monitor, re-assess and review risks.

A company is subject to a wide selection of risks. For simplicity these risks are divided into six categories of risk in literature [24]. In our paper three of those categories posed an important role, being: Technology risk, information risk and operational risk [24]. As shown in figure 47 there is significant overlap between the risks of the three categories.

FIGURE 47. RISK CATEGORIES RELATIONSHIP [24].

Governance involves the human aspect of a business and deals with hierarchies and policies that determine the organization structure of a company. Governance is in that respect important to this paper, since it was able to provide us with an overview of how the different lines of defense are organized and what the human impact is on a business structure.

In this paper we used three relevant risk frameworks to further investigate how the risk management works and how it is related to information management. The two most widely used risk frameworks are COSO [7] and COBIT [25]. COSO as a high level risk framework provided us insight into the three main objectives of risk management, being: Operating, reporting and compliance [7]. These three objectives are research when excelling at five components according to COSO, being: controlling the environment, doing risk assessments, controlling activities, collecting and communicating information and monitoring activities [7]. Right away it is clear that one of the main components of COSO involves managing information. COBIT is less high level as the COSO framework and can therefore be seen as extension of COSO. COBIT also focuses more on IT risks than COSO. COBIT is based on the plan-do-check-act (PDCA) and is therefore divided in the following four domains:

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

Obvious again is that the final step “monitoring and evaluate” needs solid information management to function. The final framework we looked into is ISO/IEC 27001 [52]. This framework is also based on the plan-do-check-act and is in that respect also similarly dependent on solid information management. ISO/IEC 27001 is in contrast to COBIT more focused on information risks [52]. The framework is however far less adopted than COSO and COBIT.

So, in short information management has proven to be important in all risk frameworks and overall risk management. Information management literature [37] further confirms this by means of the IM double split shown in figure 48. This double split shows that information management deals with the alignment of strategy and operations and the alignment of business and ICT. These alignments issues are one of the main contributors to the three relevant risk categories identified in this paper and shown in figure 47.

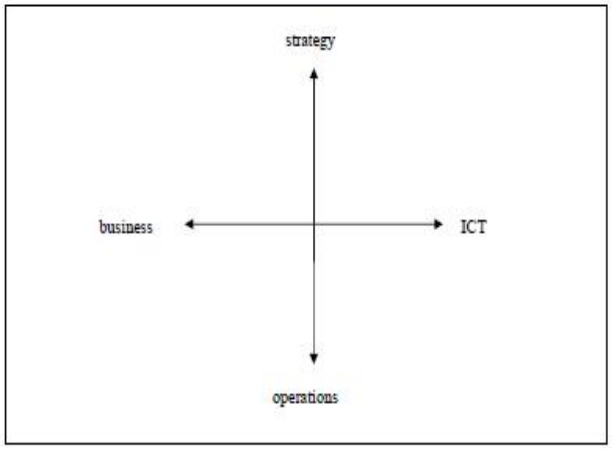


FIGURE 48. INFORMATION MANAGEMENT DOUBLE SPLIT [37].

INFORMATION MANAGEMENT & BUSINESS PROCESS MANAGEMENT

As our paper deals with information management and internal audit aspects such as complete audit trails we also looked into the relationship of information management and business process management (BPM). This subsection will discuss the answers provided on research questions four and five:

4. What is the relation between business processes and information management?
5. What information management theories are available that encompass business information derived from business processes?

In section 5.5 of chapter five of the literature study the relationship between business process management and information management has been discussed.

According to business process management literature [58] BPM involves four steps. Step one involves designing business processes, step tow involves configuring systems in the process, step three involves the enactment of the process and step four involves the diagnosis of the process performance. This cycle is shown in figure 49.

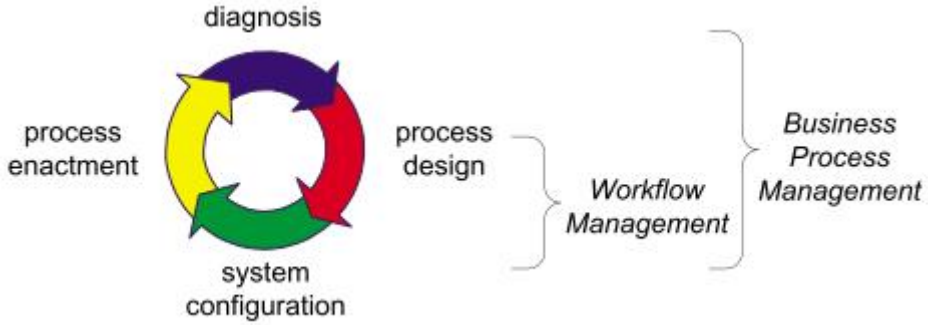


FIGURE 49. BUSINESS PROCESS MANAGEMENT CYCLE [58].

Since our thesis problem statement and research questions evolved around control process and audit processes we identified that the diagnosis step of the business process management cycle is where our paper touches the BPM domain. It is also quite obvious that information management is of vital importance in the diagnosis step of a business process. The subdomain of business process management that focuses on the diagnosis phase is called business activity monitoring, or BAM [30]. Business activity monitoring literature [30], argues that event data can provide the data needed to execute solid diagnosis steps of business processes.

When mapping business process management in the information management framework of Maes [37], which forms the information management bases of this thesis, we can see that business activity monitoring can mainly be mapped on the right and middle column of the IM framework. The right and middle column of this framework deal with the conversion of data into information and covers the technology and information/communication domains. When the using business process management information as knowledge to enhance the problem, then BPM also touches the left business collumn of the IM framework [37].

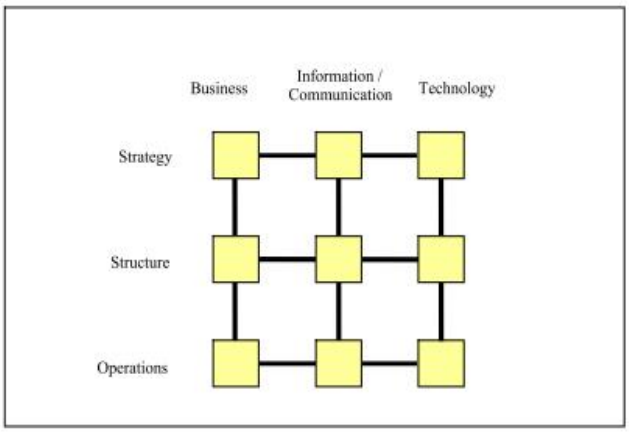


FIGURE 50. INFORMATION MANAGEMENT FRAMEWORK [37].

BUSINESS PROCESS MANAGEMENT AND EVENT DATA

In order to make information management more concrete for our desgn phase we combined business process management with event data in the last part of our literature study. This subsection will discuss the answers provided on research questions six, seven, eight and nine:

6. What are the requirements for log files in order for them to be useful in internal audit?
7. Are any log file frameworks available that support the necessary requirements, so that practical usage is possible?
8. How can log files contribute to internal audit processes?
9. What practical applications are already available that use log files for control purposes?

In section 5.6 of chapter five of the literature study the relationship between business process management, information management and event data has been discussed.

In addition to the IM framework of Maes [37] we also used the Knowledge Management Cycle of Evans et al. as shown in figure 51. This cycle is especially useful to explain how event data relates to information management through business process management. The KMC explains that when a stakeholder desires a certain dataset this data has to either be created or identified, based on the availability of the data. The data is then stored, shared, used, learned from and lastly the dataset is improved. This also forms the basis for the data, information and knowledge transition of the IM framework of Maes [37].

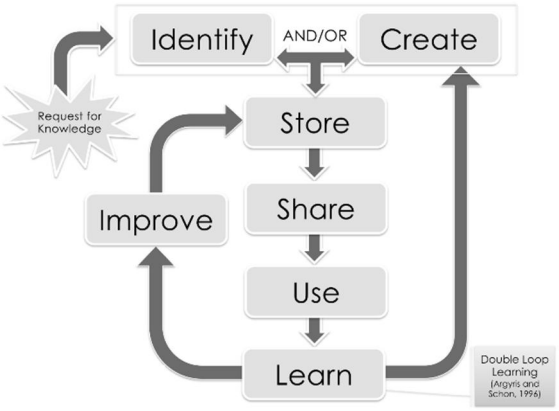


FIGURE 51. KNOWLEDGE MANAGEMENT CYCLE [15].

Event data is important at the "identify and/ or create" stage of this framework and as such forms the basis of the whole transition towards knowledge about the business. In business process mining literature the importance of event data for process controlling has also been stated in several papers [30], [59], [57]. Van der Aalst et al. [59] have developed a process mining life cycle, as shown in figure 52, which we used in the development of the artifact of this paper.

In order to support event data inclusion into our artifact design we also had to look into some requirements for the event data used in our design. Since XES is the most recent standard for event data [21] we chose to use this standard in our paper. In addition to this we choose to use the XES standard extension list as a minimum requirement list for event data in this paper, since literature argues that this set of extensions is always useful to include in event data logs [21].

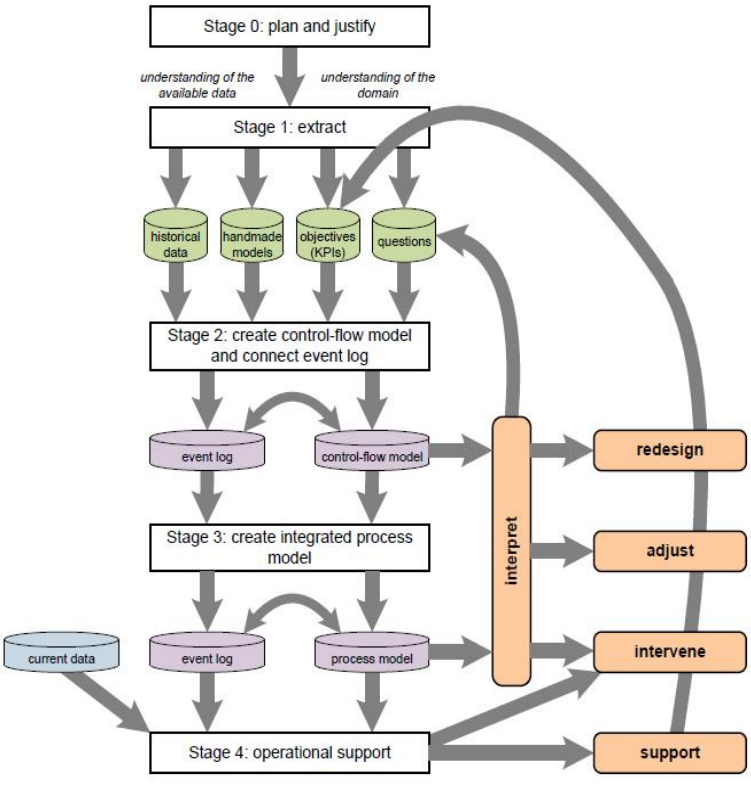


FIGURE 52. PROCESS MINING L* LIFE CYCLE MODEL [59].

The event data minimum requirement list is composed of the following extensions:

- Concept extension: Attribute that stores the name of the element.
- Lifecycle extension: Attribute specifying the lifecycle transition the element is in (standard is the value used as standard).
- Organizational extension: Three attributes specifying for an event which actor has invoked, which role the actor has and what group it belongs to.
- Time extension: Attribute defining the exact date and time the event occurred.
- Semantic Extension: Attributes specifying references to model concepts in an ontology. The ontology concepts are specified with URI's.
- ID extension: Unique element ID.
- Cost extension: Attribute specifying the costs associated with an activity within the log.

DESIGN PROCESS

In these last two subsections will discuss the research methodology used to design the artifact of this paper as well as the evaluation method used in this paper. In addition to this the answer to research question ten and eleven is discussed:

10. Can we define a framework that helps financial companies with information management to support internal audit operations?
11. How can we evaluate the effectiveness of this framework on information management in the internal audit context?

In section 3.6 of chapter 3 and adoption of the the action design research methodology of Sein et al. [51] was proposed to guide this research. The methodology is shown in figure 53.

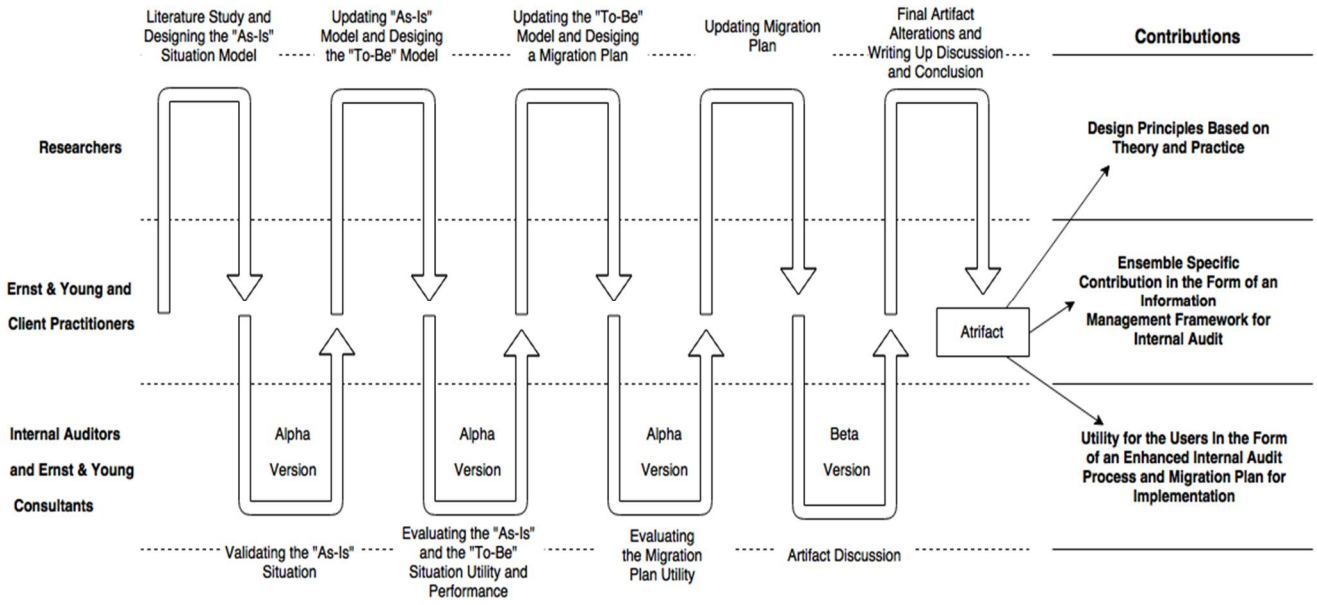


FIGURE 53. RESEARCH METHODOLOGY.

The findings from the literature study as well as the problem statement received from our supervisors within Ernst & Young suggested a "to-be" model of the three lines of defense within financial companies that improved upon information management was possible to develop. Based on the research model of figure 53 we formulated several design goals for the artifact of this paper in chapter seven:

G1: Determine the "as-is" situation of the three lines of defense model by combining expert observations and internal audit literature.

G2: Determine the "to-be" situation of the three lines of defense model by combining knowledge about the "as-is" situation of the first and second line of defense with the requirements analysis of the third line of defense base on information management principles

G3: Assessing the impact of the "to-be" three lines of defense organizational framework on information management within the three lines of defense to support internal audit, by performing a GAP analysis between the "as-is" situation and the "to-be" situation.

G4: Providing a migration plan for the process, people and technology aspects of the artifact that addresses how to "to-be" situation can be reached.

The formulated goals were operationalized in chapter eight. Based on this list of operationalized goals and the adoption of the action design science research methodology of figure 53 the research methodology of figure 54 was made. The operationalization of the design goals translated as follows:

1. Model the "as-is" situation: Creating a process model overview of the current situation of the three lines of defense.
2. Determine requirements for the "to-be" situation: Use literature and stakeholder knowledge to determine people, process and technology requirements for the "to-be" situation.
3. Model the "to-be" situation: Creating a process model overview of the "to-be" situation improving upon information management.
4. Perform a GAP analysis between "as-is" situation and the "to-be" situation to determine effectiveness of the framework in improving information management: Show off the added value of working with the framework.
5. Provide a migration plan to practitioners in order for them to implement the "to-be" situation in their companies.

DESIGN EVALUATION

In order to evaluate our designed artifact, composed of the "as-is" situation of the three lines of defense, the "to-be" situation of the three lines of defense and the migration plan we worked via several iterations in which an alpha, beta and final artifact was created. During the creation of the alpha version of the artifact several experts of the internal audit field from within Ernst & Young and clients of Ernst & Young were interviewed. In these interviews interviewees were also asked several questions concerning the constructs of the Technology Acceptance Model of Morris et al. [41] and if the models were correct according to their expertise. Interviewees were of course also questioned about expected information management improvements from the "to-be" model and migration plan. The beta version of the artifact was then re-evaluated in a discussion with three experts of Ernst & Young, using again the TAM framework [41] and information management aspects [37], [15] as well as redesign aspects in the questioning. The final artifact resulting the final discussion can be found in appendix L. The following findings resulted from the interviews and the discussion regarding the aspects of the TAM framework [41] and the information management aspects [37], [15]:

- Experts during the interviews and the discussion indicated that the topic of this paper is very relevant to the practice situation in the Dutch financial sector. As such all interviewees and discussion participants were very interested in the results and artifact of the paper.
- The discussion participants agreed that the design goals proposed in chapter seven and the research methodology derived from this were relevant and adequate to provide this paper with a structured approach.
- The discussion participants acknowledged that the literary topics used in this paper were relevant to the field and have been previously used by practitioners in several assignments. The mix of connections between the literary topics however and the focus on information management was rather new. Expert practitioners were very positive about this new approach.

- During the discussion of the beta version of the artifact experts indicated that the three models of the artifact were built logically and structurally and incorporated all the important aspects of the three lines of defense field.
- During the interviews and discussions experts pointed out that they expected the information management performance in the "to-be" situation to go up in comparison to the "as-is" situation. In addition to this the majority of experts believed that following the migration plan in a transition from the "as-is" to the "to-be" situation would maximize the information management performance of the "to-be" situation.
- During the interviews and the final discussion experts were tested positively on the aspects of the Technology Acceptance Model of Morris et al. [41]. Meaning that both client and internal expert practitioners of Erns & Young perceived the artifact of this paper to be useful, perceived the artifact to be relatively easily usable, were willing to work with the artifact and were also planning to do this in the near future.
- Interviewees and discussion participants were therefore also positive about the future potential of the artifact to be designed in terms of using it as a consultancy product within companies. For this purpose the artifact has to be tailored per company to apply to specific company needs.

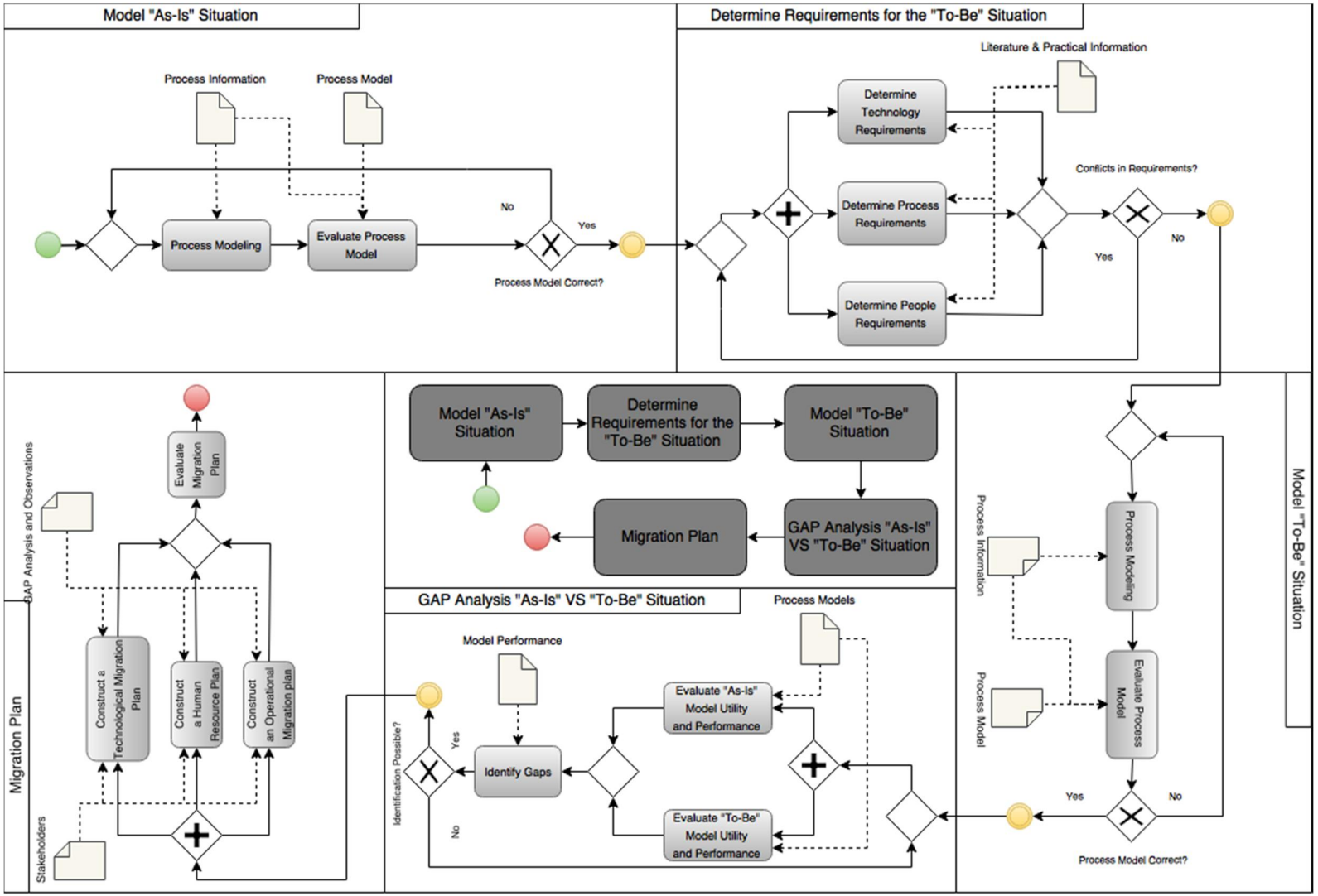


FIGURE 54. RESEARCH METHODOLOGY.

10.2. Limitations and Suggestions for Future Research

During this research several limitations were discovered, which will be discussed in this chapter. The limitations are of the following nature:

- Technical structure limitations within companies.
- Organizational structure limitations within companies.
- Qualitative approach used in this research.
- The generic nature of the artifact

The first limitation has to do with the technical structure of companies in the financial sector. The nature of our artifact is based heavily on information technology and as such the “to-be” situation and migration plan propose some big changes to the current technical structure of companies. Our paper uses a set of XES standard extensions as minimum requirements for event data capture in the “to-be” situation, but in literature [60], interviews and the discussion experts have already indicated that companies poses a lot of systems that are unable to log event data according to the requirements proposed in this paper. Many of those systems will be legacy systems and will most often be present in critical systems. It was indicated multiple times during the interviews that the cost and organizational extension of the XES minimum requirements will probably be hard to use. The vast amounts of data stored because of the “to-be” situation also means that companies will have to invest in the right infrastructure for this. More research into enabling event data capture in systems might solve some of these issues.

In addition to this the artifact of this paper proposes the development of event data-driven dashboards for all the three lines of defense, based on the controls used in the line. The focus for this is on the internal audit department because it will provide them with real-time data needed to develop internal audit objectives and perform internal audits. In practice however it might prove very hard to develop those event data-driven dashboard and not all companies might have the employees with the right skills to enable this. More research into developing event data-driven dashboards for internal audit purposes might solve some aspects of these problems.

From an organizational perspective the artifact also proposes some challenging changes. First of all the role of data analysis within the three lines of defense will increase in importance. Experts of clients of Ernst & Young indicated that at the moment not enough employees of their three lines of defense poses the right skills to do data or process analysis activities. Acquiring skilled employees will be hard for companies willing to implement the “to-be” situation. The “to-be” situation also proposes a whole new way of working for employees, which will take some time to take effect. Humans are often more inclined to work via the well-known previous way of working and fear change. Making sure the “to-be” model is followed will be challenging for companies.

Another limitation of this research is that validation and evaluation of the artifact has been done via interviews and a discussion. Preferably we would have implemented the “to-be” situation at a client company of Ernst & Young and monitored the information management performance during one audit year. This was however not possible within the limited time available for this master thesis. Therefore we propose that further research should be conducted in this area to strengthen the research results.

The last limitation resides in the fact that this research is generic of nature. This means that the artifact will not be one-on-one applicable on financial companies in the field without tailoring the artifact to the needs and the structure of a company. Form interviews and the discussion we derived that experts did believe that tailoring the artifact to match company need was not that hard and that the artifact represented a solid baseline, but for some companies tailoring the artifact will still be challenging. For this reason we have included this in the limitation list. Further research into tailoring a data-driven organizational framework to business needs so be conducted to solve this issue.

10.3. Contributions

CONTRIBUTIONS TO THEORY

The contribution to theory of this research paper lies in the in the fact that different theoretical concepts and domains have been connected with information management theory. This combination of theory has led to the development of a research and design methodology and the development of an artifact. The need for this specific combination of literary topics is further supported by several papers used in this thesis [3], [30], [59], [23]. The results of the interviews and the discussion has also given insight into the relevance of the combination of the literary topics used in this paper. Therefore we can argue that our paper accomplishes the expected theoretical relevance goals of section 3.5 of chapter three this paper:

- Extending theory about information management in the internal audit function.
- Extending theory and practical knowledge about the usage of event data files in internal audit control processes.

This research extends in this respect theory about how the data-driven internal audit function could look like from the perspective of the three lines of defense focusing on improving information management within the three lines of defense. It also extends theory about how event data and process mining could be incorporated in the three lines of defense to improve information management and support internal audit operations.

CONTRIBUTIONS TO PRACTICE

The contribution to practice is quite clear since the main focus of this paper is to develop an information management improving organization framework that supports data-driven internal audit operations. The artifact has been thoroughly tested within several companies in the financial sector, through means of expert interview and discussion. During the development of the artifact of this paper generalization of the artifact was of key importance. The paper's artifact was therefore based on the three lines of defense model of the IIA [27] and designed with generalized theoretical input to function with any form of company. Since the three lines of defense is widely used within and beyond the financial sector we can use Bayesian logic to say that similar results are expected at any company using the three lines of defense as a baseline for control mechanisms [50]. Our thesis therefore accomplishes the expected practice contribution as described in section 3.5 of chapter three:

- Providing Ernst & Young with a framework that helps them in their advisory role to organize information management within the three lines of defense of their clients.

During interviews and the discussion internal experts of Ernst & Young and external client experts further acknowledged this contribution to practice and pointed out that the artifact of this paper will most likely be used in future assignments involving the restructuring of the three lines of defense to ensure data-driven internal audit.

SOURCES

[1]. R. L. Ackoff, “From data to wisdom,” *J. Appl. Syst. Anal.*, vol. 16, no. 1, pp. 3–9, 1989.

[2]. V. Aebi, G. Sabato, and M. Schmid, “Risk management, corporate governance, and bank performance in the financial crisis,” *J. Bank. Financ.*, vol. 36, no. 12, pp. 3213–3226, 2012.

[3]. R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann, “Taming compliance with sarbanes-oxley internal controls using database technology,” *Proc. - Int. Conf. Data Eng.*, vol. 2006, no. i, p. 92, 2006.

[4]. J. H. Bernstein, “The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis,” *Nasko*, vol. 2, no. 1, pp. 68–75, 2009.

[5]. E. Brynjolfsson, L. M. Hitt, and H. H. Kim, “Strength in Numbers: How does data-driven decision-making affect firm performance?,” *ICIS 2011 Proc.*, p. 18, 2011.

[6]. B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness,” *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[7]. Committee of Sponsoring Organizations of the Treadway Commission, “Internal Control — Integrated Framework,” no. May, p. 10, 2013.

[8]. S. S. Conn, “OLTP and OLAP data integration: a review of feasible implementation methods and architectures for real time data analysis,” *Proceedings. IEEE SoutheastCon, 2005.*, no. May 2005, pp. 515–520, 2005.

[9]. Y. Demchenko *et al.*, “Security Architecture for Open Collaborative Environment,” *Lect. Notes Comput. Sci.*, vol. 3470, p. 589,599, 2005.

[10]. P. Dunleavy and H. Margetts, “The Second Wave of Digital Era Governance,” *Polit. Sci.*, pp. 1–32, 2010.

[11]. Ernst & Young LLP, “Take-aways from EY’s series of Internal Audit Analytics roundtables over 2016,” 2017.

[12]. Ernst & Young LLP, “Fighting to close the gap,” no. November, 2012.

[13]. Ernst & Young LLP, “ICT Integration Project - Target Operating Model,” 2014.

[14]. European Union, “The EU General Data Protection Regulation,” 2016. [Online]. Available: http://www.eugdpr.org/. [Accessed: 03-Feb-2017].

[15]. M. Evans, K. Dalkir, and C. Bidian, “A holistic view of the knowledge life cycle: The knowledge management cycle (KMC) model,” *Electron. J. Knowl. Manag.*, vol. 12, no. 2, pp. 148–160, 2014.

[16]. M. Fernández *et al.*, “Information Source Seleciton for Resource Constrained Environments,” in *SIGMOD*, 2005.

[17]. V. V Fomin, H. J. de Vries, and Y. Barlette, “ISO/IEC 27001 Information System Security Management Standard: Exploring the Reasons for Low Adoption,” in *EUROMOT 2008 Conference*, 2008.

[18]. Gerber and von Solms (2005), “Management of risk in the information age,” *Comput. Secur.*, vol. 24, no. 1, pp. 16–30, 2005.

[19]. G. Governatori and A. Rotolo, “Norm compliance in business process modeling,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6403 LNCS, no. 1, pp. 194–209, 2010.

[20]. D. Grigori, F. Casati, M. Castellanos, U. Dayal, M. Sayal, and M. C. Shan, “Business Process Intelligence,” *Comput. Ind.*, vol. 53, no. 3, pp. 321–343, 2004.

[21]. C. W. Günther and E. Verbeek, “Xes standard definition,” *Eindhoven Univ. Technol.*, pp. 0–24, 2014.

[22]. Q. Hu, T. Dinev, P. Hart, and D. Cooke, “Managing employee compliance with information security policies: The critical role of top management and organizational culture,” *Decis. Sci.*, vol. 43, no. 2012, pp. 615–660, 2012.

[23]. E. Humphreys, “Information security management standards: Compliance, governance and risk management,” *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 247–255, 2008.

[24]. Information Security Forum, “Aligning information risk management with operational risk management,” pp. 1–20, 2016.

[25]. Information System Audit and Control Association, “COBIT: A Business Framework for the Governance and Management of Enterprise IT,” pp. 1–94, 2013.

[26]. Institute of Internal Auditors, “Hot topics 10,” 2016.

[27]. Institute of Internal Auditors, “IIA Position Paper : The Three Lines of Defense in Effective Risk Management and Control,” no. January, 2013.

[28]. ISO, “ISO/IEC 27001:2013,” 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accessed: 09-Feb-2017].

[29]. A. A. Kalenkova, W. M. P. van der Aalst, I. A. Lomazova, and V. A. Rubin, “Process mining using BPMN: relating event logs and process models,” *Softw. Syst. Model.*, 2015.

[30]. J. Kolár, “Business activity monitoring,” *Masaryk Univ.*, no. February, p. 45, 2009.

[31]. N. Korac-Kakabadse and A. Kakabadse, “IS/IT governance: need for an integrated model,” *Corp. Gov. Int. J. Bus. Soc.*, vol. 1, no. 4, pp. 9–11, Dec. 2001.

[32]. W. Lam, “Investigating success factors in enterprise application integration : a case-driven analysis,” *Eur. J. Inf. Syst.*, no. March, pp. 175–187, 2005.

[33]. B. Laramee *et al.*, “Data information and knowledge in visualization,” *IEEE Comput. Graph. Appl.*, vol. 29, no. 1, pp. 12–19, 2009.

[34]. S. Lavalle, M. S. Hopkins, E. Lesser, R. Shockley, and N. Kruschwitz, “Analytics : The New Path to Value,” *MIT Sloan Manag. Rev.*, pp. 1–24, 2010.

[35]. Y. Levy and T. J. Ellis, “Towards a Framework of Literature Review Process in Support of Information Systems Research,” *Informing Sci.*, vol. 9, no. 8, pp. 171–181, 2006.

[36]. N. Li, Z. Bizri, and M. V. Tripunitara, “On mutually-exclusive roles and separation of duty,” *Proc. 11th ACM Conf. Comput. Commun. Secur. - CCS ’04*, vol. V, p. 42, 2004.

[37]. R. Maes, “An integrative perspective on information management,” *Inf. Manag. Setting Scene*, no. April, pp. 11–26, 2007.

[38]. A. McAfee and E. Brynjolfsson, “Big Data. The management revolution,” *Harv. Bus. Rev.*, vol. 90, no. 10, pp. 61–68, 2012.

[39]. J. S. Mcnally, “The 2013 COSO Framework & SOX Compliance: One Approach to an Effective Transition,” *Assoc. Accountants Financ. Prof. Bus.*, p. 9, 2013.

[40]. H. Mehran, A. Morrison, and J. Shapiro, “Corporate Governance and Banks: What Have We Learned from the Financial Crisis?,” *Fed. Reserv. Bank New-York (Staff Reports)*, no. 502, pp. 1–42, 2011.

[41]. M. G. Morris and A. Dillon, “How User Perceptions Influence Software Use,” no. August, 1997.

[42]. NRC, “Meer hypotheekadviseurs ABN vervalsten handtekenigen,” 2016. [Online]. Available: https://www.nrc.nl/nieuws/2016/11/25/meer-hypotheekadviseurs-abn-amro-vervalsten-handtekening-a1533620. [Accessed: 07-Mar-2017].

[43]. Object Management Group, “Object Management Group Business Process Model and Notation,” 2016. [Online]. Available: http://www.bpmn.org/. [Accessed: 08-Mar-2017].

[44]. D. Power and M. Terziovski, “Quality audit roles and skills: Perceptions of non-financial auditors and their clients,” *J. Oper. Manag.*, vol. 25, no. 1, pp. 126–147, 2007.

[45]. N. Racz, E. Weippl, and A. Seufert, “A frame of reference for research of integrated governance, risk and compliance (GRC),” *Commun. Multimed. Secur.*, pp. 106–117, 2010.

[46]. N. Racz, E. Weippl, and A. Seufert, “A process model for integrated IT governance , risk , and compliance management,” in *The Ninth Baltic Conference on Databases and Information Systems*, 2010, pp. 155–170.

[47]. H. A. Reijers and S. Liman Mansar, “Best practices in business process redesign: An overview and qualitative evaluation of successful redesign heuristics,” *Omega*, vol. 33, no. 4, pp. 283–306, 2005.

[48]. G. Ridley, J. Young, and P. Carroll, “COBIT and its utilization: a framework from the literature,” *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 0, no. C, pp. 1–8, 2004.

[49]. J. Ritchie, J. Lewis, C. M. N. Nicholls, and R. Ormston, *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* 2003.

[50]. P. B. Seddon and R. Scheepers, “Towards the improved treatment of generalization of knowledge claims in IS research: drawing general conclusions from samples,” *Eur. J. Inf. Syst.*, vol. 21, no. 1, pp. 6–21, 2012.

[51]. M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, “Action Design Research,” *MIS Q.*, vol. 35, no. 1, pp. 37–56, Dec. 2011.

[52]. R. Sheikhpour and N. Modiri, “An Approach to Map COBIT Processes to ISO / IEC 27001 Information Security Management Controls,” *Int. J. Secur. Its Appl.*, vol. 6, no. 2, pp. 13–28, 2012.

[53]. D. S. B. Soh and N. Martinov-Bennie, “The internal audit function. Perceptions of internal audit roles, effectiveness and evaluation,” *Manag. Audit. J.*, vol. 26, no. 7, pp. 605–622, 2011.

[54]. The Open Group, “ArchiMate® 3.0 Specification,” 2016. [Online]. Available: http://pubs.opengroup.org/architecture/archimate3-doc/chap06.html. [Accessed: 07-Apr-2017].

[55]. B. Tuttle and S. D. Vandervelde, “An empirical examination of CobiT as an internal control framework for information technology,” *Int. J. Account. Inf. Syst.*, vol. 8, no. 4, pp. 240–263, 2007.

[56]. Tweede Kamer der Staten-Generaal, “Kamerstuk 32643, nr2.,” 2011. [Online]. Available: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vimvkolc55vk. [Accessed: 07-Mar-2017].

[57]. W. M. P. Van der Aalst, A. K. Alves de Medeiros, and A. J. M. M. Weijters, “Genetic Process Mining,” in *ICATPN*, 2005, pp. 48–69..

[58]. W. M. P. van der Aalst, “Business process management: A personal view,” *Bus. Process Manag. J.*, vol. 10, pp. 135–139, 2004.

[59]. W. M. P. Van der Aalst *et al.*, “Process mining manifesto,” *Lect. Notes Bus. Inf. Process.*, vol. 99 LNBIP, no. PART 1, pp. 169–194, 2012.

[60]. B. F. Van Dongen and W. M. P. van der Aalst, “A Meta Model for Process Mining Data,” *Proc. 17th Int. Conf. Adv. Inf. Syst. Eng. (CAISE 2005)*, vol. 2, no. i, pp. 309–320, 2005.

[61]. P. Weill and J. W. Ross, “How Top Performers Manage IT Decisions Rights for Superior Results,” *IT Gov.*, no. Harvard Business School Press Boston, Massachusetts, pp. 1–10, 2004.

APPENDICES

Appendix A: List of Figures

Appendix B: List of Tables

Appendix C: Concept Matrix

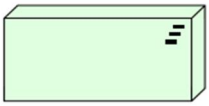
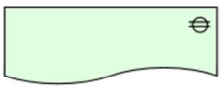
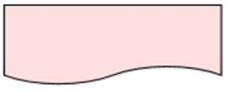
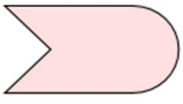
Table 5 provides an overview of the mapping of literature analyzed in the literature study on the concepts relevant to this paper.

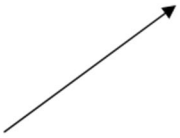
TABLE 5. CONCEPT MATRIX

Articles	Year	Data-Driven Company	Corporate/IT Governance	BRP/BPM/WFM	Internal Audit	Internal Controls	Data Quality	Data Availability	Big Data	Framework for Data-Driven Internal Control	OLTP/OLAP	Data Mining/Process Mining	Total
R. L. Ackoff	1989						X	X					2
V. Aebi, G. Sabato, and M. Schmid,	2012		X					X					2
R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann	2006	X	X	X	X	X					X	X	7
J. H. Bernstein,	2009						X	X					2
E. Brynjolfsson, L.M. Hitt & H.H. Kim	2011	X						X					2
B. Bulgurcu, H. Cavusoglu, and I. Benbasat	2010		X		X	X							3
Committee of Sponsoring Organizations of the Treadway Commission	2013		X		X	X							3
S. S. Conn	2005	X									X		2
Y. Demchenko *et al.*	2005				X	X							2
P. Dunleavy and H. Margetts	2010		X										1
Ernst & Young LLP	2012		X		X	X							3
M. Evans, K. Dalkir, and C. Bidian	2014						X						1
M. Fernández et al.	2005	X					X	X				X	4
V. V Fomin, H. J. de Vries, and Y. Barlette	2008		X		X	X	X	X					5
Gerber and von Solms	2005				X	X	X	X					4
G. Governatori and A. Rotolo	2010			X		X							2
D. Grigori, F. Casati, M. Castellanos, U. Dayal, M. Sayal, and M. C. Shan	2004	X	X	X			X		X				5
C. W. Günther and E. Verbeek	2014	X					X	X				X	4
Q. Hu, T. Dinev, P. Hart, and D. Cooke	2012				X	X							2
E. Humphreys	2008	X	X		X	X							4
Information Security Forum	2016		X		X	X							3
Information System Audit and Control Association	2013		X	X	X	X	X						5
Institute of Internal Auditors	2013		X		X	X							3
Institute of Internal Auditors	2016	X	X		X	X							4
A. A. Kalenkova, W. M. P. van der Aalst, I. A. Lomazova, and V. A. Rubin	2015	X		X			X	X				X	5
J. Kolár	2009			X			X	X				X	4
N. Korac-Kakabadse and A. Kakabadse	2001		X		X	X							3
B. Laramee et al.	2009	X					X	X				X	4
S. Lavalle e.a.	2010	X					X	X	X				4
N. Li, Z. Bizri, and M. V. Tripunitara	2004				X	X							2
R. Maes	2007	X					X	X					3
A. McAfee & E. Brynjolfsson	2012						X	X	X				3
J. S. Mcnally	2013		X		X	X							3
H. Mehran, A. Morrison & J. Shapiro	2011		X										1
D. Power and M. Terziovski	2007				X	X							2
N. Racz, E. Weippl, and A. Seufert (A Frame of Reference)	2010		X		X	X							3
N. Racz, E. Weippl, and A. Seufert (A Process Model)	2010		X	X	X	X							4
H. A. Reijers and S. Liman Mansar	2005	X	X	X		X	X	X					6
G. Ridley, J. Young, and P. Carroll	2004		X		X	X							3
R. Sheikhpour and N. Modiri	2012		X		X	X	X	X					5
D. S. B. Soh and N. Martinov-Bennie	2011				X	X							2
B. Tuttle & S.D. Vandervelde	2007					X							1
A. J. M. M. Van der Aalst, W.M.P, Alves de Medeiros, A.K., and Weijters	2005				X	X	X	X				X	5
W. M. P. van der Aalst	2004		X	X									2
W. Van der Aalst et al.	2012	X		X	X		X	X				X	6
B. F. Van Dongen and W. M. P. van der Aalst	2005	X		X			X	X				X	5
P. Weill and J. W. Ross	2004		X										1
	Total	15	22	11	24	26	19	17	3	0	2	9	152

Appendix D: BPMN 2.0 Notations & Archimate 3.0 Notations

Start Event	
End Event	
Intermediate Event: Event that takes place between start and end. In our model it indicates the end of a step in the methodological model (Figure 32)	
Activity	
Data Object: Indicates what data is needed in a task	
And-Split: Indicates that all sequential tasks have to be executed	
Or-Split: Indicaties that only one of the sequential tasks may be executed	
And/Or-split: Indicates that either one or both of the sequential tasks can be performed	
Join: Joins two seperate business process lines	
Business Process Flow	
Data Flow	

Stakeholder	
Driver: Stakeholder concerns	
Assessment: What is being observed	
Goal: Stakeholder desires	
Outcome: High level result that will be achieved.	
Principle: Abstract description of the intended properties of the artifact	
Requirement: Prescribes intended funcitonality	
Constraint: Constraints functionality	
Plateau: Represents a relative stable state of the architecture that exists during a limited period of time	
Gap: Represents the differences between plateaus	
Deliverable	
Work package: Actions identified and designed to achieve a specific outcome	
Implementation event: Denotes a state change related to an implementation or migration	

Association relation	
Composition relation	
Acces relation	
Realization relation	
Influence relation	
Triggering relation	

Appendix E: "As-Is" Situation Exploratory Interview

In order to model the current practical implementation of the three lines of defense model in businesses, called the "as-is" situation, we had to interview an expert of the practice. This exploratory interview was conducted according to the book *"Qualitative Research Practice: A Guide for Social Science Students and Researchers"* by Ritchie et al. [49]. As such it combines flexibility with structure. The interview will be interactive and the three lines of defense model will be used as a probe to achieve depth. In addition to this the six stages of a qualitative interview will be followed in the interview structure. As this interview is an exploratory interview the questions are designed to be content mapping. The goal of the interview can be summarized as follows:

Goal of the interview: Determine the practical implementation of the three lines of defense model in businesses in order to mode the "as-is" situation in BPMN 2.0.

One expert participated in this interview:

- Expert 1: EY internal expert. This expert will answer the questions from a market point of view. The expert has substantial expertise with both mature and immature clients in the financial sector on the subject of information management within the three lines of defense.

Interview Structure:

- Thanking the Interviewee for his/her time.
- Provide a short introduction about the topic of the research.
- Describe the three lines of defense model if needed.
- Questions:

Question 1: Can you describe how the first line of defense is practically implemented in businesses? (Operational – strategic alignment and business - IT alignment [37])

Question 2: Can you describe how the second line of defense is practically implemented in businesses? (Operational – strategic alignment and business - IT alignment [37])

Question 3: Can you describe how the third line of defense is practically implemented in businesses? (Operational – strategic alignment and business - IT alignment [37]).

Question 4: Can you describe the communication between the third line of defense and the first and second line? (Operational – strategic alignment and business - IT alignment [37]).

- Ending the Interview.
- Thanking the interviewee for his/her time.

RESULTS

Interview Expert 1:

Question 1: The first line of defense consists of the operational department that is actively involved in the business processes. They have to check their own departments work for errors via a control process that is followed. The controls used in this process are based on the controls that the risk department has identified. The input for the control process is the data that is being stored in the different business process of the company. This data can be transactional data and event data, depending on the systems the company uses and if those systems generate any event data.

Question 2: The second line of defense is the risk department. Dependent on the situation of the company (active in the United States or not) they have to accommodate to certain rules which define how tight the company manages their risk. Either way almost all companies work with the ideas of the COBIT literature. This means that the risk department is responsible for identifying risks and determining risk appetite based on the company's strategy. Based on the identified risks and the risks appetite some controls will be selected and implement. These controls will be monitored and their performance is reported to the senior management.

Question 3: The third line of defense is the internal audit department and functions separate from the first and second line of defense. The internal audit department receives a set of audit objectives from the top management every year. These audit objectives define which systems and business processes will be audited in that year. So the internal audit department does not recheck every system and business process of the company, but in theory if nothing has changed this should also not be necessary. Just like the second line of defense the internal audit department uses a control based approach to audit. This means that they will use the controls determined by the risk department and use them to check the relevant information systems. Information system data is requested from the responsible departments, which often leads to some problems:

- The data send is of bad quality.
- The necessary data is not available.

Auditing the IT is often possible but requires some time due to the fact that getting the right data from the systems is hard and time consuming. Auditing from a data perspective, meaning that business process instances are audited from initiation to completion by looking at the data transfers with data mining is not often done in all cases. Business often do not have the right information (event data) available to facilitate this.

Question 4: The internal audit department uses the same controls that are selected by the risk department and therefore asks for those controls before staring the audit processes. Data from the systems that are being audited are requested at the responsible operational departments.

Appendix F: "As-Is" Model Validation Interview

In order to start building upon the "as-is" situation towards a "to-be" situation we will have to know if our model as shown in figure 34 is correct. In order to validate this several experts will be asked to provide feedback on the model. This validation interview was conducted according to the book *"Qualitative Research Practice: A Guide for Social Science Students and Researchers"* by Ritchie et al. [49]. As such it combines flexibility with structure. The interview will be interactive and the "as-is" model will be used as a probe to achieve depth. In addition to this the six stages of a qualitative interview will be followed in the interview structure. As this interview is a validation interview the questions are designed to be content mining. The goal of the interview is as follows:

Goal of the interview: Validate that the "as-is" situation as modeled in figure 34 represents the reality of the three lines of defense in practice.

Two experts participated in this interview:

- Expert 1: EY internal expert. This expert will answer the questions from a market point of view. The expert has substantial expertise with both mature and immature clients in the financial sector on the subject of information management within the three lines of defense.
- Expert 2: Client expert of an immature company on the subject of information management within the three lines of defense. The company of this expert is situated at the "as-is" situation described in this paper.

Interview structure:

- Thanking the Interviewee for his/her time.
- Provide a short introduction about the topic of the research.
- Show and explain the "as-is" situation model to the experts and explain how the process flows work if needed.
- Questions:

Question 1: Does the model explain the function of the first line of defense well? Explain.

Question 2: Does the model explain the function of the second line of defense well? Explain.

Question 3: Does the model explain the function of the third line of defense well? Explain

Question 4: Does the model explain the function of the senior management well? Explain.

Question 5: Does the model explain the function of the top management well? Explain.

Question 6: Is de sharing of data and other information between the different defense lines and management lines represented well in the model? Explain.

- Ending the Interview.
- Thanking the interviewee for his/her time.

RESULTS

Interview Expert 1:

Question 1: First line of defense is explained well. Operational department does however not get all of its controls from the risk department. Sometimes they work ad-hoc when controlling a process by establishing their own controls.

Question 2: Risks department establishes controls which are not used by the internal audit department. They use their own set of controls. The process in the risk department is correct.

Question 3: It is not the case that top management designs audit objectives for the internal audit department. In practice the internal audit department will construct a report with audit objectives and will present this to the top management, who will approve this or not. The action perform audits should be split in financial, operational and IT audit. Furthermore there is a division between compliance audit and normal audit. The first only looks at regulations while the second also takes business performance into account.

Question 4: Senior management function is correct, when only looking at it from an audit perspective.

Question 5: Top management function is correct, when you remove the action design audit objectives and add an action that is called approve audit plan, which is linked to the internal audit department.

Question 6: The risk department might also look at some transactional data when establishing risks and controls. Internal audit department does not receive audit objectives but instead sends their audit objectives for approval to the top management. The operational department uses their own controls next to the controls of the risk department.

Interview Expert 2:

Question 1: First line of defense is explained well. I think the activity “Establish list of controls” is situational. At our company the first line of defense only implements and monitors controls established by the second line of defense.

Question 2: The process of the risk department is very much COBIT focused. COBIT focuses only at IT risks and controls and therefore you should make sure that the process also supports COSO activities.

Question 3: Top management does not design audit objectives for the internal audit department. The internal audit department designs audit objectives based on findings that the first and second line have reported and based on key processes within the company. Splitting up the audit function in financial, operational and IT audit activities clarifies the differences.

Question 4: The function of the senior management within the three lines of defense is correct.

Question 5: Within the top management process the management should only approve or decline internal audit objectives and not design the objectives themselves. The other processes activities are correct in this context.

Question 6: The internal audit department looks at findings from both the first and second line of defense when designing audit objectives. Audit objectives are not received from the top management.

Appendix G: "As-Is" Model Utility and Information Management Performance Interview

In order to identify the gaps between the "as-is" situation and the "to-be" situation we will have to identify the utility and information management performance of the "as-is" situation. Because of time constraints imposed on this research, we choose to do identify this performance via expert interviews. This utility and information management performance interview was conducted according to the book "*Qualitative Research Practice: A Guide for Social Science Students and Researchers"* by Ritchie et al. [49]. As such it combines flexibility with structure. The interview will be interactive and the "as-is" model as well as the three lines of defense model will be used as a probe to achieve depth. In addition to this the six stages of a qualitative interview will be followed in the interview structure. As this interview is a utility performance interview the questions are designed to be content mining. In the development of the questions the constructs of the TAM framework of the paper "*How User Perceptions Influence Software Use"* by Morris et al. [41] are used. The goal of the interview is as follows:

Goal of the interview: Determine the utility and information management performance of the current internal audit function and identify activities in which problems arise.

Two experts participated in this interview. For this interview the same experts as the interview of appendix H are questioned:

- Expert 1: EY internal expert. This expert will answer the questions from a market point of view. The expert has substantial expertise with both mature and immature clients in the financial sector on the subject of information management within the three lines of defense.
- Expert 2: Client expert of an immature company on the subject of information management within the three lines of defense. The company of this expert is situated at the "as-is" situation described in this paper.

Interview Structure:

- Thanking the interviewee for his/her time.
- Provide a short introduction into the topic of the paper.
- Explain the three lines of defense model, which is used in this paper as a baseline.
- Provide the expert with the "as-is" model as described in figure 35.
- Questions:

Information Management Questions:

Question 1: The idea behind the three lines of defense is that they operate independently from each other. Findings of the first and second line of defense might however be interesting for the third line of defense. How is information sharing between the lines organized at the moment and does this often result in data shortages? (Operational – strategic alignment and business - IT alignment, data to information transition [37], [15]. Perceived ease of use [41]).

Question 2: When performing internal audits, how often do information shortages occur and do they influence the overall assurance result? Explain. (Business – IT alignment, data to information transition [37], [15]. Perceived ease of use [41]).

Question 3: Do you believe that information sharing within the organization of the three lines of defense could be improved? Explain. (Operational – strategic alignment, data to information transition [37], [15]. Attitude towards using "to-be" situation [41]).

Event Data Questions:

Question 4: Does your company capture log files and are they conform the requirements proposed in this paper? Explain. (Business – IT alignment, data capture basics [37]).

Question 5: How is the event data used during the internal audit activities? (Business – IT alignment, data to information transition [37], [15]. Perceived ease of use [41]).

Process Questions

Question 6: The internal audit department determines annual internal audit objectives. Do you believe that the selection of those objectives could be improved if the internal audit department had real-time insight into the findings of the first and second line of defense? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge transition [37], [15]. Perceived ease of use, perceived usefulness, attitude towards using and behavioral intention towards using [41]).

Question 7: Can you point out in which activities of the model the most problems arise in practice? Explain. (Business – IT alignment [37]. Perceived ease of use [41]).

Question 8: Do you think that internal audit departments could benefit from a framework that dictates the capture of data in the organizational processes and shares this data real-time? (Operational – strategic alignment and business - IT alignment, data to information to knowledge transition [37], [15]. Perceived ease of use, perceived usefulness, attitude towards using and behavioral intention towards using [41]).

- Ending the interview.
- Thanking the interviewee for his/her time.

RESULTS

Interview Expert 2:

Question 1: The third line of defense looks into the reports of the first and second line of defense. Interesting findings will be retrieved this way. In addition to this a ticket system is used in which risks to the company will be reported by the second line of defense. The tickets will have to be resolved by the first line of defense and closed after a resolution has been found. These tickets can provide us with additional information for establishing audit objectives. Double checking if these tickets are solved well enough by the first line of defense can be vital in critical systems.

Question 2: At the moment there are no real problems, since we do not really audit from a data perspective. We know that not enough data is stored by our systems at the moment and that the data that is stored is of poor quality, so we do not perform any data or process analysis activities.

Question 3: The reports and the ticket systems do not provide us with real time information. Real time information would give us a better insight into current issues and will maybe even help us predict some arising issues.

Question 4: Some systems might capture log files but their log files are probably not as rich as they should be according to the XES standard minimum extension requirements proposed in this paper.

Question 5: Event data is not used real-time. Sometimes a dataset of a specific time period is used for some analysis activities, but this is all historic data.

Question 6: Yes, real-time insight into the dashboards of the first and second line of defense will improve our internal audit objectives because we have more up to date information available to us.

Question 7: Overall the processes of both the second and third line of defense are subject to information latency. The main problems that arise at the operational level is that controls that the operational department implement may or may not mitigate the risks identified by the risk department. Because the second and third line of defense use the reports written by the first line of defense and sometimes historic data from the systems of the company there will always be latency in the processes of the second and third line.

Question 8: Yes, this will improve the performance of the three lines of defense and certainly within the third line of defense this will make a difference. It will take a lot of time however to enable event data capture in all the relevant systems. The XES standard requires fairly much in terms of standard extension and this will take time to implement. Furthermore our company does not possess the employees with data analysis skills and process mining skills. Training and acquisition of employees will also take time.

Interview Expert 1:

Question 1: I am not quite sure how my clients organized the information sharing between the three lines of defense at the moment. What I do know is that most of them do not use any form of tooling to track findings and the subsequent actions needed for these findings. Almost all of the information that is being shared is done via the reports that are send to senior management. This does of course mean that there will be some information latency between the three lines of defense.

Question 2: They do occur. I do not know how often. Mostly these information shortages are “solved” by means of interviews with the practitioners to find out what has happened during their working processes.

Question 3: Yes I do think that it could be improved. Certainly between the second and third line of defense there occur some problems when for example the second line of defense does not want to report some findings and the third line of defense has to find these findings again by themselves.

Question 4: No. Most companies do not actively capture event data. Event data that is available is not conform any standards.

Question 5: During internal audits event data is not often used. One of the reasons behind this is that it is not qualitatively available.

Question 6: Yes, the internal audit objectives could be improved if there was more accurate and up-to-date information available to the third line of defense. So real-time insight into the findings of the first and second line of defense will improve the process of determining internal audit objectives.

Question 7: Most problems arise in the communication between second and third line of defense. So not really in any of the activities but more in the information sharing. Sometimes the second line of defense does not want to share some findings because of strategic reasons for the company they work for.

Question 8: Yes dictating the capture of event data makes sure that people can expect some sort of quality from even data that is being captured. Real-time insight will improve the accuracy of the internal audit processes.

Appendix H: "To-Be" Model Utility and Information Management Performance Interview

In order to identify the gaps between the "as-is" situation and the "to-be" situation we will have to identify the Utility and information management performance of the "to-be" situation. Because of time constraints we choose to do identify this performance via expert interviews. This utility and information management interview was conducted according to the book "*Qualitative Research Practice: A Guide for Social Science Students and Researchers"* by Ritchie et al. [49]. As such it combines flexibility with structure, the interview will be interactive and the "to-be" model as well as the three lines of defense model will be used as a probe to achieve depth. In addition to this the six stages of a qualitative interview will be followed in the interview structure. As this interview is a utility performance interview the questions are designed to be content mining. In the development of the questions the constructs of the TAM framework of the paper "*How User Perceptions Influence Software Use"* by Morris et al. are used [41]. The goal of the interview is as follows:

Goal of the interview: Determine if the "to-be" model would improve the internal audit function utility and performance.

Two experts participated in this interview. For this interview the same experts as the interview of appendix G are used:

- Expert 1: EY internal expert. This expert will answer the questions from a market point of view. The expert has substantial expertise with both mature and immature clients in the financial sector on the subject of information management within the three lines of defense.
- Expert 2: Client expert of an immature company on the subject of information management within the three lines of defense. The company of this expert is situated at the "as-is" situation described in this paper.

Interview Structure:

- Thanking the interviewee for his/her time.
- Provide a short introduction into the topic of the paper.
- Explain the three lines of defense model, which is used in this paper as a baseline.
- Provide the expert with the "to-be" model as described in figure 41.
- Questions:

Process Questions:

Question 1: As shown in the "to-be" model dashboards are developed and maintained by the IT department. One of the reasons for this is to ensure that the first, second and third line of defense remain separate lines of defense. What do you think of this approach? (Operational – strategic alignment and business - IT alignment [37]. Attitude towards using [41]).

Question 2: In the "to be" model the internal audit department has insight into the dashboards of both the risk and operational departments when establishing annual internal audit objectives. Do you think that this will improve the quality of the internal audit objectives? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge transition [37], [15]. Attitude towards using, behavioral intention to use and perceived usefulness [41]).

Question 3: Do you think that using event data for internal audit processes will increase accuracy of the internal audit processes and will save time of doing the internal audit processes? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge transition [37], [15]. Attitude towards using, behavioral intention to use and perceived usefulness [41]).

Question 4: Do you think that the dashboards based on event data of the processes within your company and your departments controls will make your job easier to perform? Explain. (Business - IT alignment, data to information to knowledge transition [37], [15]. Attitude towards using and perceived ease of use [41]).

People Questions:

Question 5: Creating and maintaining event data driven dashboards will require sufficient expertise from the IT department. Do you believe that your company is able to provide this expertise or is additional training required? Explain. (Business - IT alignment [37]. Attitude towards using and perceived ease of use [41]).

Question 6: Working with event data driven dashboards will require sufficient insight from the three lines of defense on the functioning of the dashboards. Do you think that additional training will be prerequisite to working with dashboards in the three lines of defense? Explain. (Business - IT alignment [37]. Attitude towards using and perceived ease of use [41]).

Technological Questions:

Question 7: Using event data within the three lines of defense requires the company to follow a specific standard. The most recent standard used by the IEEE is the XES standard. Do you believe that the different systems within the company can support the event data requirements proposed by this standard? Explain. (Business - IT alignment [37]. Perceived ease of use [41]).

Question 8: For the purpose of keeping up with modern day technology and processes, do you believe that your company's leadership is willing to invest into enabling processes mining in your company? Explain. (Operational – strategic alignment [37]. Attitude towards using [41]).

Question 9: Sophisticated analysis algorithms can eventually allow for automated process control mechanisms and automated process control reporting. Do you believe this to be useful and vital to the continuity of your company? Explain. (Operational – strategic alignment and Business - IT alignment, data to information transition [37], [15]. Perceived ease of use and Perceived usefulness [41]).

- Ending the interview.
- Thanking the interviewee for his/her time.

RESULTS

Interview Expert 2:

Question 1: I think that it is smart to allocate development and maintenance of the dashboard to the IT department. Keeping the separation between the three lines is one of the factors in this, but I do also think that the three lines at many companies do not have the employees with the skills to construct the dashboards themselves.

Question 2: In comparison to the ticket system used currently this will provide real-time insight into several performance aspects. The design of the dashboards does however dictate much of the usefulness when another department wants to use the dashboard of a different department. When designing the dashboard the information needs of the other lines must be taken into account which will be complicated.

Question 3: I think that it will increase the accuracy of the audit processes and will provide additional operational assurance to our current way of working. When we are ready to start using more process data in our audit processes these dashboards will definitely save us time. These dashboards can also analyze some basic controls automatically, which will also improve assurance.

Question 4: I think that my job will not be easier to perform, as data analysis and process mining also complicate my job. I do however think that process mining is inevitable for our company and these dashboards will certainly help increasing the ease of use.

Question 5: I do believe that training in the subject is still required within the company. It might even require us to hire some new employees with the right skills.

Question 6: Our employees do not have sufficient expertise in process mining and data analysis techniques at this moment in time. Additional training is required to uplift the expertise level in these subjects. Additional employees with the right skills might also be needed.

Question 7: I am unsure about this, but I do not think that all our systems are able to log as substantially as required by the minimal extension requirements of the XES framework.

Question 8: At this moment in time they are already investing in enabling data-driven control processes, so yeah the top management is willing to invest in these things to a certain extend of course.

Question 9: Enabling computerized control processes will enable us to analyze far more data than we can currently analyze. As the whole sector will be moving towards a more computerized approach we will have to keep up.

Interview Expert 1:

Question 1: It is a good approach, but the name IT department is confusing because this can also be a subdivision of any of the three lines of defense of all of them. You should specify this further in the text.

Question 2: Yes, insight into the dashboards of the first and second line of defense will increase will improve the establishment of the annual internal audit objectives.

Question 3: I do not think it will reduce the time needed to do the tasks, but I do think it will increase the accuracy of the internal audit processes.

Question 4: I do not think it will make the job easier to perform. It will also not make the job harder to do necessarily if employees get the right training for the job.

Question 5: I think most companies in the financial sector have highly skilled IT department employees. So I doubt they will need any training to perform these new tasks of creating and maintaining event data-driven dashboards.

Question 6: I think that people in within the three lines of defense of companies do not have the required data and process mining skills to perform the new activities right away. Training is needed to implement it, or employees with the rights skills should be attracted.

Question 7: I think that most of the requirements are possible at clients of EY. Only the cost and organizational extension may prove to be complicated to implement. Mostly because the costs associated to the activities are often not clear within the companies themselves.

Question 8: I think the leadership of EY's clients is mostly not eager to invest a lot of money in these capabilities even though this is probably smart to do. Budget is always an issue in these cases.

Question 9: I believe that this is very useful yes since it will reduce the need for employees on these jobs and so also the cost of hiring employees for these tasks. I do not know if it is vital for business continuity.

Appendix I: Migration Plan Evaluation Interview

In order to identify if the proposed migration plan model of this paper is perceived to be useful by experts in managing a transition from the "as-is" situation to the "to-be" situation and if the migration plan model will help experts maximize the "to-be" process performance we will conduct several expert interviews. This utility interview was conducted according to the book "*Qualitative Research Practice: A Guide for Social Science Students and Researchers"* by Ritchie et al. [49]. As such it combines flexibility with structure. The interview will be interactive and the "as-is" model, the "to-be" model as well as the migration plan model will be used as a probe to achieve depth. In addition to this the six stages of a qualitative interview will be followed in the interview structure. As this interview is a utility performance interview the questions are designed to be content mining. In the development of the questions the constructs of the TAM framework of the paper "*How User Perceptions Influence Software Use"* by Morris et al. are used [41]. The goal of the interview is as follows:

Goal of the interview: Determine if the migration plan model will help experts maximize the "to-be" process information management performance and is perceived usable to manage the transition process from the "as-is" situation to the "to-be" situation.

Three experts participated in this interview:

- Expert 1: EY internal expert. This expert will answer the questions from a market point of view. The expert has substantial expertise with both mature and immature clients in the financial sector on the subject of information management within the three lines of defense.
- Expert 2: Client expert of an immature company on the subject of information management within the three lines of defense. The company of this expert is situated at the "as-is" situation described in this paper.
- Expert 3: Client expert of a slightly more mature company on the subject of information management within the three lines of defense. The company of this expert has started with data analysis activities and therefore already poses some more knowledge about this subject.

Interview Structure:

- Thanking the interviewee for his/her time.
- Provide a short introduction into the topic of the paper.
- Explain the three lines of defense model, which is used in this paper as a baseline.
- Provide the expert with the "as-is" model as described in figure 35.
- Provide the expert with the "to-be" model as described in figure 41.
- Provide the expert with the migration plan model as described in figure 44.
- Questions:

Process Questions:

Question 1: The migration model and "as-is" model are based on a situation in which no systematical data analysis and process analysis activities are performed. Some companies are already busy with the transition towards a more data-driven audit approach. Can you indicate in which plateau of the migration model your company is at the moment? Explain. (Operational – strategic alignment and business - IT alignment [37]. Attitude towards using [41]).

Question 2: In the migration model we argue that the transition will have three steps, being: Developing a strategic plan, developing the technical infrastructure and developing the organizational infrastructure. Do you believe that this approach is correct and do you believe these steps are in the right order? Explain. (Operational – strategic alignment and Business - IT alignment [37]. Attitude towards using, behavioral intention to use and perceived usefulness [41]).

Question 3: In the migration model we argue that halfway through the process employees of the three lines of defense should start with data analysis tasks in order to provide feedback on the implementation and provide practical training for the employees. Do you believe this to be a useful early adoption choice or do you believe that this approach will be complicated due to the nature of event data capture implementation in the previous step? Explain. (Operational – strategic alignment and Business - IT alignment [37]. Perceived usefulness [41]).

Question 4: During the transition the migration model prescribes some deliverables to the different steps. Are there any deliverables missing or do you think that some deliverables are wrong? Explain. (Operational – strategic alignment and business - IT alignment [37]. Attitude toward using, behavioral intention to use [41]).

Question 5: Do you think that the migration model misses some steps to make the transition from the "as-is" situation to the "to-be" situation or is it complete? Explain. (Operational – strategic alignment and business - IT alignment [37]. Attitude toward using, perceived ease of use [41]).

Question 6: The goal of the migration plan is that it is able to guide a transition from the "as-is" situation to the "to-be" situation. Can you provide any feedback on the completeness of the model from your point of view? If you believe it to be incomplete can you indicate what is missing? Explain. (Operational – strategic alignment [37]. Attitude toward using, behavioral intention to use [41]).

Question 7: Do you believe the migration model to be practically useful for experts to organize a migration from the "as-is" to the "to-be" situation? Explain. (Operational – strategic alignment [37]. Perceived usefulness [41]).

Question 8: Do you believe that the performance of the "to-be" model will be increased when this migration model is followed, or do you think the transition time towards the "to-be" model will be decreased a lot? Explain. (Business – IT alignment [37]. Perceived usefulness [41]).

People Questions:

Question 9: In the migration model three training activities are proposed. Do you believe that those training activities are of vital importance to the success of the migration or do you believe that your IT department and three lines of defense departments do not need substantial training to be able to work with data a process mining technologies? Explain. (Operational – strategic alignment [37]. Perceived usefulness [41]).

Question 10: As can be seen in the migration model the initiation requires a letter of commitment deliverable, which represents the commitment of the stakeholders and top management to the transition. Commitment is one of the key critical success factors for the success of the project. Do you believe it will be hard to commit the top management and stakeholders to the project? Explain. (Operational – strategic alignment [37]. Attitude toward using, behavioral intention to use [41]).

Technological Questions:

Question 11: The migration plan model is based on the minimum XES event data capture requirements proposed in this paper. How likely do you is it that your company will be able to capture event data in all its critical systems according to the requirements? (Business – IT alignment [37]. Perceived ease of use [41]).

Question 12: The migration model proposes that key processes and systems should be addressed first in the migration to ensure the audit quality of these key processes. Do you agree with this approach or would you start with the less critical processes and systems? If you do agree, does your company already poses a list of key processes and systems? Explain. (Operational – strategic alignment [37]. Attitude toward using, behavioral intention to use [41]).

Question 13: One of the aspects of the technical architectural plan deliverable in the strategic planning step of the migration plan is that experts should determine an event data capture plan based on their own companies information systems environment. The paper proposes this plan with the aim on smoothening the transition for some complicated systems that might be around in any company. What do you think of this approach? (Business – IT alignment [37]. Perceived ease of use, perceived usefulness [41]).

- Ending the interview.
- Thanking the interviewee for his/her time.

RESULTS

Interview Expert 1:

Question 1: Most companies are still at the “as-is” situation. Some companies will already have the strategic planning plateau done and will have made some progress into the technological infrastructure plateau. There will also be some organization that have started with implementing some of the technical infrastructure plateau, without properly doing the strategic planning plateau beforehand. None of the companies in the financial sector will have developed further than that.

Question 2: I do think this approach is correct. I do not believe that you have forgotten important plateaus or gaps between the “as-is” and the “to-be” situation. The order of the plateaus is self-explanatory since it is unwise to start with the technical infrastructure plateau before the strategic plan plateau is finished. The organizational infrastructure plateau cannot logically be switched with the other plateaus.

Question 3: Yes I think this is important to do. The implementation of the data capture in all the systems will probably take a long time. It is important that employees gain experience with data analysis tasks in the meantime and also provide feedback on the implementation and indirectly on the deliverables of the strategic planning plateau.

Question 4: In the model I miss a deliverable where certain policies are written up regarding the data mining process and the process mining process. In addition to this I miss a deliverable where tooling strategies and tools for enabling event data capture, data mining and process mining are selected.

Question 5: I think the plateaus on the top level and the gaps between the plateaus are explained well and I do not think any extra plateaus should be identified. As earlier said I do miss some deliverables for some of the plateaus. Naturally this will also imply that some extra actions on the bottom layer will have to be identified. I also miss feedback loops in the model as it is very linear at the moment, but this will not be the case during actual implementation. I do not know if modeling feedback loops is allowed in Archimate 3.0 however.

Question 6: I think the model, with addition of my comments, will provide a very good baseline of the implementation from the “as-is” model to the “to-be” situation. I even think the model is already slightly complicated so adding more to it will not improve the readability for practitioners.

Question 7: I do believe that this model provides a rather easy overview of all the steps that have to be taken in order to go from the “as-is” situation to the “to-be” situation. Certainly the deliverables provide a good indication of what needs to be done in order for an organization to arrive at the final “to-be” situation.

Question 8: I do not think the performance of the “to-be” situation can be improved using this migration model. Following the steps systematically will probably decrease the implementation time however and will probably cause the “to-be” situation to be utilized sooner. Transition time does however depend a lot on the company architecture itself.

Question 9: I do not think that many companies have sufficient employees with the right skills to either capture event data from business process systems or to systematically include data and process analysis into the internal audit function. So I do think that organizations should acquire new employees with the right skills and/or should train their current employees in these skills.

Question 10: Top management is always hard to commit to projects that will potentially cost a lot of money. Stakeholders will be easier to commit to the project if they are trained well and are involved in the project throughout the whole project timespan. I think it is good that you display this commitment from the start of your migration model since it will probably determine much of the success of such a project.

Question 11: This will probably not be easily doable in most company’s right from the start and will probably take a long time to complete. It does depend a lot on what a company is logging already at the moment of initiation of the project.

Question 12: I think this is a consideration of the company and is mainly dependent on how certain they are in the success of the project. The advantage of implementing critical process systems first is that you can start with data analysis on these processes sooner and really experience the benefits of it. Choosing to implement less critical systems first ensures business continuity.

Question 13: I think this is the right approach since this has to be done anyway. A company can better do this in the planning stage then do it when implementation has already begun. This will also make sure that the same standards will be upheld throughout the whole transition.

Interview Expert 2:

Question 1: We are at the moment very much at the "as-is" situation. We have arranged a data discovery team that is starting up the process of making a strategic plan for future data analysis implementations. More than that we currently do not have in this company.

Question 2: I do believe this is a correct approach. I think the three steps provide a good and conclusive overview of the things that have to be done. The content of the steps themselves is more important I think.

Question 3: I do think that it is a good approach, but only given that the right data analysis employees are providing the feedback. Employees which do not yet poses the right skillset will need to obtain this skillset first before providing feedback to the data capture implementation team. The reason for this being that wrong feedback can and will probably delay the implementation process, which is probably already costly on its own.

Question 4: I think that is useful to include a business case in the deliverables in which the three lines of defense describe the added value of the "to-be" situation to the business. This business case can also provide an overview of the data need of the three different lines of defense.

Question 5: I do think that the migration model is for its purpose complete. For an actual transition to a "to-be" situation within a company the steps and deliverables will have to be made more specific. This will however differ per company and therefore I think the generic version serves its purpose as a baseline.

Question 6: I think the model can serve as a baseline for a transition and in that respect it is complete. If a company is going to use it the experts of the company will have to design roles and a project structure around the model. This structure and the employee roles in the structure will however be company dependent and is therefore hard to put in your generalized model.

Question 7: It is practically useful as baseline on which experts performing a transition can base their company specific version.

Question 8: I do think that following the same standards and strategy companywide during a transition will eventually lead to a better working "to-be" situation yes. It will certainly create clarity for the project team and will provide data clarity for the employees of the three lines of defense.

Question 9: I think that the IT department, or a similar responsible department, will have the right skills for this job. Training them if needed is however never a bad idea. Training the employees of the three lines of defense is more necessary. I do even think that we will have to hire employees with these skills, since I doubt that we will have enough data analysts in the company when a transition to the "to-be" model can be realized.

Question 10: This is one of the most critical aspects of the migration model I think. Committing all stakeholders and the top management to a project like this will be very hard to do. The reason I proposed a business case deliverable is because it can help with creating this commitment.

Question 11: I think it will be unlikely that we will be able to implement these requirements companywide in the systems. There are multiple factors important to this. Much of the systems are not custom made and will require us to contact the supplier. They will or will not be able to implement this based on the system configurations and based on

the cost of doing the implementation. Much of the legacy systems will not be able to be configured like this. These requirements should be taken into account when buying new systems however.

Question 12: Piloting in a process that already captures most of the required data will be helpful I think. After that it is certainly smart to start with the critical systems and business processes. I do think that prior to this a risk analysis should be done but the implementation will first be done in the test environment, so I do not see much risks for business continuity.

Question 13: I do think this is a good approach. This will certainly smoothen up the implementation and will also provide an overview of complicated systems and business processes.

Interview Expert 3:

Question 1: Within our company we have already started experimenting with data analysis. We have recently purchased a tool for this but at the moment we are still doing much of the work in Excel. I would say that we started in the “technical architecture in place” plateau without actually doing the strategic planning plateau.

Question 2: Yes, I do think this is a good approach and a logical one. I do not specifically identify a step that you have missed in this approach and I do also think that the order of the steps should remain the same. The order can also not really change since they rely heavily on each other. We however started migrating without developing a strategic plan, but I realize now that this will lead to complications further down the road.

Question 3: I believe this to be an excellent approach since the data capture implementation supports the training of employees and the training provides feedback to the implementing IT experts. I do however not think that training via this approach will be substantial enough. Training via taught courses into data analysis will also have to be provided to the employees of the three lines of defense. I am missing the feedback loop in the Archimate model for this mutual beneficiary proposal.

Question 4: I think the current deliverables are sufficient, but high level. For practical usage the deliverables will have to be further defined on a company level.

Question 5: I think the migration plan model is an excellent baseline to manage a transition towards a more data-driven “to-be” model. The model is however constructed on such a generalized level that a practical company specific version of the model should be included.

Question 6: I think the model is very complete and certainly usable to guide a transition from the “as-is” situation to the “to-be” situation. The only thing missing are feedback loops in the lowest level of the model. At this moment the model is a linear process, but in practice there will be feedback loops needed to complete the process.

Question 7: Yes, I do believe that the model can be of practical use for experts organizing a migration to the “to-be” situation. Mainly because it provides a generic, but complete, baseline of deliverables and actions to be taken in order to complete the transition. Experts of different companies can use this model to make a company specific approach that fits their organization.

Question 8: I do think that following a project wide generalized approach will lead to better performance of the “to-be” situation, since experts will treat all systems and business processes the same during the transition according to the strategy developed in the first transition step. As a result of this almost all systems will provide the same types of data, which will make the job for internal auditors easier and will increase “to-be” model performance.

Question 9: It depends a lot on the background of the employee. I for example have an IT background and will require less training in data analysis and process mining to be able to use it for audit purposes. Other employees with non-IT backgrounds might require more substantial training. Since the “to-be” situation relies heavily on analysis capabilities. I do think it is vital for the success of a transition to train all the employees of the three lines of defense to the same level of skill. I do not think that IT employees need training in enabling event data capture, since I think this is basic knowledge for them.

Question 10: At the moment we are trying encourage the usage of analytics in the company via a bottom-up approach. The reason for this is because at the moment there is limited top management commitment to implement a “to-be” situation in our company. Mainly because it will cost a lot of money and will take a lot of time to implement the “to-be” situation companywide. However if you want to implement the “to-be” situation companywide as proposed by your paper, you will have to do this from a top-down approach, which means you will definitely have to have all stakeholders, including the top management, on board. Getting their commitment will be hard though.

Question 11: I think it will be relatively easy to implement data capture according to most of the XES requirements proposed in your paper. The cost extension will be too hard to implement for us at this moment. Mainly because this will also require us to store this type of data about the processes, which is not being done at the moment.

Question 12: We already have a list of key processes available and we know what actions are taken during those key processes and what data is being stored. I do agree that you would want to start the project by enabling event data capture in the key processes first, but I would propose to do an implementation trial on one process first before I would take the other processes.

Question 13: Yes, I do think this is of vital importance. Preparing such a plan will make sure you know about the harder to implement systems beforehand and will make sure you encounter less unexpected problems during the project. It will probably also help you to better understand the costs of the project.

Appendix K: Artifact Beta Version Validation Discussion

In order to identify if the proposed beta version of the artifact of this paper, composed of the "as-is" situation, "to-be" situation and migration plan, is perceived to be corrected well according to feedback provided to us in the interviews of appendix E to I we will perform an artifact validation discussion with experts of the three lines of defense subject. During this discussion we will also evaluate if the design goal of this paper, which evolves around designing a "to-be" situation of the three lines of defense that focuses on improving information management is achieved. Elements of the TAM framework of the paper "*How User Perceptions Influence Software Use"* by Morris et al. [41] are incorporated in the discussion questions. This discussion was conducted according to the book "*Qualitative Research Practice: A Guide for Social Science Students and Researchers"* by Ritchie et al. [49]. As such it combines flexibility with structure. The discussion will be interactive and the "as-is" model, the "to-be" model as well as the migration plan model will be used as a probe to achieve depth. Several questions will be used to guide the discussion, but diversion from the questions is encouraged by us. The group size in this discussion is rather small, but since two of three of the participants were highly involved in the development of the artifact we expect them to have a lot to say on this topic. In addition to this the artifact models are rather complex and are therefore better discussed in smaller groups. Both reasons are stated in the book by Ritchie et al. [49] as being valid reasons to use smaller groups. The discussion questions are designed to be content mining. The goal of the discussion is as follows:

Goal of the discussion: Determine if the corrections to the alpha version of the artifact, which resulted in the beta version the artifact, are implemented according to the feedback given in the interviews of appendix E to I as well as determining if the beta artifact is expected to improved information management within the three lines of defense.

Three experts participated in this discussion:

- Expert 1: EY internal expert. This expert was highly involved in the development of the artifact of this paper and was also interviewed several times during the alpha version evaluations.
- Expert 2: EY internal expert. This expert was highly involved in the topic selection of this paper and was one of the main contributors to the problem statement of this paper.
- Expert 3: EY internal expert. This expert was possesses substantial knowledge about the internal audit field and the three lines of defense, but did not previously contribute to this paper and is likely to be less acquainted with the artifact.

Discussion Structure:

- Thanking the participants for their time.
- Provide the expert with the "as-is" model as described in figure 35.
- Provide the expert with the "to-be" model as described in figure 41.
- Provide the expert with the migration plan model as described in figure 44.
- Provide a PowerPoint presentation about the design goals and the construction of the artifact based on the feedback provided in previous interviews.
- Provide questions during the presentation and discuss the different views:

Design Methodology and Research Relevance Questions:

Question 1: In this paper we propose design goals for the three parts of our artifact. These design goals focus mainly on improving information management in the three lines of defense. This in order to improve the third line of defense's performance. Are there any important aspects missing in the design goals used in this paper? Explain. (Operational – strategic alignment and business - IT alignment [37]).

Question 2: Do you perceive this research to be relevant for Ernst & Young and the three lines of defense in financial companies? Explain. (Perceived usefulness [41]).

Question 3: In our research we combine multiple literary topics with the information management topic. Do you believe that these topics are all relevant to information management and did we miss some important topics? Explain. (Operational – strategic alignment and business - IT alignment [37]).

Question 4: Do you believe that this research will only prove its worth after it has been used in a transition towards the "to-be" situation in a company or do you think that the artifact can provide other insights to experts too? Explain. (Perceived ease of use, perceived usefulness [41]).

"As-Is" Situation Questions:

Question 5: Modelling the "as-is" situation provided this research with a starting point on which to model the "to-be" situation. Do you believe that this "as-is" situation model can also be used to convince companies into changing the three lines of defense or do you believe it to be useful for another purpose? Explain. (Perceived ease of use, perceived usefulness, attitude towards using, behavioral intention to use [41]).

Question 6: In our paper we argue that information management could be improved in "as-is" situation, as this is also the problem proposed to us in the problem statement given by our supervisor within Ernst & Young. What do you think about the "as-is" situation information management when comparing it to aspects of the IM framework of Maes [37] and the KMC of Evans et al. [15]? (Operational – strategic alignment and business - IT alignment, data to information to knowledge conversion [37], [15]. Perceived ease of use [41]).

Question 7: Are there any more missing aspects to the "as-is" situation or has all feedback been incorporated correctly? Explain.

"To-Be" Situation Questions:

Question 8: The "to-be" situation was developed based on requirements derived from literature that was linked to information management, as well as expert opinions. Has our "to-be" situation model achieved a situation in which information management is improved? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge conversion [37], [15]. Perceived usefulness [41]).

Question 9: Do you think that employees of the three lines of defense will have a harder time working via the proposed "to-be" situation compared to the "as-is" situation? Explain. (Perceived ease of use [41]).

Question 10: Do you believe three lines of defense practitioners and consultants to be willing to implement the "to-be" situation and do you believe experts will be willing to work via the "to-be" situation? Explain. (Attitude towards using, behavioral intention to use [41]).

Question 11: Are there any more missing aspects to the "to-be" situation or has all feedback been incorporated correctly? Explain.

Gap Analysis Questions:

Question 12: During prior interviews the interviewees indicated that the main gaps between the "as-is" and "to-be" situation are in the organizational transition and the technical transition. Do you also believe that the hardest parts of the transition are enabling XES logging in company systems, creating data driven dashboards as well as converting the three lines of defense to a data-driven approach? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge conversion [37]. Perceived ease of use [41]).

Question 13: Do you believe the hard parts of the transition will influence the stakeholder's (Top management and three lines of defense employees) willingness towards implementing the "to-be" situation? Explain. (Perceived ease of use, perceived usefulness, attitude towards using, behavioral intention to use [41]).

Question 14: During the prior interviews the interviewees indicated that the expected information management to improve, because analytics helps with capturing more data and helps with converting data to information. Do you believe this is a good observation or do you not expect much difference between the two situations? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge conversion [37], [15]. Perceived usefulness, attitude towards using, behavioral intention to use [41]).

Migration Plan Questions:

Question 15: The migration plan aims to provide a structural overview of how a company should make a transition towards the "to-be" situation. It therefore aims to tackle the gaps identified in the gap analysis. Do you believe this migration plan is practically usable in managing a transition and how hard is it to use this model? Explain. (Perceived ease of use, perceived usefulness, attitude towards using, behavioral intention to use [41]).

Question 16: Would you be willing to use this migration plan when implementing the "to-be" situation in at a client? Do you believe that internally at clients experts would be willing to use the migration plan when implementing a transition towards the "to-be" situation? Explain. (Attitude towards using, behavioral intention to use [41]).

Question 17: Do you think that following the migration plan will have any influence on the resulting "to-be" situation implemented at the end of the transition in terms of information management performance? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge conversion [37]).

Question 18: Are there any more missing aspects to the migration plan or has all feedback been incorporated correctly? Explain.

Future Potential Questions:

Question 19: The artifact was designed mainly for Ernst & Young internal usage in their consultancy jobs. Does the artifact answer provide an answer to the problem statement proposed to us during the initiation of this project? Explain. (Operational – strategic alignment and business - IT alignment, data to information to knowledge conversion [37]).

Question 20: How likely is it that the artifact of this paper will be used in future assignments where Ernst & Young has to help make a transition towards a data-driven internal audit approach at a customer? (Attitude towards using, behavioral intention to use, perceived usefulness [41]).

Question 21: Do you see any other future potentials for this research in addition to being a consultancy product? Explain.

- Ending the discussion.
- Thanking the participants for their time.

QUESTION RESULTS SUMMARY

Question 1:
Expert 3: I think these goals cover all the aspects of what you want to design in your paper.
Expert 2: I agree with this I do not see anything that would want to add to this.
Expert 1: I also agree.

Question 2:
Expert 3: Yes this is very relevant to Ernst & Young since we encounter a lot of customers that struggle with the same problem statement as proposed in your paper and internally within Ernst & Young the literary relations in your paper will also be valuable knowledge.
Expert 2: Yes I would say the same. Certainly for consultancy we can use this for our clients.
Expert 1: I agree with both their comments.

Question 3:
Expert 3: I think you covered most of the important aspects of related to managing information. I cannot think of anything else I would like to see you add to this list.
Expert 2: I think that even if there are more topics than this related to information management, they would not be as relevant as the list you have now. I cannot think of anything I would like to see you add.
Expert 1: I agree with both their comments.

Question 4:
Expert 3: I do think it can be useful also for explaining how internal audit works to people that need that knowledge. But I do think the main advantage of this research.
Expert 2: The main advantage of this research is that it focuses on solving a business problem, in this case information management problems within the three lines of defense. When this research has been used for its purpose it will probably prove even better that it is useful yes.
Expert 1: I agree with both their comments.

Question 5:
Expert 2: I do not think that this model is alone will be useful in convincing a company for example to change their current way of working since it does not specifically show that there is an information management problem from there business process model of the “as-is” situation. The paper will be needed along with the model to convince companies.
Expert 3: I agree with this statement
Expert 1: I also agree with this statement.

Question 6:
Expert 2: I think that information management in the current situation could certainly be improved. Like said in the problem statement of your thesis data is often lacking or of bad quality. In addition to this companies often do not completely know how their business processes work. This makes managing information hard according to the IM framework.
Expert 3: I agree with this. The knowledge management cycle of Evans et al. is of course also based on producing information from quality data. Improvement is always possible.
Expert 1: Improvement is always possible yes.

Question 7:
Expert 1: To clarify the connection between the IIA Three Lines of Defense model and your “as-is” model it is smart to not allocate department names to the swim lanes but simply call them first, second and third line of defense. You should also connect the reports made by the first and second line to the internal audit activities in the third line to clarify that they are used in the internal audits.
Expert 2: Yes I think you should use the same naming as in the IIA model of the Three Lines of Defense.
Expert 3: I agree to this, but I do not think that you missed much important aspects in your model. It looks complete to me.

Question 8:
Expert 3: I certainly believe that in the “to-be” model information management has improved. Data collection is more accurate and controlled and the sharing of information between the three lines is also clear from this model.
Expert 2: I think it is good that you combined information management with the current three lines of defense in a company and I do think information will be more accurate in the “to-be” model compared to the “as-is” model.
Expert 1: I agree with both of them.

Question 9:
Expert 3: Only initially, but I think this is always the case with changes in business processes.
Expert 2: I agree with this. But this is of course never a reason to not do something new.
Expert 1: I do not even think that working via the “to-be” model is that much harder it is just a different skill that is required.

Question 10:
Expert 3: Yes, if they realize the benefits of it.
Expert 2: Technology is becoming more and more important in companies so I do think that it is inevitable that they will have to start working more data driven.
Expert 1: Yes I agree with this.

Question 11:
Expert 1: Basically you should change the department names to first, second and third line of defense like the changes in the “as-is” model. The development of dashboards will also be a first line of defense objective and so you should change the name IT department to first line of defense also
Expert 2: Yes I think it is important that you show the similarities between your models and the IIA model used as basis. IT department is a vague term and developing dashboards will most often be a first line of defense task.
Expert 3: I agree with this.

Question 12:
Expert 3: Yes, I do believe the technical aspects of the “to-be” situation will be really hard to implement and will take a lot of time to do.
Expert 2: Changing the way of working for people will also be a challenge per company and involves often the culture of the company itself too.
Expert 1: I think a lot of companies have systems that will not be able to log event data conform the requirements in the paper. This will of course pose a problem to the implementing experts.

Question 13:
Expert 3: Top management is always reluctant to do things that cost money and yes these gaps will make them somewhat more reluctant I think.
Expert 2: In regard to other stakeholders. The first line will probably see less benefit in this new model than the second and third line, because they believe everything is fine as it is now. Company culture also has a lot of influence in this.
Expert 1: I agree with this.

Question 14:
Expert 1: Analytics improves the conversion between the data and information and results in more accurate information. This is also a big part of your Maes IM framework, so I do expect information management to improve yes.
Expert 2: The business will also be able to check more using analytics than before which also increases the business control.
Expert 3: I also agree with both of this.

Question 15:
Expert 3: Certainly on a high level. I think it is already quite complex, but per company this will have to be made more concrete.
Expert 2: As a baseline I think you did a good job of structuring all important aspects of the gaps on a migration plan. It is certainly practically useful as a baseline for experts.
Expert 1: Yes I agree, but conversion to a company specific plan will be a challenge.

Question 16:
Expert 3: I think that if I have a client with this problem I will certainly want to use your work yes.
Expert 2: Yes, I agree.
Expert 1: I also agree. I think it provides a good overview.

Question 17:
Expert 2: I think that you need to do a transition systematically, so in that respect your migration plan is an example of this. I think it also does not miss any steps. The "to-be" performance will depend a lot on the systematic approach of implementation.
Expert 3: I agree with this.
Expert 1: I also agree with this.

Question 18:
Expert 1: I think you already improved a lot upon the alpha version of this migration plan. I do not see any big issues for this version.
Expert 2: I also see no missing pieces.
Expert 3: I think it is complete.

Question 19:
Expert 2: I think that your connection between the problem statement, that we provided you with, and information management is a good connection. Your master thesis does also connect a lot of other relevant topics to the problem statement this way. Your artifact certainly improves upon the current way of working and therefore I think you did a good job at answering the problem statement.
Expert 1: I agree with this.
Expert 3: Yes, I think you have a good combination of a narrowed down approach to information management, but you also go very wide by connection several other topics to information management.

Question 20:
Expert 3: I think your work will certainly be used in the future. I think we should present your work at the next department meeting to show what you have done.
Expert 2: I heard that your other supervisor is already looking for jobs to implement your work at the moment. So yes, it will definitely be used.
Expert 1: I agree.

Question 21:
Expert 3: I cannot think of anything at the moment no.
Expert 2: I think we can use it internally for learning about the three lines of defense to, but its main contribution will be based on being a consultancy product.
Expert 1: I cannot think of anything else too.

Appendix L: Final Artifact

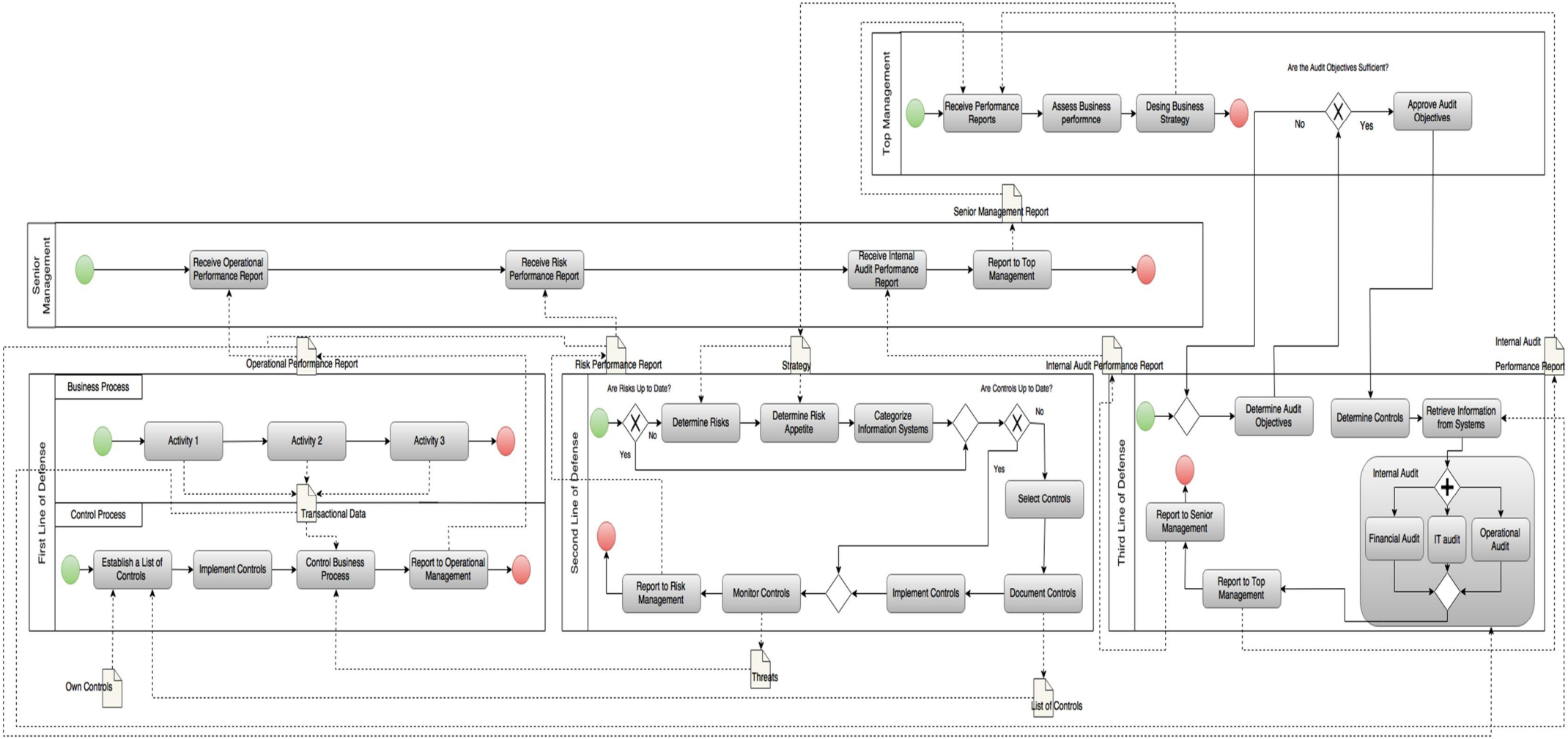
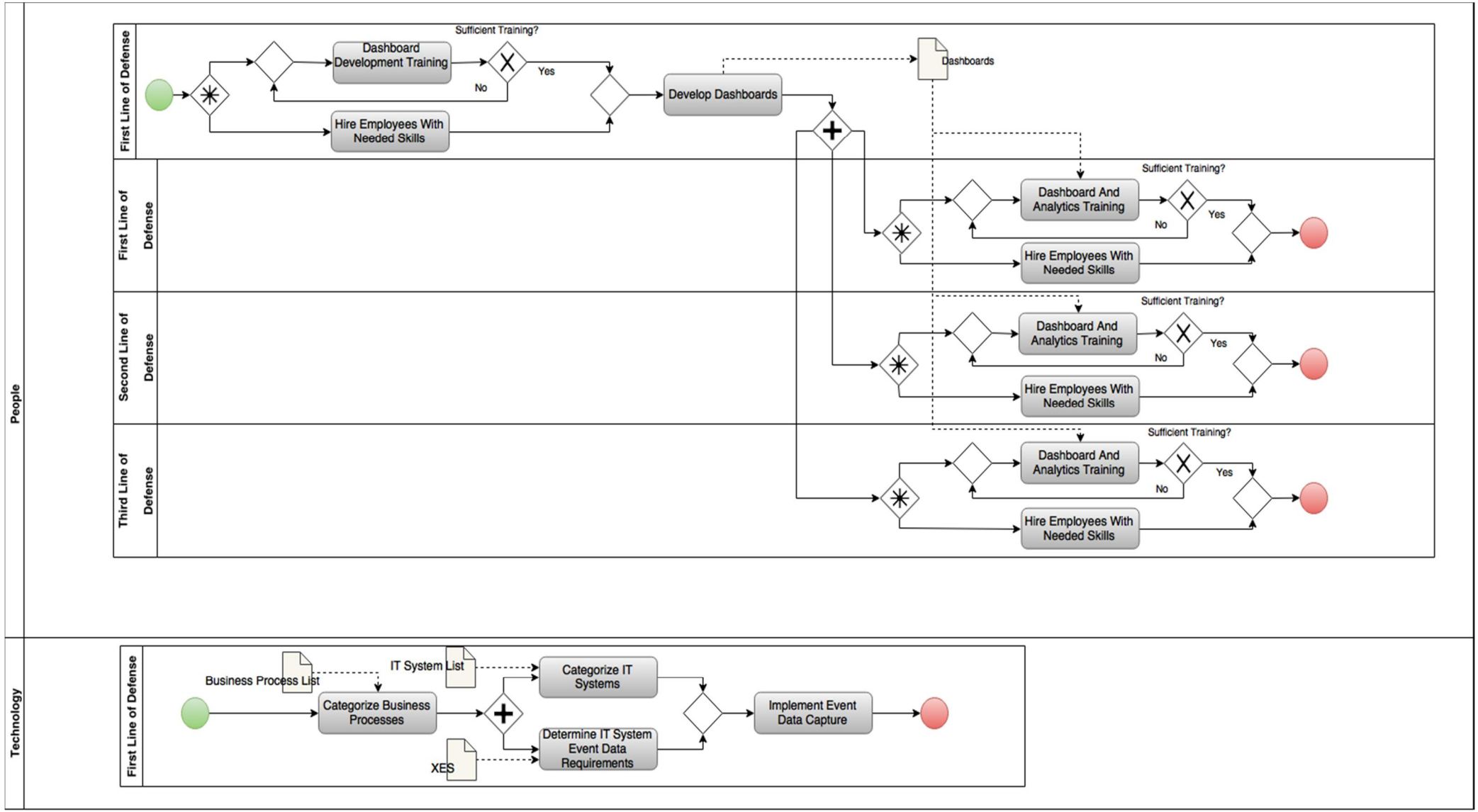


FIGURE 55. AS-IS SITUATION OF THE THREE LINES OF DEFENSE.


People
First Line of Defense
Sufficient Training?
Dashboard Development Training
Yes
No
Hire Employees With Needed Skills
Develop Dashboards
Dashboards
First Line of Defense
Sufficient Training?
Dashboard And Analytics Training
No
Yes
Hire Employees With Needed Skills
Second Line of Defense
Sufficient Training?
Dashboard And Analytics Training
No
Yes
Hire Employees With Needed Skills
Third Line of Defense
Sufficient Training?
Dashboard And Analytics Training
No
Yes
Hire Employees With Needed Skills
Technology
First Line of Defense
Business Process List
IT System List
Categorize Business Processes
Categorize IT Systems
Determine IT System Event Data Requirements
XES
Implement Event Data Capture

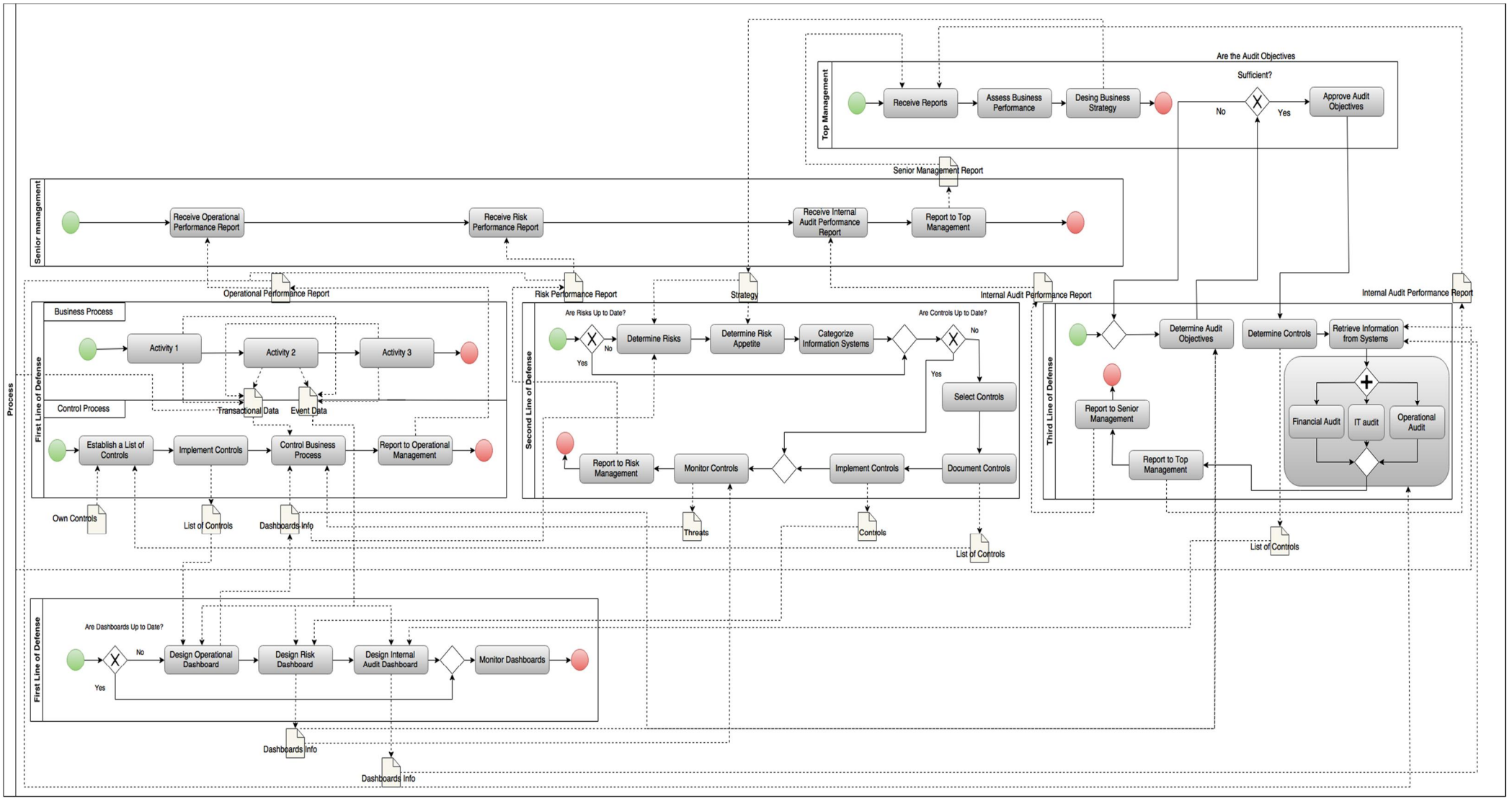


FIGURE 56. TO-BE SITUATION OF THE THREE LINES OF DEFENSE.

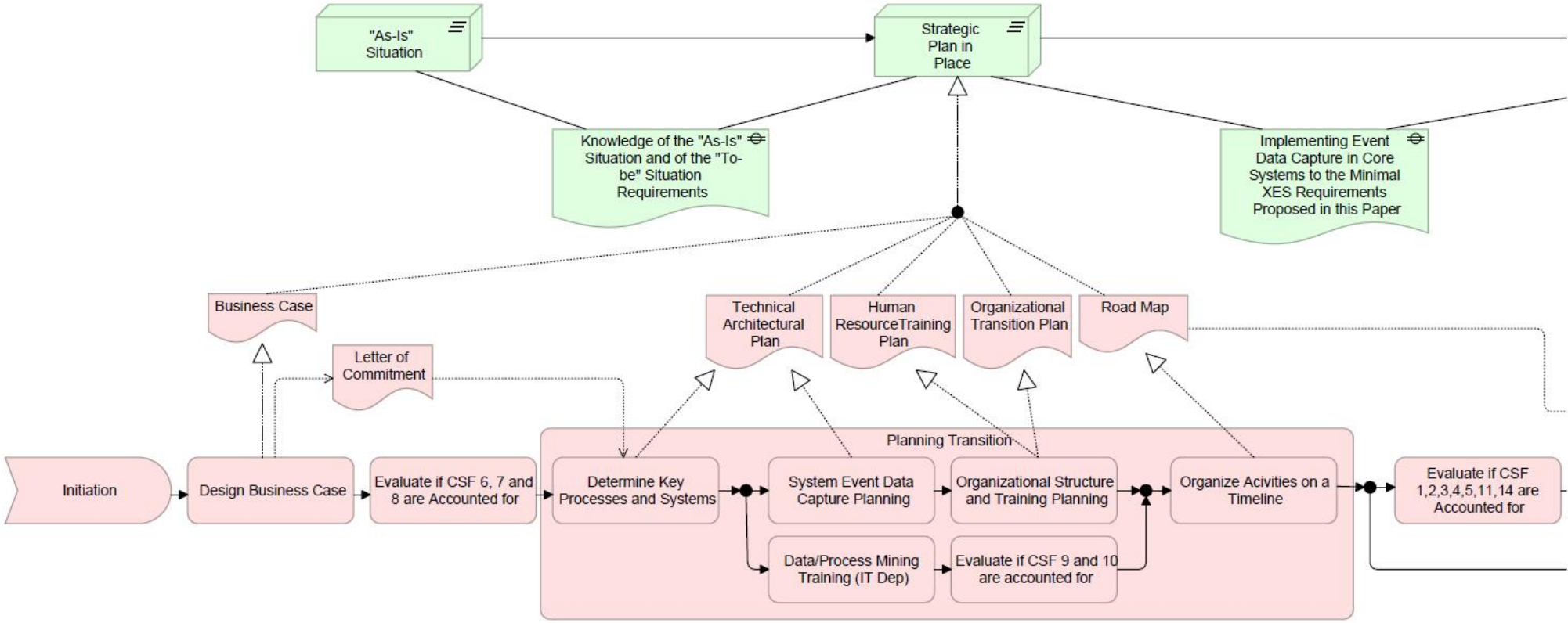
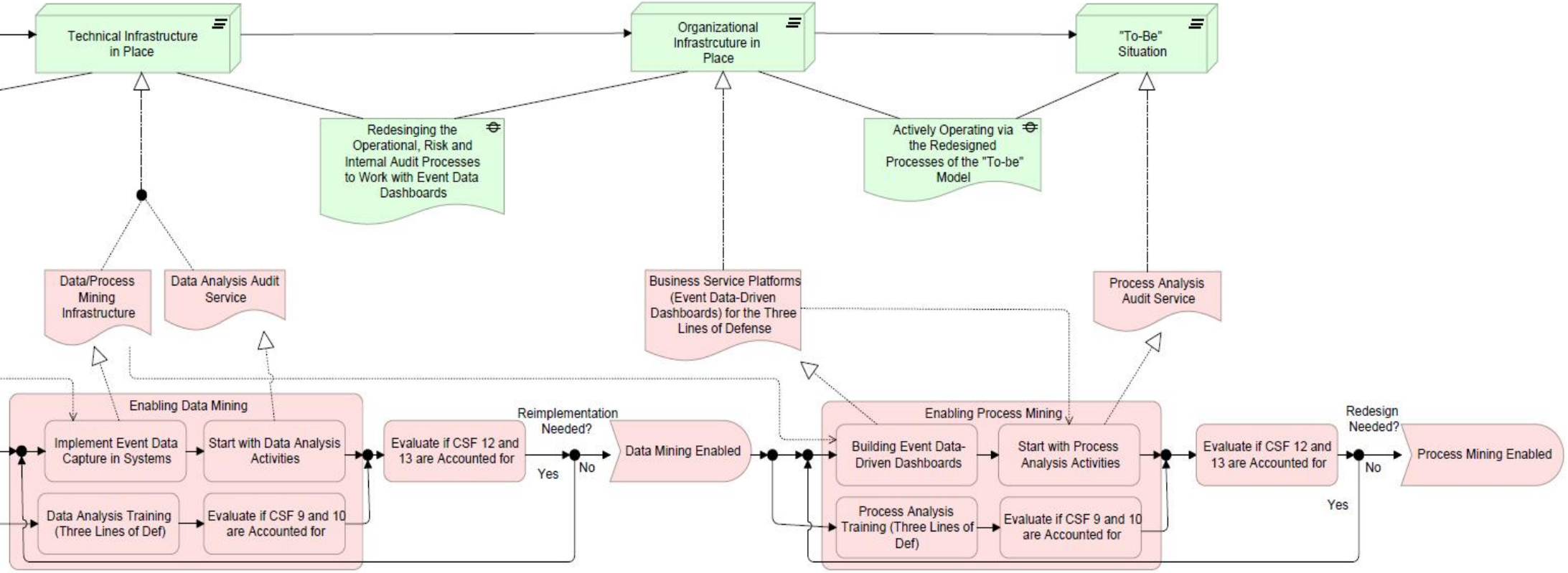


FIGURE 57. MIGRATION PLAN.


Technical Infrastructure in Place
Organizational Infrastrcuture in Place
"To-Be" Situation
Redesinging the Operational, Risk and Internal Audit Processes to Work with Event Data Dashboards
Actively Operating via the Redesigned Processes of the "To-be" Model
Data/Process Mining Infrastructure
Data Analysis Audit Service
Business Service Platforms (Event Data-Driven Dashboards) for the Three Lines of Defense
Process Analysis Audit Service
Enabling Data Mining
Implement Event Data Capture in Systems
Start with Data Analysis Activities
Data Analysis Training (Three Lines of Def)
Evaluate if CSF 9 and 10 are Accounted for
Evaluate if CSF 12 and 13 are Accounted for
Reimplementation Needed?
Yes
No
Data Mining Enabled
Enabling Process Mining
Building Event Data-Driven Dashboards
Start with Process Analysis Activities
Process Analysis Training (Three Lines of Def)
Evaluate if CSF 9 and 10 are Accounted for
Evaluate if CSF 12 and 13 are Accounted for
Redesign Needed?
Yes
No
Process Mining Enabled