ASSESSING THE LEVEL OF SECURITY OF AN ORGANIZATION BY ANALYZING THE ENTERPRISE ARCHITECTURE

A METHODOLOGY

SEBASTIAAN KOENEN
Business Information Technology
Faculty of Electrical Engineering,
Mathematics and Computer Science

April 7, 2015
Enschede

UNIVERSITY OF TWENTE.

Deloitte.

ASSESSING THE LEVEL OF SECURITY OF AN ORGANIZATION BY ANALYZING THE ENTERPRISE ARCHITECTURE

Enschede, 07-04-2015

AUTHOR

Sebastiaan Koenen
Study Programme *Business Information Technology*
Faculty of Electrical Engineering,
Mathematics and Computer Science
Student No. *1002074*
E-mail *s.k.koenen@alumnus.utwente.nl*

GRADUATION COMMITTEE

Maria Iacob, PhD
Department *Industrial Engineering and Business Information Systems*
E-mail *m.e.iacob@utwente.nl*

UNIVERSITY OF TWENTE.

Marten van Sinderen, PhD
Department *Information Systems*
E-mail *m.j.vansinderen@utwente.nl*

UNIVERSITY OF TWENTE.

Erik Hegeman
Department *Enterprise Architecture*
E-mail *ehegeman@deloitte.nl*

Deloitte.

PREFACE

This thesis presents the master research which concludes my master study 'Business Information Technology' at the University of Twente. This also marks the end of my life as a student, which I enjoyed very much. During the past 5 ½ years, I've met fantastic people, done amazing things and learned a lot; both personal and professional.

The research presented in this thesis was performed as a graduate intern at Deloitte Consulting within the department "Enterprise Architecture". Colleagues from within this team provided great input regarding Enterprise Architecture and the application in practice. As this research has a strong security component, additional experts were involved during this. These experts from Deloitte Risk Services provided valuable information on security and its impact in practice.

First, I would like to thank my university supervisors Maria Iacob and Marten van Sinderen for their support during this project. They provided guidance and valuable insight regarding this project. Their experience and feedback helped me improving my research.

Second, I would like to thank Deloitte Consulting for providing me this amazing opportunity. I would especially like to thank Erik Hegeman. His great supervision and energizing meetings really helped me through these months. By providing a critical view when needed, he helped improving this research enormously. I would also like to thank Eric Onderdelinden for his inspiring discussions and valuable expertise during the past months. Next to that, I'd like to thank Willem van der Valk and Jos van der Peet for their involvement in this research. Their knowledge and experience provided the much needed expertise on the field of security. I'd also like to thank my colleagues for the Enterprise Architecture department for their insights and discussion.

A special thanks goes out to the companies that provided my case studies. Without their involvement, the validation of this research would have been much harder. Besides that, they also offered me a very interesting insight in their companies.

Finally, I would like to thank my family, who supported me during my years of study and really helped me get through this final project.

I hope you will enjoy reading my thesis.

EXECUTIVE SUMMARY

In our personal life, we increasingly use Information Technology (IT) to perform our daily tasks and to keep in touch with our friends and family. The same goes for businesses. Even the smallest of businesses make use of IT to perform their tasks. In some cases people rely so much on their IT, they become dependent on their IT facilities (e.g. electronic vs cash payments). As businesses and IT are linked so closely together now, business security and IT security should be observed as one. Security failures in any possible way endanger the business' performance and might harm the organization and its clients. This research sees Enterprise Architecture as a vehicle for integrating security into the organizational design.

There are several initiatives that integrate EA and security, but these look at the process of integrated development. These initiatives, however, do not provide any insight in the quality of the resulting architecture in terms of its security. Therefore, it would be interesting to know how well the architect succeeded in creating a *secure by design* architecture. Up until now, there are very little initiatives looking into the assessment of the security level of an enterprise architecture. This research provides a methodology that can be used as a guideline during such analysis.

As a result, this research provides organizations with a framework and a methodology. This allows for the assessment of the level of information security within an organization by analyzing the enterprise architecture. The provided framework explicates which Enterprise Architecture documentation is needed for the suggested assessment. Also, the framework describes the requirements Information Security imposes on an organization. For each of the requirements, it is determined which artifacts contribute to the fulfillment of the requirement and which content is expected to be present in the concerned artifact. Based on this framework, a methodology is designed. This methodology (roughly) consists of five steps:

Step 1: Determine State and Goal This step aims for providing context to the analysis outcome. The goal of the analysis is explicated. Based on the goal of the analysis, an assessment on the state of the architecture is made.
Step 2: Gather Artifacts In order to start the analysis, the specified documents need to be collected. To check for completeness and to make the analysis easier to perform, the collected documents are mapped to the expected artifacts.
Step 3: Review Requirements Based on the provided framework, each requirement is reviewed. First, evidence for each of the requirements is gathered from the documentation. Second, a conclusion is formed based on this evidence. Finally, a rationale for the conclusion is provided.
Step 4: Determine score After a score is assigned to each requirement, scores for the functions and complete architecture can be determined.
Step 5: Determine improvements Based on the scores assigned in the previous steps, the most important improvements for further development are derived.

Based on the demonstration and evaluation of the methodology in practice, it can be stated that the research are met. The methodology provides insight into the level of integration of information security in the enterprise. Based on a set of expert interviews for each case, the scores assigned by the methodology are believed to be correct. The improvements derived from these scores are seen as valuable input for future development, according to the experts.

Evaluation of the methodology yields the conclusion that the designed analysis method can provide insight in the level of information security in an organization. It does this based on the enterprise architecture of this organization. Therefore, the methodology provides insight into the extent to which a *secure by design* architecture is created.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS **X**

LIST OF TABLES **XI**

LIST OF FIGURES **XII**

1 INTRODUCTION **1**
1.1 INTRODUCTION 1
1.2 BACKGROUND 1
1.2.1 ENTERPRISE ARCHITECTURE 2
1.2.2 (INFORMATION) SECURITY 2
1.3 RESEARCH DESIGN 3
1.3.1 PROBLEM STATEMENT 3
1.3.2 RESEARCH OBJECTIVE 3
1.3.3 RESEARCH QUESTIONS 4
1.3.4 RESEARCH SCOPE AND FOCUS 5
1.3.5 RESEARCH APPROACH 5
1.3.6 DOCUMENT STRUCTURE 6

2 LITERATURE REVIEW **7**
2.1 LITERATURE REVIEW METHODOLOGY OVERVIEW 7
2.2 ENTERPRISE ARCHITECTURE 8
2.2.1 FRAMEWORKS 10
2.2.2 ARTIFACTS 12
2.3 INFORMATION SECURITY 15
2.3.1 FRAMEWORKS AND STANDARDS 17
2.4 COMBINING INFORMATION SECURITY AND ENTERPRISE ARCHITECTURE 19
2.5 DISCUSSION 21

3 SOLUTION DESIGN: FRAMEWORK **23**
3.1 PHASE 1: DEFINING THE CONCEPTS 23
3.1.1 ENTERPRISE ARCHITECTURE 23
3.1.2 INFORMATION SECURITY 27
3.2 PHASE 2: DEFINING THE RELATIONS 29
3.2.1 DEFINING AND TESTING THE DESIGN PROCESS 31
3.2.2 BUILDING THE FRAMEWORK 31
3.2.3 REVISING THE FRAMEWORK 33

4 SOLUTION DESIGN: METHODOLOGY **35**
4.1 METHODOLOGY GOALS 35
4.2 METHODOLOGY DESCRIPTION 36
4.2.1 STEP 1: DETERMINE STATE AND GOAL 36
4.2.2 STEP 2: GATHER ARTIFACTS 39
4.2.3 STEP 3: REVIEW REQUIREMENTS 41
4.2.4 STEP 4: DETERMINE SCORE 42
4.2.5 STEP 5: DETERMINE IMPROVEMENTS 44

5 DEMONSTRATION **47**
5.1 CASE 1: COMPANY A 47

5.2 CASE 2: COMPANY B 47
5.3 CASE 3: COMPANY C 47

6 EVALUATION 49
6.1 METHODOLOGY EVALUATION 49
6.2 OUTCOME EVALUATION 50
6.3 OVERALL DISCUSSION 51

7 CONCLUSION 53
7.1 CONCLUSIONS 53
7.2 CONTRIBUTIONS 56
7.2.1 CONTRIBUTION TO THEORY 56
7.2.2 CONTRIBUTION TO PRACTICE 57
7.3 LIMITATIONS AND SUGGESTIONS FOR FUTURE WORK 57

8 REFERENCES 59

APPENDIX A ENTERPRISE ARCHITECTURE ARTIFACT SELECTION 63

APPENDIX B NIST CATEGORY SPECIFICATION 65

APPENDIX C DEFINITION OF ARTIFACTS 69

APPENDIX D EA - INFORMATION SECURITY FRAMEWORK 79
D.1 COMMENTS ON IDENTIFY FUNCTION 82
D.2 COMMENTS ON PROTECT FUNCTION 84
D.3 COMMENTS ON DETECT FUNCTION 87
D.4 COMMENTS ON RESPOND FUNCTION 88
D.5 COMMENTS ON RECOVER FUNCTION 89

APPENDIX E SCORE SHEET – EMPTY 91

APPENDIX F SCORE SHEET – COMPANY A 95

APPENDIX G SCORE SHEET - COMPANY B 97

APPENDIX H SCORE SHEET - COMPANY C 99

LIST OF ABBREVIATIONS

EA	Enterprise Architecture
InfoSec	Information Security
ISO	International Organization for Standardization
IT	Information Technology
SME	Subject Matter Expert
TOGAF	The Open Group Architecture Framework

LIST OF TABLES

TABLE 1. DOCUMENT STRUCTURE 6
TABLE 2. SELECTION CRITERIA PER SOURCE 8
TABLE 3. KEYWORDS USED FOR LITERATURE RESEARCH 8
TABLE 4. FRAMEWORK ARTIFACT MATRIX 63

LIST OF FIGURES

FIGURE 1. PROBLEM FIELD 3
FIGURE 2. RESEARCH APPROACH 5
FIGURE 3. LITERATURE REVIEW METHODOLOGY BY WOLFSWINKEL ET AL. (2013) 7
FIGURE 4. EA DEFINITION *(GARTNER, 2013)* 9
FIGURE 5. ZACHMAN FRAMEWORK (J. ZACHMAN, 2002) 10
FIGURE 6. FOUR DOMAIN ARCHITECTURE 11
FIGURE 7. TOGAF ADM (THE OPEN GROUP, 2011) 11
FIGURE 8. ESSENTIAL LAYERS OF ENTERPRISE ARCHITECTURE 12
FIGURE 9. PRODUCT CREATED BY ENTERPRISE ARCHITECTURE (BOSTER ET AL., 2000) 13
FIGURE 10. TOGAF ARTIFACT OVERVIEW 14
FIGURE 11. ESSENTIAL ENTERPRISE ARCHITECTURE ARTIFACT. 14
FIGURE 12. OVERVIEW OF ARTIFACT IN AN ENTERPRISE ARCHITECTURE PROJECT 15
FIGURE 13. MCCUMBER CUBE (MCCUMBER, 1991) 17
FIGURE 14. 10 DOMAINS OF THE ISO 17799 18
FIGURE 15. EXTENDED MATRIX SHOWING NIST CATEGORIES 19
FIGURE 16. SECURITY DECISIONS PLOTTED ON THE EA GRID 20
FIGURE 17. GENERIC ARCHITECTURE LAYERS 25
FIGURE 18. ARTIFACT SELECTION PER ARCHITECTURE LAYER 27
FIGURE 19. NIST CATEGORIES PER FUNCTION 29
FIGURE 20. FRAMEWORK DEVELOPMENT PHASES 32
FIGURE 21. BOUNDARY OF EA 32
FIGURE 22. SUMMARIZED FRAMEWORK 34
FIGURE 23. OVERALL METHODOLOGY DESCRIPTION 36
FIGURE 24. PROCESSMODEL STEP 1 37
FIGURE 25. GENERIC MATURITY MODEL (VISUALIZATION BY ROEST (2013)) 38
FIGURE 26. PROCESSMODEL STEP 2 40
FIGURE 27. PROCESSMODEL STEP 3 41
FIGURE 28. INFLUENCE DIAGRAM EXAMPLE 42
FIGURE 29. PROCESSMODEL STEP 4 43
FIGURE 30. PROCESSMODEL STEP 5 45
FIGURE 31. PRACTICAL PROBLEM AND SOLUTION 49
FIGURE 32. SELECTED ARTIFACTS FOR THE REPRESENTATION OF ENTERPRISE ARCHITECTURE 53
FIGURE 33. NIST REQUIREMENT CATEGORY OVERVIEW 54
FIGURE 34. OVERALL METHODOLOGY DESCRIPTION 55

1 INTRODUCTION

This chapter provides an introduction into the research that was conducted. Section 1.1 describes the incentive for this research and section 1.2 provides basic background information on the subjects involved in this research. Section 1.3 presents the problem statement (1.3.1), research objectives (1.3.2) and research questions (1.3.3).

1.1 Introduction

Information Technology (IT) becomes much more important in our daily life. In our personal life, we increasingly use IT to perform our daily tasks and to keep in touch with our friends and family. The same goes for businesses. Even the smallest of businesses make use of IT to do their work. As our usage of IT is growing, people start to rely on the availability of the devices and their correct working. In some cases people rely so much on their IT, they become dependent on their resources. For example, businesses relying fully on their electronic payment systems instead of cash payments.

The impact of an information breach became painfully demonstrated by Sony in November 2014. The "Sony-pocalypse", as it was called by Adrian Sanabria (Pagliery, 2014), had an enormous impact. On November 24th Sony stated that an I.T. matter was being investigated. This turned out to quite an understatement. In the days following this statement more information became available to the press. Sony was hit by a cyberattack of enormous scale.

On the one hand, the business was hit. The internal network of Sony became unusable as was their email. This caused an enormous inconvenience for Sony and endangered their business. The illegal distribution of several stolen movies will probably impact the company financially as well. On the other hand, enormous amounts of internal documents were released. These documents contained private memos, employee salaries, social security numbers, health information and a lot of other information. Information that would not typically be shared this openly (Pagliery, 2014). This impacted not only the business, but also the employees of Sony.

At one point the staff was told “There is no playbook for us to turn to” (Cieply & Barnes, 2014). This seems unbelievable, but is more common than one would hope. Based on this major incident, Marc Hijink created a list of 10 lessons all businesses could learn from Sony (Hijink, 2014). These lessons could be grouped in three main categories: keep track of your information, invest in training and professionals and monitor both the presence and activity of accounts.

This example demonstrates the impact of malfunctioning business IT. Whenever business is hit by any form of attack, it should be capable of coping with it. This is why the importance of security is growing. As businesses and IT are linked so closely together now, their security should be looked at as a unity. Failure in any possible way endangers the business’ continuity and might harm themselves and their clients. Also the storage of huge amounts of (personal) data creates a new type of hazard for businesses and their clients. As this problem has a lot of attention now, an incident will have a very big influence on the image and reputation of the firm. In order to help businesses improve their security, this research aims to find out how the use of Enterprise Architecture can support their security.

1.2 Background

The proposed solution is based on two fields which increasingly gain more attention. The first is the field of Enterprise Architecture (EA). EA focuses on the integration of business and IT. It does this by looking at business-IT alignment in several ways. The other field on which this research is

based is the field of Security. Security, in its many forms, has been around forever (e.g. people use fire to scare away animals for centuries). However, its application in the field of (business) IT is relatively new. The remainder of this section will provide a little more background information on these subjects. The full literature review can be found in chapter 2.

For the remainder of this thesis, a writing convention is introduced. Whenever the field of Enterprise Architecture is meant, capitals are used. When enterprise architecture refers to an instance, for example the architecture of a specific organization, lowercases are used. This convention is also used for the field and instance of Information Security.

1.2.1 Enterprise Architecture

As stated before, Enterprise Architecture is a (relatively) new discipline which focuses on business and IT alignment. This means that the IT delivery is adapted to the business needs. This makes business and IT work together, instead of against each other. Enterprise Architecture supports this alignment by creating structured designs of all elements in the organization. These elements can consist of persons, applications, hardware or information.

In time, several definitions of Enterprise Architecture have been created. One of the founders of the EA discipline is John Zachman. He created the following definition of Enterprise Architecture: *"Architecture is that set of design artifacts, or descriptive representations, that are relevant for describing an object such that it can be produced to requirements (quality) as well as maintained over the period of its useful life (change)."* (J. A. Zachman, 1997). This definition of EA is rather technical. It is based on the activities the enterprise architects perform and outcome. As years passed and EA evolved, the definition got another focus as well. The following definition created by Gartner (2013) shows the evolution of the EA discipline: *"Enterprise architecture (EA) is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes. EA delivers value by presenting business and IT leaders with signature-ready recommendations for adjusting policies and projects to achieve target business outcomes that capitalize on relevant business disruptions. EA is used to steer decision making toward the evolution of the future state architecture."*

In this context, Enterprise Architecture is used as the formal representation of the business. This is done guided by the artifacts that the EA process generated and is the tangible form of the EA activities. Therefore these artifacts are very well suited as basis for the analysis that this research presents. More information on Enterprise Architecture will be provided in Section 2.2, where the results of the literature review are presented. In section 3.1.1, the choice for artifacts will be elaborated.

1.2.2 (Information) Security

Whitman and Mattord (2011) define security as "Protection from danger". In business this can mean various things, ranging from a physical guard at the front porch till digital defense. For this thesis a specific part of Security is chosen: Information security (InfoSec). This part of security focuses on all information present in the organization in physical as well as digital form. Based on the presented definition, Whitman and Mattord (2011) define Information Security as "The protection of information assets that use, store, or transmit information from risk through the application of policy, education, and technology."

The ISO 27000 series offers as similar view on information security: "The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable". The assurance of confidentiality, integrity, and availability of data and information, also known as the CIA triad, is a reoccurring phenomenon in

different view on InfoSec. A more extensive view on Information Security is presented in the literature review, more specifically section 2.3.

1.3 Research Design

1.3.1 Problem Statement

A recent study performed by Van den Bosch (2014) presents an effort into the direction of bringing Enterprise Architecture and Security together. This research integrates the TOGAF standard (The Open Group, 2011) for Enterprise Architecture and the SABSA framework (Sherwood, Clark, & Lynas, 2009) for Information Security. The research specifies three parts: (1) a framework, (2) a method and (3) a modeling language. Through executing the combined method, every step of the EA development process now also incorporates security. Combining this with the proposed extension for the Archimate modeling language (The Open Group, 2013), this research enables the modeling of security within the Enterprise Architecture.

The above mentioned research helps to create an integrated view of Enterprise Architecture and Information Security. Based on these extended models, analysis on the state of the security throughout the enterprise would be the next logical step in this direction. This pursuit of the *secure by design* architecture is one that still continues. There are several initiatives that integrate EA and security, but these look at the process of development. These initiatives, however, do not provide any insight the quality of the resulting architecture. Therefore, it would be interesting to know how well the architect succeeded in creating a *secure by design* architecture. Up until now, there are very little initiatives looking into assessing the security level of the architecture. This is the void where this research fits in to.

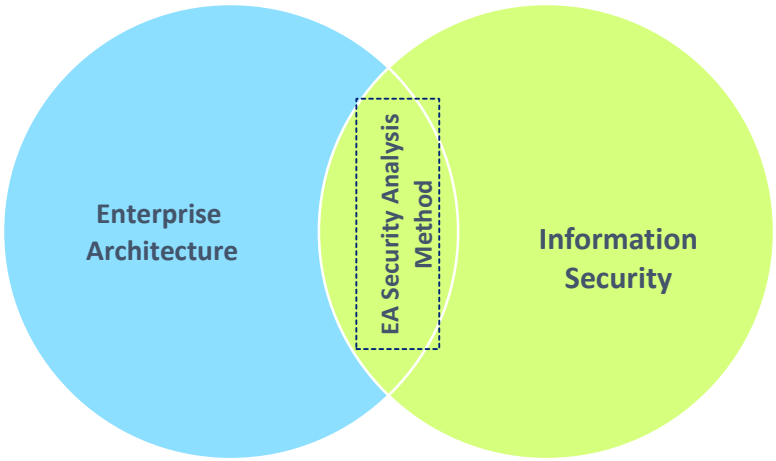

FIGURE 1. PROBLEM FIELD

1.3.2 Research Objective

As stated before, the areas of Enterprise Architecture and Information Security are evolving. At this point in time however, there is a relatively big gap between these two fields. This research aims to close this gap a bit more. This is done by aiming for three objectives:

1. This research aims to find those elements in the Enterprise Architecture that help to fulfill requirements from Information Security. By doing this, connections between the now distant fields become clearer and can be used in order to integrate the fields (a little) further.

2. This research aims to find Information Security metrics in the Enterprise Architecture. When it is determined which elements help to fulfill Information Security requirements, it can be determined how this is done. A description of what is expected to be found within each artifact can be created. This enables the use of these relations as metrics.
3. This research aims to create the first version of a methodology to analyze the state of the Information Security of an organization based on its Enterprise Architecture. In this methodology the earlier established metrics will be used.

By achieving these objectives, this research can contribute to both theory and practice. The proposed framework should describe the relation between Information Security and Enterprise Architecture in a way that is not yet present. Based on this framework, new theories can be developed. The proposed methodology should be a guideline in using this framework. The methodology should provide guidance in the measurement of the metrics described in the framework.

The framework and methodology this research proposes, offer new possibilities for organizations. The use of a scientifically developed methodology could provide a new service offering, especially in the consulting sector. This new offering could be usable at existing clients to improve the quality of their current architecture, but also help consultants to make better designs from the start. It also could enable a (rare) collaboration between the Enterprise Architects and the Security Officers.

The methodology this research proposes could evolve into a maturity model. If measurements can be made on the architecture, certain levels could be identified. These levels could be described in the form of a maturity model. However, this requires a certain maturity of the methodology. This maturity cannot be reached within the timeframe of this research. Therefore, this subject will not receive any more attention.

1.3.3 Research Questions

In order to present a solution to the aforementioned problem and to complete the research objectives, this research answers the following research question:

How can we assess the level of information security within an organization by analyzing the enterprise architecture?

To answer this question, the following sub questions are answered:

SQ 1: Which enterprise architecture descriptions are suitable for this analysis?

Based on a literature review, the field of Enterprise Architecture is defined and characterized for this research. For the development and maintenance of Enterprise Architecture, many frameworks and standards are available. Based on one of these frameworks or standards, a representation for Enterprise Architecture for this analysis is derived.

SQ 2: Which information security descriptions are suitable for this analysis?

For answering this sub question, the same approach as with SQ 1 is followed. A literature review provides commonly accepted ways of looking at (information) security in an enterprise perspective. The methodology uses these to determine the requirements Information Security imposes to Enterprise Architecture.

SQ 3: Which integrated approaches are available?

To complete the view upon security and EA, it is interesting to know what initiatives already have been undertaken in the field. The integrations might show where these fields touch and how these initiatives handle this.

SQ 4: Which requirements does Information Security impose on Enterprise Architecture?
Based on the descriptions developed in SQ1 and SQ2, the relation between the two concepts can be determined. In order to be able to derive a methodology from these relations, their description should be as precise as possible. Expectations on the fulfillment of the requirements need to be added.

SQ 5: Can a methodology be defined to analyze the level of security within an Enterprise Architecture?
The aim for this question is the development of the methodology and supporting tool(s). This is be done based on the results of the literature review and input from various SME's. The methodology will aim for several goals, which will be established in section 4.1.

1.3.4 Research Scope and Focus
This research focuses on the development of tool and method for the analysis of Enterprise Architecture from an Information Security viewpoint. As the method should be easily applicable in all sorts of enterprises, no scoping has been done to any industry. To show its industry independency, the case studies will be conducted in different fields.

1.3.5 Research Approach
In order to answer the research questions, the approach shown in Figure 2 is used. As this is design research, the research approach is based on the Design Science Research Methodology by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007). This methodology describes what steps need to be taken in order to get to a rigid design. The first stage of the research methodology is to identify and motivate the problem. This is done in the previous part of this thesis. Then an extra phase is introduced in order for this research to be more solid: a literature review (shown in dark shade in Figure 2). This review is done following the guidelines of Wolfswinkel, Furtmueller, and Wilderom (2013) and Webster and Watson (2002).
The findings of this search are then processed in order to create a comprehensible framework for the analysis of EA. Then a methodology is described for performing the analysis based on the established framework. The methodology and underlying framework are demonstrated by use of case studies. The outcome of these demonstrations is evaluated using interviews. These interviews are conducted using several external and internal SMEs.

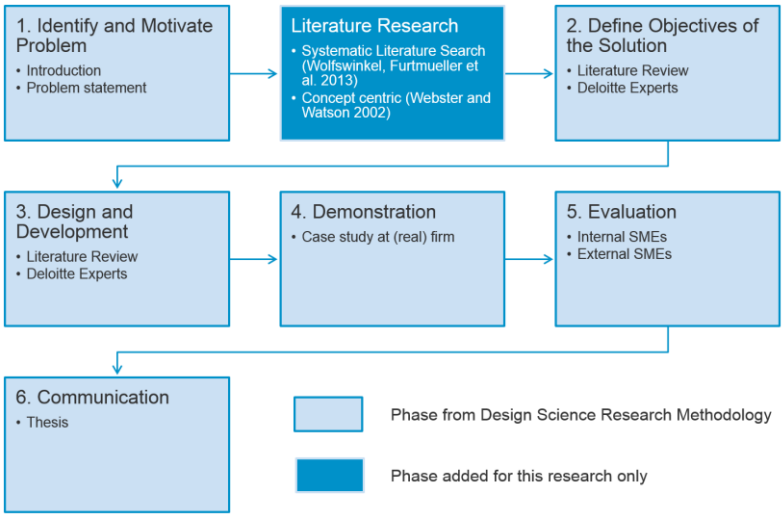

FIGURE 2. RESEARCH APPROACH

1.3.6 Document Structure

The remainder of this document is structured as follows: Chapter 2 presents the process and outcome of the literature review. Chapter 3 describes the first part of the solution design. In this chapter the process and outcome of the framework design is described. This is used in the methodology design; which is presented in Chapter 4. In Chapter 5, the designed methodology is demonstrated by the use of case studies. Chapter 6 presents the evaluation of the performed case studies. In Chapter 7 the final conclusion of this research is presented.

This document is the final step of the research approach. It focuses on providing answers to the formulated research questions. Table 1 describes the relation between this document and the research questions.

TABLE 1. DOCUMENT STRUCTURE

Research Question	Answered in	Methodology	Outcome
SQ 1: Which enterprise architecture descriptions are suitable for this analysis?	Section 2.2 and 3.1.1	Literature review and design	A suitable description of Enterprise Architecture for the use in the proposed analysis method.
SQ 2: Which information security descriptions are suitable for this analysis?	Section 2.3 and 3.1.2	Literature review and design	A suitable description of Information Security for the use in the proposed analysis method.
SQ 3: Which integrated approaches are available?	Section 2.4	Literature review	An overview of the available integrated approaches.
SQ 4: Which requirements does Information Security impose on Enterprise Architecture?	Section 3.2	Design based on answers SQ 1 and SQ 2. In this design, expert workshops and interviews were used.	A framework describing the Enterprise Architecture artifacts involved in fulfilling Information Security requirements.
SQ 5: Can a methodology be defined to analyze the level of security within an Enterprise Architecture?	Chapter 4, 5 and 6	Design based on answer SQ 4. In this design, expert workshops and interviews were used.	A methodology that serves as a guideline for assessing the level over information security in the enterprise architecture.

2 LITERATURE REVIEW

The second phase of the research methodology is the literature review. This chapter presents this review. Section 2.1 outlines the approach that was followed. In sections 2.2 till 2.4, the outcomes of the literature review are presented. In section 2.5 a discussion on the results is presented.

2.1 Literature Review Methodology Overview

This chapter will present the methodology that was used to execute the literature review. This approach is based on the rigorous method for reviewing literature as described by Wolfswinkel et al. (2013). In this paper a five-step method for performing a structured literature search using Grounded theory is presented. Figure 3 shows an overview of these steps.

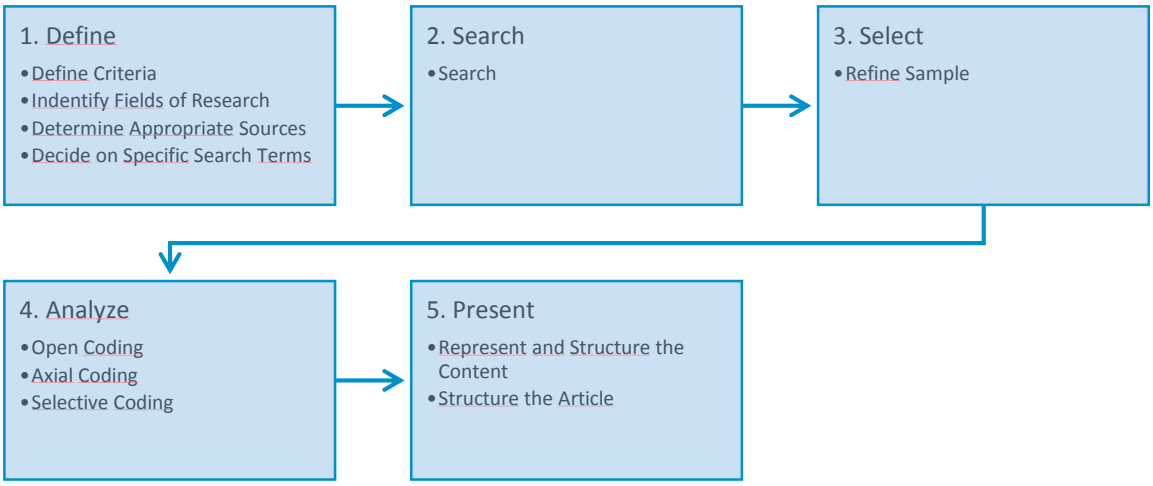

FIGURE 3. LITERATURE REVIEW METHODOLOGY BY WOLFSWINKEL ET AL. (2013)

Before starting the literature research, several parameters need to be defined. First, it was decided that Google Scholar and Scopus would be the most appropriate sources. Both sources offer a broad selection of papers and are known for their high quality result. Google Scholar stands out because of the many sources it consults. Scopus is used as a source because of its peer-reviewed articles.

In order to get high quality set of papers as input, a number of selection criteria was defined. Because the sources have different default settings and offer a different set of search options, both got their own set of selection criteria (shown in Table 2, page 8). The selection was done in 3 steps. The first step was the creation of the Long List. All references that matched the criteria given in Table 2 were added onto this list. In the second step, the relevance of the references was determined based on their title and source. This resulted in the middle list. The third step was the creation of the short list. In order to decide which papers would be on this list, the abstracts were looked at and a quick scan of the paper was performed.

TABLE 2. SELECTION CRITERIA PER SOURCE

Google Scholar	Scopus
	Search within "Article Title, Abstract and Keywords"
Sorted by Relevance	Sort by Citation Count
Select top 30 results	Select top 30 results

As Enterprise Architecture and Security are both relatively new domains, they are developing at a rapid pace. Therefore the more recent work probably will be more relevant. However, introducing a tight publication date limit might exclude fundamental papers. It was decided to use the publication date only as a criterion is case of doubt when creating the middle list. If the relevance of a paper was doubtful, a publication date after 2004 would get it on the middle list. The last part of the research preparation consists of the selection of keywords. The first set of keywords was based on section 1.2 & 1.3 in which the basis for this research is presented.

As the literature search developed, the set of keywords expanded. The research started as a concept-centric search, as it is called by Webster and Watson (2002); searching for keywords (and combinations of keywords) based on the subject you want to research. As results from these queries might often refer to certain authors, these author might be worth investigating as well. These author become keywords on their own. This is called a author-centric approach (Webster & Watson, 2002).

As indicated above, the limitation in publication date might exclude certain papers that are important to the field. In order to cope with this, two measures were taken. The first being the introduction of the author-centric approach. The second measure was used during the examination of the relevant articles. At this point in time, the references of the articles were checked for relevant literature. Articles that are highly relevant are often based on relevant literature. This approach was also used to reinforce the literature review.

TABLE 3. KEYWORDS USED FOR LITERATURE RESEARCH

Keywords:	Combined with:
Enterprise Architecture	artifact
Security	activities
	component
	element
	framework
	standard
	security
	risk
Separate keywords:	
Enterprise AND Security	
Information AND Security	

In section the folling sections (2.2 till 2.5), the results of this research will be presented. The results are structured using the concept-centric approach of Webster and Watson (2002).

2.2 Enterprise Architecture

Enterprise architecture is a field that is hard to catch in a definition. It embraces so many elements of business and IT, it become hard to pinpoint what EA exactly is. Nevertheless the definitions provided for the EA field and profession are aiming to describe more or less the same.

One of the first to define was John Zachman, founder of the Zachman Framework. As mentioned before he describes EA as: *"Architecture is that set of design artifacts, or descriptive representations, that are relevant for describing an object such that it can be produced to requirements (quality) as well as maintained over the period of its useful life (change)."* (J. A. Zachman, 1997). This definition displays a rather technical view on EA, which has three notable elements. Enterprise Architecture is (1) a discipline of design artifacts and representations; these are used to document the present and future state of the enterprise. This helps to ensure (2) the quality of the solutions now and in the future and (3) provides support for future change.

The Open Group, founder of the TOGAF framework, has more or less the same view on EA: *"Generic building blocks, their inter-relationships with other building blocks, combined with the principles and guidelines that provide a foundation on which more specific architectures can be built."* (The Open Group, 2011). In their definition principles and guidelines are added for the consistency between the various deliverables.

The past few years the focus within the Enterprise Architecture field has shifted. Where the rather technical views on EA used to predominate, a new view on EA is rising in academic and practice. The emphasis now moves increasingly towards the guidance in the process of business IT alignment. This was in an early stage recognized by Aziz, Obitz, Modi, and Sarkar (2005) who talk about EA as "*the holistic view of an enterprise's processes, information and information technology assets as a vehicle for aligning business and IT in a structured and therefore more efficient and sustainable way."*.

This is easily seen in the equation Bernard (2012) uses to (partly) define his view on Enterprise Architecture:

EA = Strategy + Business + Technology

This equation defines EA to be 2 parts of business on 1 part of technology. Where Zachman and TOGAF focus mainly on the production of artifacts and requirements, this definition looks more into the business and IT merger.

This movement has also been embraced by Gartner and therefore they update their definition in 2013. Their definition now states more of a consulting advisory role for the enterprise architect in all projects throughout the company:

> *"Enterprise architecture (EA) is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes. EA delivers value by presenting business and IT leaders with signature-ready recommendations for adjusting policies and projects to achieve target business outcomes that capitalize on relevant business disruptions. EA is used to steer decision making toward the evolution of the future state architecture." (Gartner, 2013)*

FIGURE 4. EA DEFINITION *(GARTNER, 2013)*

This definition of EA is considered by the authors as the most accurate view of the discipline as it is now. Therefore this definition is adopted as the definition of EA for this thesis.

2.2.1 Frameworks

Enterprise Architecture frameworks are one of the main tools in the architect's toolbox. A framework provides guidance in the development and maintenance of an Enterprise Architecture. These frameworks offer guidance in various different ways. In this section a set of frameworks will be discussed for their similarities and differences.

ZACHMAN FRAMEWORK

The first framework to be discussed is the Zachman Framework. This framework, created by J. A. Zachman (1987), was one of the first frameworks for Enterprise Architecture. Since then, the framework got extended to the form it is now. In the past years the Zachman framework got accepted as one of the foundation for EA.

The framework consists of a 6x5 matrix. In this matrix the columns represent the fundamental questions that are concerned with architecture development (J. A. Zachman, 1997). These question help determining what needs to be look at in the Enterprise, how it is used in the enterprise, where it is positioned with regards to its peers, who are involved, when it is used or executed and why all of this is the way it is. These questions are very important in the development of an enterprise architecture, but their answers can be different depending on the person asked.

As Enterprise Architecture is a holistic view on the enterprise, these questions can be approached from different angles. These angles are represented by the rows of the matrix; the viewpoints. These viewpoint define the subject on which the questions are answered and to which level of detail (J. Zachman, 2002). These levels range from the planner, which is the environmental level of the enterprise, to the user, which looks at the most low level of the architecture. By looking at the different questions from the various viewpoint, a well-balanced enterprise architecture is developed.

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (contextual) *Role: Planner*	List of things important in the business	List of Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goal & Strategies
Enterprise Model (conceptual) *Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (logical) *Role:Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (physical) *Role:Builder*	Physical Data/Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Reprentation (out of context) *Role: Programmer*	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise *Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

FIGURE 5. ZACHMAN FRAMEWORK (J. ZACHMAN, 2002)

THE FOUR DOMAIN ARCHITECTURE

The Four Domain Architecture (FDA) was developed by Iyer and Gottlieb (2004). This architecture is proposed as a supportive instrument in the usage of a framework like the Zachman framework. By grouping similar elements into domains, domain-specific architectures can be constructed which reflect a common composition and are simple and clearly focused.

The first domain they describe, is the process domain. This domain contains *"the processes, procedures, business tools, tasks that encode business rules, and dependencies required to support the various functions within a business"* (Iyer & Gottlieb, 2004). The Information Knowledge domain looks into the business rules and data/information. Of this data/information several things are described, for example ownership, usage, definitions and interrelationships. The third domain is the infrastructure domain and describes all hardware available in the organization including networks and human interfaces. The last domain is the Organization domain. This domain specifies all business people and organizational structure. Also this domain specifies the roles and responsibilities of these business people.

Process Domain	Information/Knowledge Domain	Infrastructure Domain	Organization Domain
Business context engines	Business data	Computers	People
Planning engine	Business profiles	Operating systems	Roles
Visualization engine	Business models	Display devices	Organizational structures
Business tools	Data models	Networks	Alliances

FIGURE 6. FOUR DOMAIN ARCHITECTURE

TOGAF

The *The Open Group Architecture Framework (TOGAF)* is a product of The Open Group (2011). In their view the enterprise architecture consists of 4 layers: the Business Architecture, the Application Architecture, the Data Architecture and the Technical Architecture. This however is not the main feature of their framework. The main feature of the TOGAF is the Architecture Development Method (ADM) (Sessions, 2007). The ADM describes what phases should be performed in the development of an architecture and which artifacts and deliverables should be created in order to build a sound and complete architecture.

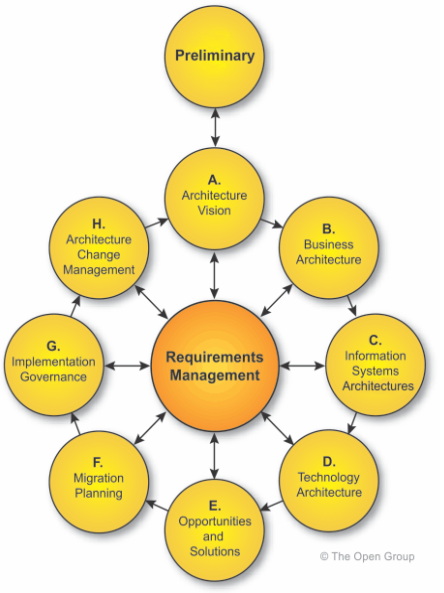

FIGURE 7. TOGAF ADM (The Open Group, 2011)

The ADM also defines several phases before and after the actual creation of the architecture. Before the actual architectures can be created, several steps need to be undertaken. For example, the Architectural Principles need to be set and the stakeholders need to be determined. These decision will guide the design choices that need to be made later on. The choices are also influenced by the requirements that rest upon the project. Finally, the ADM also provides guidance in the delivery of the architecture.

According toTang, Han, and Chen (2004), the TOGAF ADM is rather generic method. It is not prescriptive on breadth of coverage, level of detail or time horizon. These decisions are left to the architects of the particular project. This is a big difference with a framework like Zachmans. TOGAF describes the artifact that need to be created and how to do this. A framework like the Zachman Framework, describes how to categorize them (Sessions, 2007).

ARCHIMATE

To model the designed architectures, The Open Group also developed a modeling language. This language is called Archimate and is composed of three layers. Each of the layers offers set of possibilities for modeling the enterprise. Using the language it is possible to create one model,

describing the whole enterprise(M. M. Lankhorst, 2004). In the Archimate language, the same layers are defined as within TOGAF.

ESSENTIALS

In this paper, Winter and Fischer (2006) observe the enterprise architecture domain. They compare several architectural frameworks and observe their differences and similarities. Using this observation, they extract the essentials of Enterprise Architecture layers.

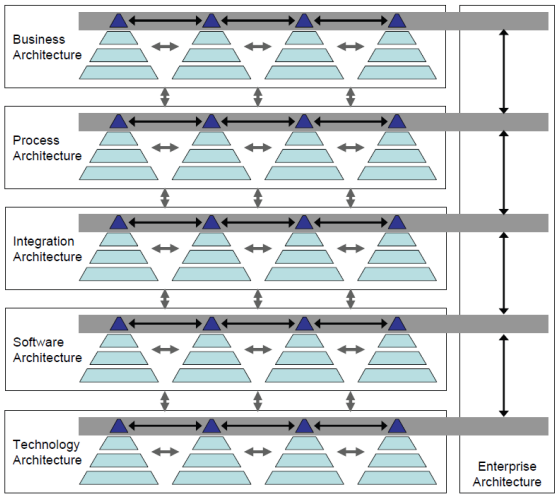

FIGURE 8. ESSENTIAL LAYERS OF ENTERPRISE ARCHITECTURE

They define their set of essential layers as a set of five. The Business layer describes the products and services that the business is aiming to deliver. How this is achieved is specified in the process layer. They propose not use too many detail in this architecture. The level of a sub process should be enough. The Integration layer describes the dependencies and data flow between applications (components). How these applications work fit together is described in the Software architecture. This however does not present detailed description of data objects and specifics of the behavior of one piece of software. This is managed elsewhere. The final layer is the Technology layer. Here the hardware components are presented.

2.2.2 Artifacts

In the use of these frameworks and methods a lot of activities are performed. The Enterprise Architecture artifacts are the only tangible outcome of these activities. Even more than there are frameworks, there are different artifacts. Each different framework, method or even architect has its own way of describing the architecture. This section will provide insight in these different artifacts.

GETTING THE MOST FROM YOUR ENTERPRISE ARCHITECTURE

In this article, Boster, Liu, and Thomas (2000) look into getting the effectiveness of the Enterprise Architecture activities. Based on this observations, they create a set of activities one should perform, a set of skills one should have and a set of products one should create. These products are categorized as technical or business products. Both follow roughly the same structure; firstly, it needs to be known what are the drivers for the coming change. Then a baseline architecture should be created, the as-is situation. Subsequently, an architecture is determined towards which the change should lead. This is called the to-be architecture. In order to really achieve the goal, an implementation plan needs to be created. From a technical perspective, this mainly contains a transition plan. On the business side, an investment plan is needed and strategies for procurement need to be determined. Finally, the architecture is implemented. In this phase, government practices and information systems are produced on the IT side, while the business is performing market research and investment reviews.

Table 3. Products in each step of the architecting process. Make sure that business stakeholders understand your measures and models.

Process step	Technical products	Business products
Initiate the effort	Technical drivers Architecture framework	Business drivers Performance measures
Describe where we are	Baseline IT architecture	Current business models
Identify where we'd like to be	Target IT architecture	Target business models Valued outcomes and features
Plan how to get there	IT transition/migration plan IT asset management plan	Capital IT investment plan Procurement strategies/practices
Implement the architecture	Architecture governing practices Information systems	Market research Investment management review

FIGURE 9. PRODUCT CREATED BY ENTERPRISE ARCHITECTURE (BOSTER ET AL., 2000)

This paper seems to present a rather complete overview of the documents needed in the architecture process. However, it is not really specific on how the architecture should be described. It provide more of a high-level description of what is needed, than what is should contain.

TOGAF

The TOGAF framework (The Open Group, 2011) provides more low level information about the expected artifacts. The artifacts shown in the artifact overview (Figure 10) all match a specific step in the Architecture Development Method (ADM). For each phase of the ADM a set of artifacts is described which are needed to cover the entire phase.

Within these artifacts three types can be distinguished: Catalogs, Matrices and Diagrams. Each of these types has its own target. The catalogs provide information on the building blocks available in a specific domain (e.g. applications or requirements). The matrices provide information on the relationships between the different building blocks. The actor/role matrix, for example, specifies which physical person is assigned which role. By creating these matrices, the relations between building blocks of different types are defined. The diagrams have a similar goal. Diagrams show the different building blocks and their relationships in a graphical way. For example, a data diagram is used to specify the data entities and their cohesion. By creating a graphical representation, it supports more effective stakeholder communication.

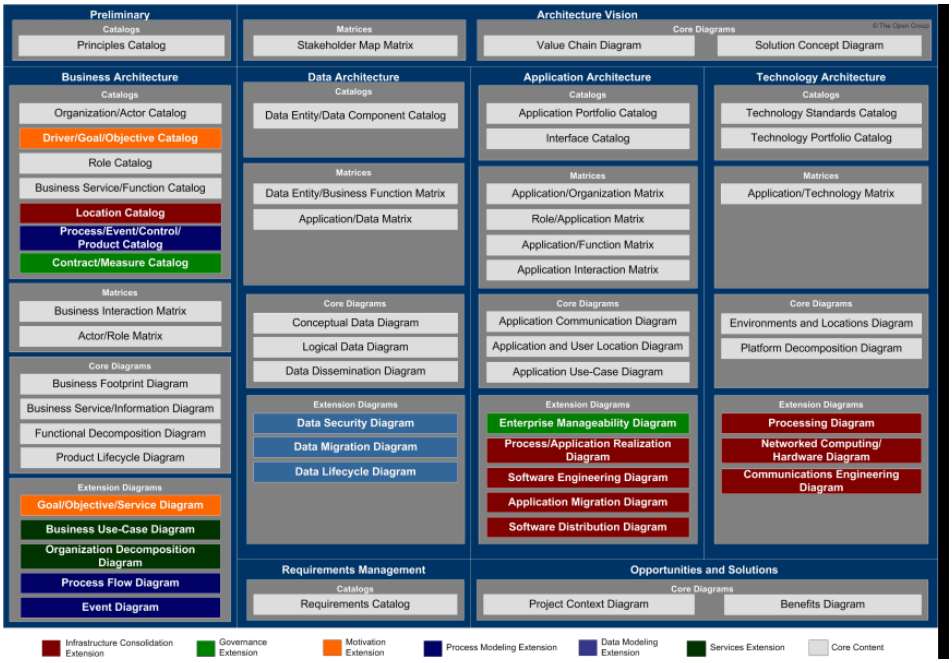

FIGURE 10. TOGAF ARTIFACT OVERVIEW

ESSENTIALS

As presented above, in their paper Winter and Fischer (2006) aim for capturing the essentials of Enterprise Architecture. Parallel to their set of layers, they also describe a set of essential artifacts. This list is not as extensive as the list provided by TOGAF, but still quite big. They distinguish a separate set of artifact that is used to represent the strategy of the business. In this layer a reference is made to other activities going on in the business. They enlist strategic projects and targeted market segments. This is something for which the other do not provide.

Strategy specification ("what" questions):

- hierarchy of organizational goals and success factors, product/service model (including partners in value networks), targeted market segments, core competencies, strategic projects, maybe business principles, dependencies between these artifacts

Organization/process specification ("how" questions):

- Specification of structure, Specification of behavior, Specification of information logistics and Dependencies between these artifacts, e.g. responsibilities, information requirements

Application specification (business IT alignment questions):

- Specification of applications and application components, Specification of enterprise services and service components

Software specification:

- Specification of software components, Specification of data resources, Dependencies between these artifacts, e.g. data usage by software components (CRUD)

Technical infrastructure specification:

- Specification of IT components, Dependencies between these artifacts

Specification of dependencies between layers, e.g.:

- Organizational goals/success factors vs. process metrics, Products/services vs. process deliverables, Organizational units vs. applications (ownership), Activities vs. applications, Activities/business processes/information requirements vs. enterprise services (orchestration), Applications/enterprise services vs. conceptual data entity types, Applications/enterprise services vs. software components (composition)

FIGURE 11. ESSENTIAL ENTERPRISE ARCHITECTURE ARTIFACT.

Another difference is the special section for the specifications of dependencies. Where most other choose to put these definitions with one of the architectural layers, the paper provides a separate category for them. However, (almost) all of the documents mentioned here are also present in the TOGAF specification. It seems like TOGAF specifies more documentation than needed in the essentials.

AN ARTIFACT MODEL FOR PROJECTS CONFORMING TO ENTERPRISE ARCHITECTURE

In this paper Foorthuis, Brinkkemper, and Bos (2008) describe the artifacts that are used in an EA project. Although the artifacts described in this paper are created in an EA project and not in the definition of the complete enterprise architecture, they are still worth mentioning. In this paper four artifacts are described that are not mentioned by others. The first one is the Business PSA. This artifact describes the boundaries of the business analysis phase at the start of the project and is a precursor of the PSA. The PSA provides all business and IT prescriptions that are relevant for the specific project. This is a subset of the full list of prescriptions that is available in the enterprise.

The other two notable artifacts are present at the end of an EA project. The Lessons Learned artifact is that collects improved practices. These can be improved based on new information or based on experience from this project. This artifact can be used as input for the next project. The EA Feedback Report is the other notable artifact. This artifact provides feedback to the Enterprise Architect about the application of the architectural principles and using the Enterprise Architecture services. This feedback is used to create better collaboration within the enterprise

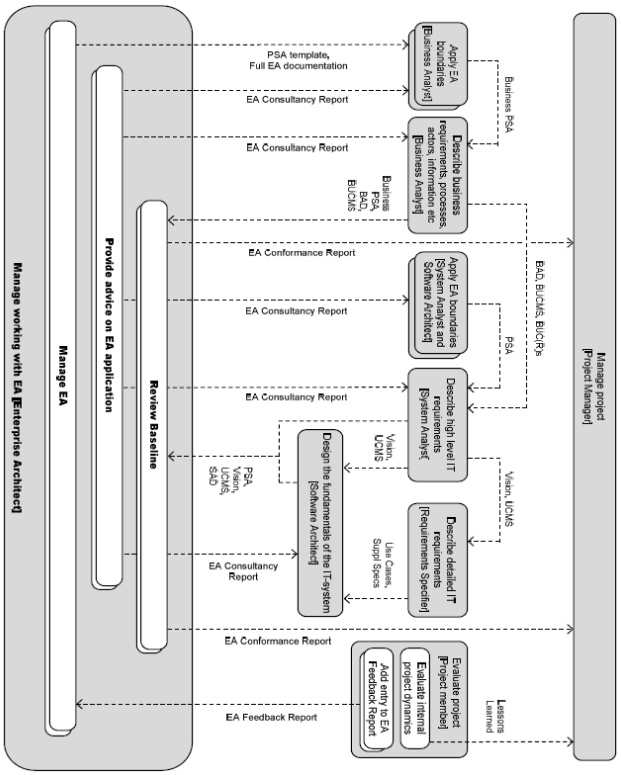

FIGURE 12. OVERVIEW OF ARTIFACT IN AN ENTERPRISE ARCHITECTURE PROJECT

2.3 Information Security

This thesis focusses on determining the level of Security in an organization. However, security comes in many forms. Some are very basic, like using a fire to scare away animals, some are more sophisticated. Nevertheless, they all have the same main goal: to provide protection from danger (Whitman & Mattord, 2011). These types of security can be placed in a variety of realms, e.g. Physical, Political, Monetary and IT (Wikipedia, 2014). In this thesis Information Security is selected as the type of security to be researched. This was chosen because Information Security spreads over all of the enterprise, just like EA, and focuses on the information assets present in the company.

But what is Information Security exactly? Just as with EA, there are many definitions available. The differences between these definitions are much smaller though. The afore mentioned book by Whitman and Mattord (2011) describes Information Security as follows: "*"Information security is*

the protection of information assets that use, store, or transmit information from risk through the application of policy, education, and technology.". The Information Assets in this definition can be very diverse. They can be logical object, such as computer files or websites, but also physical objects, like a printed document or a person (Whitman & Mattord, 2011).

The *International Organization for Standardization (ISO)* is the world's largest developer of voluntary International Standards (The International Organization for Standardization, 2014a). They provide standards on many different fields, one of them being Information Security. In their 27XXX series, the ISO describes many aspects of Information Security. They see Information Security as: "*preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information"* (The International Organization for Standardization, 2014b). This definition is completed by referencing other parts of the standard. Combining these element, the following definition would arise: *"The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable."* (Praxiom Research Group Limited, 2015).

Noteworthy in this definition is the explicit mentioning of *Confidentiality*, *Integrity* and *Availability* (CIA). These terms turn out to be very important in Information Security, as will be shown in the remainder of this section. Here these terms will be explained more extensively. Another notable difference between the two definitions is the mentioning of *accountable*. By doing this, the linkage between information and organizational entities is made. It does not only focus on the asset that needs to be protected, but also who is accountable for managing the asset and can be addressed if something is wrong.

The third standard nearly combines the definitions provided by the two standards mentioned above. The *National Institute of Standards and Technology* (NIST) describes information security as: "*Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide*

i) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
ii) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
iii) Availability, which means ensuring timely and reliable access to and use of information." (Paraphrased from Kissel (2013))

NIST has the same sort of technical view on InfoSec as Whitman and Mattord (2011) . It looks at the moves that can be made with information (assets) and describes a way for handling this in a sound manner. On the other hand, this definition also adopts the CIA approach as described by the ISO standard.

Another way of combining the mentioned views, is presented by the McCumber Cube (McCumber, 1991). This cube combines all aspects mentioned in the definitions above. It shows on the front that CIA should be ensured in as well storage as in processing information as in the transmission of information. This can be done by creating policies, educate all involved people and put in place the right technologies for doing this.

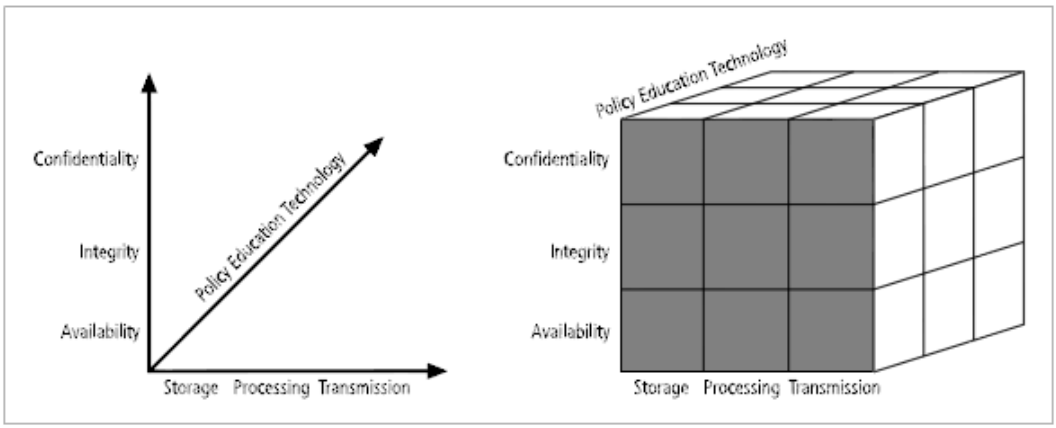

FIGURE 13. MCCUMBER CUBE (MCCUMBER, 1991)

There is one other thing that all views agree about on Information Security: It touches on many aspects of the enterprise. According to Whitman and Mattord (2011) the main ingredients for InfoSec are Software, Hardware, Data, People, Procedures and Networks. These items are all somehow addressed by the standards and definitions shown.

2.3.1 Frameworks and Standards

Like for Enterprise Architecture, there are a lot of frameworks and standards for Information Security. These standards and frameworks help in building a solid information security. In this section an overview of these tools is provided.

COBIT

The first framework to discuss is the *Control Objectives for Information and Related Technology* (COBIT) (ISACA, 2012) framework. The COBIT framework positions itself as the tool for information technology governance. This means it embraces a lot more aspects than just Information Security. It helps organizations in balancing IT risks and the investments needed in control. Because COBIT has a rich history in auditing, it is often preferred by IT auditors and IT risk managers (Von Solms, 2005).

Throughout the framework, information security is completely integrated. In their Professional Guide *Cobit 5 for Information Security* (REF), the creators of COBIT have filtered out all the relevant information for Information Security. The guide describes the enablers needed on every subject. This ranges from Principles & Policies to processes and from Information to Culture, Ethics & Behavior. In the remainder of the document COBIT offers some more detailed guidance on the covered subject. However, the level of detail is not always considered adequate. Von Solms (2005) states that a downside of this framework is that is sometimes lacks to answer the “how”-question. It states what should be done or paid attention to, but it does not prescribe any suggestions.

ISO 17799 & 27000 SERIES

Another well-known standard is presented by the ISO. The ISO 17799 (REF) is an international standard for Information Security introduced in 2000. The standard describes 10 sections of interest, which result in 36 objectives for information security (Saint-Germain & others, 2005). The objective can be placed into one of three categories (Figure 14): it is an Organizational aspect, a Technical aspect or a Physical aspect. In this the full width of information security can be recognized. The security measures need to be taken into account throughout the organization. This also goes for the levels within the organization. On the highest level, the organization needs to determine its security policies and these be implemented in the lower levels, as visualized in the

figure below. According to Von Solms (2005), the upside of using this standard is that more practical usability. It also provides quite good guidance on how to implement things.

In 2007, the ISO 17799 was incorporated in the new 27000 series and became ISO 27002. The series provides a best practice recommendations on Information Security. It provides these practices on the subjects of IS management, risks and controls. The scope of this standards is quite broad. This was done on purpose. By doing this, the standard is applicable on a variety of organization. The series as it is now consists of about 25 ISO standards, but based on recent developments, several additions are in preparation. Examples of these additions are the management of cloud systems and the handling of digital evidence (REF).

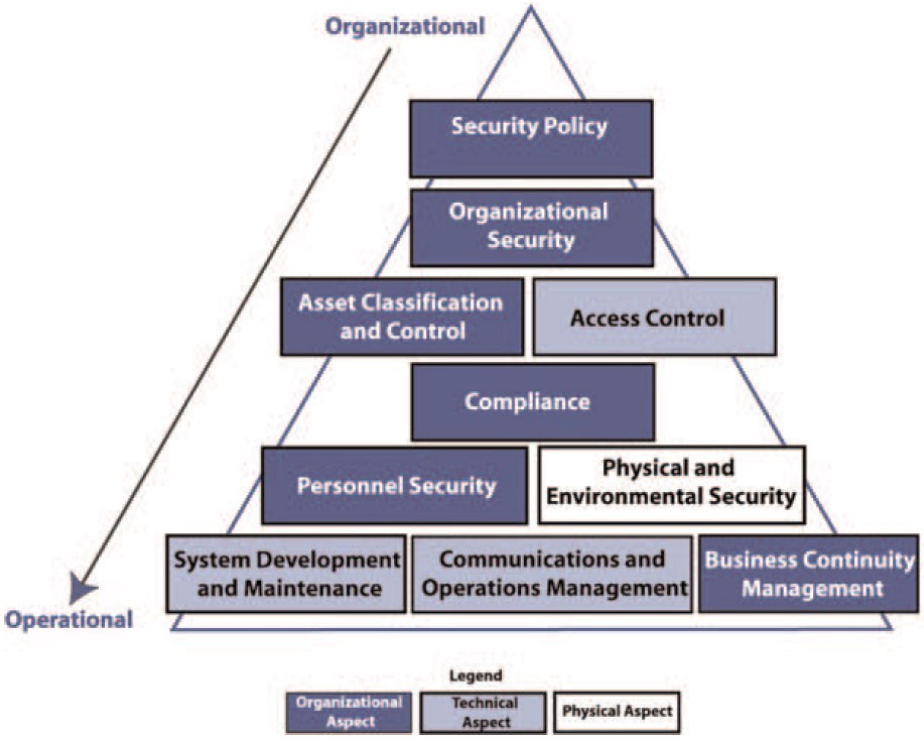

FIGURE 14. 10 DOMAINS OF THE ISO 17799

NIST

The third and last standard discussed in this section is the NIST. The NIST is a standard organization (REF) similar to the ISO. It is based in the US and provides standards in many different areas. One of them being Information Security.

In their NIST SP 800-100 (NIST, 2007) a handbook for Information is presented. The handbook *"provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program."* (NIST, 2007, p. 1). In many ways it is very similar to the subject described in the ISO standard. It looks into Information Security Governance, system development and Awareness & Training. Besides this, the handbook also discusses how to control the investments and system interconnections.

In a recent addition, the NIST created the NIST Cybersecurity Framework (NIST, 2013). As most of the information is stored and processed digitally these days, this is a very welcoming addition to this handbook. The framework helps in reducing a common problem; it makes the provided guidance more specific.

The NIST framework distinguishes five core functions: The Identification of risk, the Protection from risk, the Detection of incidents, the Response to incident and the Recovery from incidents (REF). For each of the functions, several categories are identified. These categories describe field that deserve attention when looking at this function. These categories are even further specified to a level of specific activities that should be undertaken.

These categories are derived from several other standards. The framework rests on standards created by the NIST itself, but also on the ISO 27000 series and COBIT 5. This makes the framework a selection of best practices from Information Security. In the use of this framework for the complete information security, it is required to interpret some of the requirements a bit wider than described.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

FIGURE 15. EXTENDED MATRIX SHOWING NIST CATEGORIES

2.4 Combining Information Security and Enterprise Architecture

There are already several initiatives looking into the collision of Enterprise Architecture and Information Security. A selection of these initiatives is discussed here.

One of the first attempts in making this step, is the Gartner EISA (Kreizman & Robertson, 2006). In this whitepaper, Gartner described how the inclusion of security requirements in the EA process and the addition of Security Experts to the EA team could help enterprises. They state that by doing this the security requirements would be much better embedded in the priority investments and solutions.

Based on the idea the SABSA framework is developed (Sherwood et al., 2009). The SABSA framework is based on the earlier mentioned Zachman framework. This framework has replaced the vertical viewpoints from the Zachman framework by Security Service Management aspects. SABSA consist of the framework and a method that guarantees the security of enterprise information. It does not explicitly mention EA elements, but it uses its structure and way of working.

A recent study performed by Van den Bosch (2014) presents an effort into the direction of bringing Enterprise Architecture and Security together. This research integrates the TOGAF standard (The Open Group, 2011) for Enterprise Architecture and the SABSA framework (Sherwood et al., 2009) for security. The research consists of three parts: (1) a framework, (2) a method and (3) a modeling language. Through executing the combined method, every step of the EA development process now also thinks of security. Combining this with the proposed extension for the Archimate modeling language (The Open Group, 2013), this research enables the modeling of security within the Enterprise Architecture.

Another initiative is the RISE method (Anderson & Rachamadugu, 2008). This method describes how an Enterprise Security Architecture. In this method three phases are acknowledged: Profile, Plan and Protect. In the Profile phase the as-is situation should be assessed for the risks that are present. In the Plan phase, the plan is created how to take away a part of these risks or mitigate them. This plan is then executed in the Protect phase.

In the paper *"Enterprise Architecting: Critical Problems"* Kaisler, Armour, and Valivullah (2005) also address security. They label security as a *"major concern in the building of an EA"*. According to this paper, the CIA triad needs to be considered in every part of the architecture. By providing a score based on the CIA triad, the component can be classified, assigning them a level of protection.

According to Pulkkinen, Naumenko, and Luostarinen (2007) the responsibility of an organization growth beyond its own enterprise. The protection of the confidentiality, integrity and availability of information is not only applicable to its own information. It should also take care of the information in the virtual enterprise it belongs to. EA is proposed as a comprehensive and coordinated tool for planning. By using EA, the planning of business and IT developments is combined.

The EA Grid	BA – security	IA – security	AA – security	TA – security
Enterprise level	Pursuing the remote maintenance services business as part of the services business portfolio Estimates of the business benefits for the partners Partnerships building with clients	User data managed centrally Product data (considered in the second phase of the security architecture) Security policies and guidelines for the enterprise	Applications to be secured: client site ERP's, workflow systems, automated control systems Applications at Metso: user data management and authentication provisioning system with SSO solution (Second step: extended to system of product data management)	Technology design for the security architecture Adoption of OASIS standards: the SAML v2.0, standard for SOAP messages 1.1 Security policy compliance checks Identity federation architecture with technical details (Fig. 1)
Domain level	Assign the system ownership of the identity and access management to a domain (e.g. the enterprise IM function) Roles of staff	Turning the high level policy statements to principles of managing user accounts Rights of the roles	Map of systems for services provisioning and IAM systems System use by roles	Map of the data communications connections Specify devices used by roles
Systems level	Business requirements for the systems (level of confidence)	Database schema for user data Role details	The ISA with interconnections and identity provision Patterns to be used in development; Developer guidelines	System-level technology architecture; technical implementation guidelines

FIGURE 16. SECURITY DECISIONS PLOTTED ON THE EA GRID

2.5 Discussion

As seen in section 1.3.6, this literature review is performed in order to (partly) answer three of the research questions. This section discusses what contribution the literature review has to the sub-question and how this information is used in this research.

The first goal of this review was to gather information on the possible descriptions of Enterprise Architecture. As presented in section 2.2, there are three ways Enterprise Architecture could be described for this analysis. The first option is to observe Enterprise Architecture by its development method (e.g. The Open Group (2011)). This method describes the activities of the enterprise architect in order to come to the enterprise architecture design. During this process, the subject of security should be addressed. The second option is to observe Enterprise Architecture by its framework (e.g. J. A. Zachman (1997)). In this framework, a description of the artifacts is provided. In these artifact descriptions, attention for security could be embedded. Looking at these descriptions is like looking at the outline of the actual documentation. The third and final option is to observe Enterprise Architecture by its documentation. This documentation is the outcome of the combination of process and framework. It is the actual description of the enterprise architecture. As presented in section 2.2.2, there are several types of documents that could be used to make this description. Which option (method, framework or artifacts) fits best for use in this research is decided during the solution design (section 3.1.1).

The second goal of this literature review was to gather information on the possible descriptions of Information Security. During the literature review, several standards were found to describe Information Security in this research. The first option is the COBIT standard (ISACA, 2012). Being known for its completeness and its reputation, this standards is often preferred by auditors. It is an integrated framework for IT management, which incorporates information security in all elements. However, it is not specifically meant for this. This can be seen in its high level descriptions of the requirements for the organization. Often this is a positive thing, as the auditor is given some room for interpretation. The same applies to the second option: the ISO standard (The International Organization for Standardization, 2014b). The standards presented by the ISO are widely known and used in many places of the world. In contrast to COBIT, this standard focuses completely on Information Security. Therefore, it presents a much higher level of detail the information security aspects. These details provide great guidance for the information security, but, as mentioned above, fail to address the *how*-question in several occasions. The third option for use in this analysis does not present this problem. The NIST framework (NIST, 2013) presents a high level of detail in the requirements it draws upon an organization. However, having its main focus on cyber security, use of this framework needs some caution. Which option fits best for use in this research is decided during the solution design (section 3.1.2).

The third goal of this literature review was to gather insight in the research field of combined Enterprise Architecture and Information Security. In this field, four types of initiatives were found. The first type of initiative focuses on the team composition. Kreizman and Robertson (2006) describe how the introduction of a security officer in the EA team can provide a more secure design. This, however, does not give any guarantees on the resulting architecture. The second type of initiatives provides guidelines for how to address security in the EA. Pulkkinen et al. (2007) describe how Enterprise Architecture can be used as a coordination tool for security initiatives. The application of the Enterprise Architecture approaches on Information Security development, results in a methodology that ensures *implementation control by integrating the processes and responsibility with enterprise-level portfolio management*. (Anderson & Rachamadugu, 2008). The third type of initiative is the SABSA framework (Sherwood et al., 2009). This framework and associated method describe the artifacts and steps needed to build an *enterprise information security architecture*. This framework is also used in the fourth initiative. Van den Bosch (2014) describes a framework, a method and a modeling language based on the integration of SABSA and TOGAF. These initiatives are used as guidelines and inspirational sources during the design process. How these are used is presented in section 3.2.

3 SOLUTION DESIGN: FRAMEWORK

The third phase of the research methodology is solution design. This chapter presents the development of the framework. This framework describes the relations between Information Security requirements and Enterprise Architecture artifacts. The framework was designed in two phases:

- Phase 1 (section 3.1): In the first phase, the concepts of enterprise architecture and information security are defined. This section explains the options that were considered and why the selected representation was chosen. Also, it explains the structure and elements of the chosen representation.
- Phase 2 (section 3.2): In the second phase, the relation between Enterprise Architecture and Information Security is determined. This section explains how the relation was defined, the choices made along the way and it presents the final result.

Based on this framework, the analysis methodology was designed. A description of this methodology is presented in Chapter 4.

3.1 Phase 1: Defining the concepts

As presented in the previous chapters, Enterprise Architecture and Information Security show clear similarities in their composition. Both try to define their field in terms of people, processes and forms of technology. This was seen by others as well (e.g. Van den Bosch (2014), Kreizman and Robertson (2006) & Sherwood et al. (2009)) and several views on the combination of these disciplines were established. However most of these combined views focus on a parallel development of EA and Information Security. As presented in the introduction of this thesis, this research focuses on the next step: Analyzing how well the integration of EA and Security has succeeded. In order to be able to define a relation and derive a method from these relations, suitable descriptions for both concepts are needed.

3.1.1 Enterprise Architecture

There are many enterprise architecture descriptions that can be used for analysis. For this research, we decided to analyze enterprise architecture by its artifacts. As seen in the literature review, other descriptions for enterprise architectures were available as well. These other description were also considered for usage in the analysis. However, they were deemed unfit for a number of reasons.

The first description that was considered, is the method by which the EA is developed. During the development of an enterprise architecture, the steps of the development method need to take security into account. Looking at the development method, e.g. the TOGAF ADM (The Open Group, 2011), can show the thoughts taken into consideration during the development process. However, thinking of security aspects does not necessarily mean incorporating them well. Just looking at the steps of the development method, will not provide a good inside in the incorporation of security in the architecture.

The second option considered for describing EA was the framework used during the development. In the framework (or taxonomy) the artifacts that need to be created are described (e.g. J. A. Zachman (1997)) . This is done in different level of detail, but these description have a very generic nature. For their intended use this is fine. The architects are allowed some space to find their own implementation of the artifact at hand. For this research however, the same problem as for the activities arises. The intention of a certain artifacts can be what is needed. Nevertheless, it is the

actual contents that determines its value. This is the reason why the frameworks were deemed unusable for the representation of EA in this research.

The third option for describing Enterprise Architecture was by its artifacts. The artifacts are the documents produced by the enterprise architecture process. These documents describe the enterprise in several ways. Overviews of different artifacts are, for example, presented by TOGAF (The Open Group, 2011) and Winter and Fischer (2006). The descriptions provided in the artifacts provide evidence to support the scores and conclusions from the analysis. An additional advantage of using artifacts, is in its transparency. The documents present the facts, decisions and results of the work that has been done. All undocumented intentions and thoughts are neglected. Based on these reasons, we decided to represent EA by its artifacts. Therefore, this research assumes: “If it’s not documented, it does not exist.”.

This assumption has two implications. First, the assumption helps focusing in on the main question. The goal of this research is to look at the incorporation of Information Security in the EA, not in the real-life organization itself. This involves removing the dependencies on specific employee skills or initiatives. If someone is to leave the organization, their tasks and roles in the enterprise need to be transferred to the successor. This is done through the description in the EA. Therefore it is necessary to measure how well it is documented here. Also, this separation of designed and actual organization allows for this analysis to be performed before implementation.

The second implication of focusing on artifacts, is in the application of the analysis. The assumption that was made, might create a gap between the analysis outcome and the real world experience. Depending on the maturity of the Enterprise Architecture and the adoption of it within the organization, the designed organization might differ from the actual one. There are three possible scenarios:

(1) The enterprise architecture is a perfect reflection of the organization; this will not create a gap.
(2) The organization has engaged in more activities than described by the architecture; this allows for a problem to be detected by the analysis that does not exist in reality.
(3) The organization has engaged in less activities than described by the architecture; this allows for problem to be undetected as it does not exist in the artifacts.

None of these scenarios has to be a problem. However, their existence has to be given attention when performing the analysis. When the analysis is used to screen the architecture, these scenarios are not important. The outcome of the analysis will strengthen the design of the enterprise. However, a problem could arise when the analysis results are used to improve the real-life organization. When an organization is in scenario 1, the improvements found in the design will also directly improve the actual organization. When an organization is in scenario 2 or 3, this is not necessarily the case. The analysis outcome might identify a problem that is not present in the real-life organization, or the other way around. Awareness of this problem is the most important part of avoiding it. Therefore the method shall address this.

As a next step, the actual artifact types for the description of enterprise architecture needed to be selected. As seen in the literature review, several framework provide structure to Enterprise Architecture. Notable here is the structure in which these frameworks and artifacts are structured. All frameworks define layers in which the organization could be split up. The layers are then used to structure the artifacts accordingly. This structure is maintained in this research.

Although the implementation of the layers differs between frameworks, there are certain similarities. All frameworks describe a layer which describes the people and their behavior, a layer

for information, data and applications and a layer for the technical implementation. This translates into the generic model presented in Figure 17.

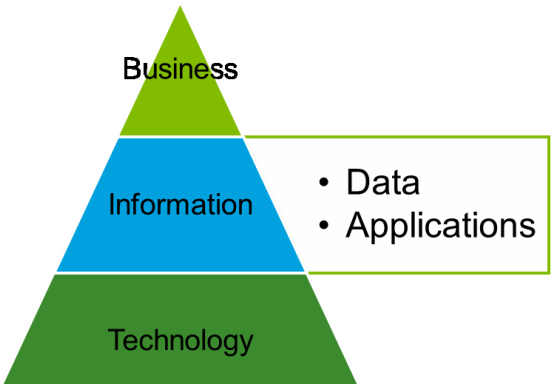

FIGURE 17. GENERIC ARCHITECTURE LAYERS

Although this is generic model, one division in framework needs to be explicated. A set of frameworks defines an information layer (e.g. Iyer and Gottlieb (2004)). This layer involves data and the tools needed in processing it. Another group of framework defines this in two different layers: The data layer and the application layer. An example of this separation is presented in the Zachman Framework (J. A. Zachman, 1997).

Literature does not provide evidence for the three or four layer layout to be better or more convenient. It seems to be a matter of opinion and they exist side-by-side. Even The Open Group is not consistent in their products. The Archimate modelling language (The Open Group, 2013) is defined using the three layers; thus using an Information layer. The TOGAF ADM (The Open Group, 2011) however uses the four layer structure.

For this research, we decided to adopt the four layer layout, thus splitting the information layer. This was done because this separation seemed useful. We believed that the requirements on the data could be significantly different from those on applications. The separation of these layers was believed to be helpful in providing insights in this difference.

We also recognized that some information in Enterprise Architecture does not fit one specific layer. An example of this could be the principles used to perform architecture. The experts and author believed that these layer transcending information could contain very useful input for the analysis. Therefore we defined that an extra, more general layer was needed.

Based on the layers defined, a great similarity with the TOGAF ADM structure was recognized. TOGAF defines the required layers as described above and also offers a more general overview layer. Therefore, we decided to adopt the layer structure provided by TOGAF (The Open Group, 2011). An additional advantage of adopting this standard, is the fact that it is widely known (according to the SMEs). Therefore most people will be familiar with the layers, thus having less trouble understanding them.

The layers are defined as follows (by TOGAF):

Vision

A succinct description of the Target Architecture that describes its business value and the changes to the enterprise that will result from its successful deployment. It serves as an aspirational vision and a boundary for detailed architecture development. *For this thesis the Vision is interpreted a bit wider. Some artifacts are defined in the process of the TOGAF ADM, but are not part of a specific*

architectural layer. For this research, these layer transcending artifact are housed in the Vision part of the framework.

Business Architecture
A description of the structure and interaction between the business strategy, organization, functions, business processes, and information needs.

Application Architecture
A description of the structure and interaction of the applications as groups of capabilities that provide key business functions and manage the data assets.

Data Architecture
A description of the structure and interaction of the enterprise's major types and sources of data, logical data assets, physical data assets, and data management resources.

Technical Architecture
A description of the structure and interaction of the platform services, and logical and physical technology components.

Based on these architectural layers the set of architecture artifacts was composed (presented in Figure 18). These artifacts were selected by picking the common denominators from various frameworks. This method was chosen for two reasons. The first reason is to exclude “exotic” artifacts. Every framework is designed with a certain focus and rational. This causes highly specific artifact to appear in some of the artifact lists. For example, Boster et al. (2000) mention *Market Research* as one of the deliverables from EA; a document that is not mentioned by any of the others. Keeping usability in mind, we argue that the method should be based on artifacts that are common in most organizations. Something that is accomplished by this selection method.

The second reason for picking this approach is applicability. The level of Enterprise Architecture within organizations varies. To make sure the solution is applicable in the majority of the organizations, the set of artifacts needed should be limited. When organizations start building their EA, they often will start with the core artifacts. The more specific documents will follow as they develop. One of the goals of this research is to take security in mind from the start (section 1.3.2). By making the solution applicable to early stage enterprise architecture, this goal can be achieved. This results in using the core artifacts, which are selected by taking the common denominator.

For the selection of these artifacts, the outcome of the literature review was used. The literature review on EA artifact provided the most relevant papers on this subject: The Open Group (2011), J. Zachman (2002), Boster et al. (2000), Winter and Fischer (2006) and Foorthuis et al. (2008). These papers were then compared in order to find the core artifacts of EA (see 0). In the decision of selecting an artifact for the further development, one criterion was used: The artifact is present in more than one of the papers. By using this criterion the most “exotic” artifacts were eliminated. It was assumed that the resulting set would still be too extensive. At this point however, it was impossible to determine which artifacts could be dismissed as well. Therefore all artifacts matching this criterion proceeded to the next phase. The outcome of this comparison is presented in 0. The selected artifacts are presented in Figure 18

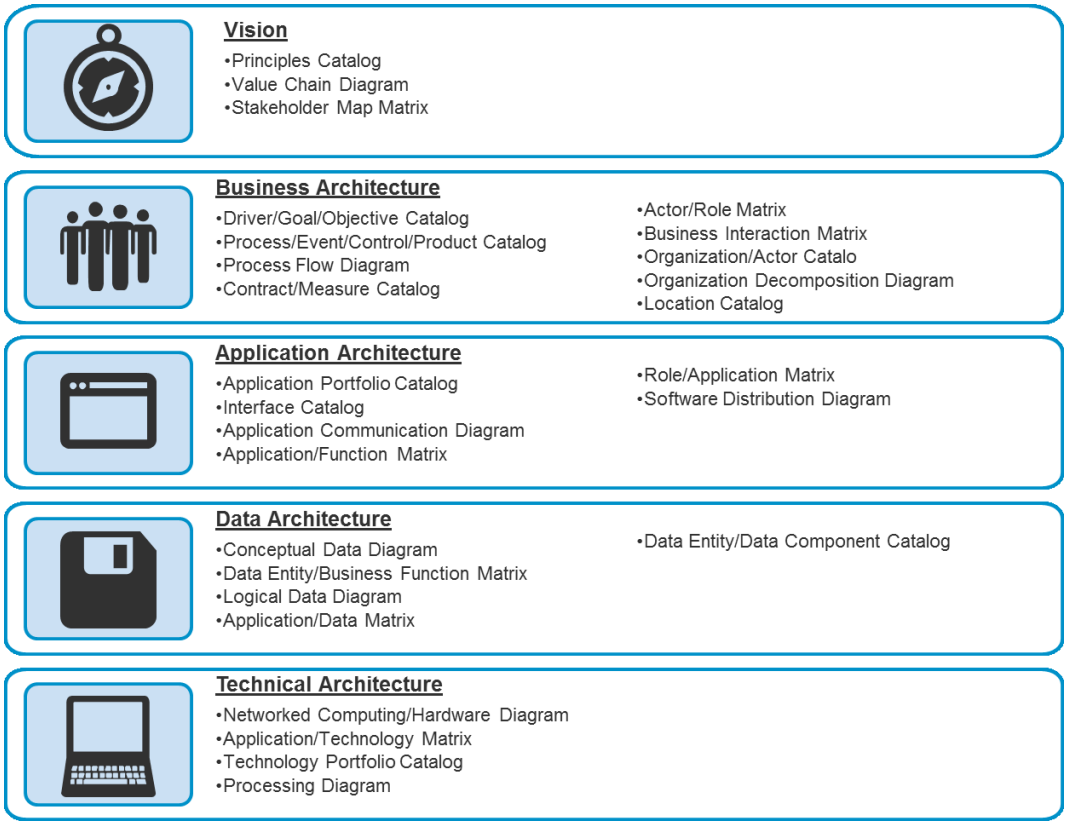

FIGURE 18. ARTIFACT SELECTION PER ARCHITECTURE LAYER

During this procedure, it was chosen to make TOGAF the leading standard. This was done for two reasons. Firstly, TOGAF is a widely approved standard that also offers an extensive overview of the artifacts used in documenting Enterprise Architecture. As TOGAF offers the most extensive artifacts overview of all papers, it was assumed that the artifacts mentioned in these paper could all be mapped to a TOGAF artifact. In the process this assumption was found to be correct. Second, TOGAF provides a clear definition with each described artifact. These definitions can be used in the method to make sure the right artifacts are used, even if they are named differently in the company at hand. This also allowed for pinpointing description given by various standard to one specific artifact. Again, this decision was based on usability and applicability for organizations in the future.

3.1.2 Information Security

In the current times, the nature of information is shifting from physical to digital. This trend is developing; more in some companies than others. Often heard slogans like *Clean desk policy* and *Paperless office* are stimulating this trend. Therefore it is necessary to represent information security in a way that supports this development. As presented in the literature review (section 2.3), several standards and frameworks could be used to describe Information Security. For this research, we decided to adopt the NIST framework and handbook.

For the description of information security three options were identiefied in the literature review. The first is the COBIT framework (ISACA, 2012). As an IT risk management framework, it provides insight in the actions needed to cope with the risks faced. Being a governance framework, it offers much more features than only ensuring Information Security. This is perfectly suitable for its intended use, however not for this research. Looking for the specifics of Information Security, this framework is to shallow on the details. As stated by Von Solms (2005), the framework sometimes

lacks to answer the “how”-question. Exactly the information needed in order to define the relations needed.

The second candidate was the ISO 27000 series. The ISO standard being wide recognized in Europe, this would have been a logical choice. Although the standard does not provide the lowest level of detail, it is much more practically usable than COBIT (Von Solms, 2005). Suggestion for implementation are provided, an addition which helps in the applicability. However, it was not yet detailed enough to define specific requirements for Enterprise Architecture artifacts. The ISO standard leaves some room for interpretation. This might be seen as an advantage during a normal audit, turned out to be a disadvantage here.

The final candidate is the NIST. Although the standard provided by NIST are not as widely known in Europe, they are by a large part of the world. This framework turned out to be perfectly suited for the development at hand.

For this research, a combination of two NIST products is used. The main building block is the *Cybersecurity Framework* (NIST, 2013). This recently developed framework provides detailed requirements on the organization. It was developed using a combination the ISO standard, NIST standard, COBIT and a set of others. Because of this solid basis and the involvement of many experts during its development, this framework is believed to be a solid representative for the security side of the framework. The concreteness of the requirements made it very useful for this research.

However, the framework is developed for cybersecurity. One might argue that this is not enough to cover information security. This problem was recognized during the selection procedure and dealt with in three ways. First, a large part of information security focuses on the digital information. Keeping in mind the trends described at the beginning of this section, this focus will probably be growing in the future. Therefore this problem should have little impact (according to the information security SMEs). Second, the focus of this framework suits Enterprise Architecture well. As EA focuses on the combination of business and IT, an important part of the architecture focuses on the linkage to the cyber realm.

The third way this risk was mitigated, was in the development method. By selecting Information Security experts for the development process, a broad view was kept. This resulted in the relation definition that was sometimes broader than one might expect from cybersecurity. To support this broad view on Information Security, the *Handbook for Information Security (NIST, 2007)* was consulted throughout the relation definition phase.

The functions of information security are defined by NIST as follows:

Identify
Develop the institutional understanding to manage (cyber)security risk to organizational systems, assets, data, and capabilities.

Protect
Develop and implement the appropriate safeguards, prioritized through the organization’s risk management process, to ensure delivery of critical infrastructure services.

Detect
Develop and implement the appropriate activities to identify the occurrence of a (cyber)security event.

Respond
Develop and implement the appropriate activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected (cyber)security event.

Recover
Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a (cyber)security event.

As stated in the literature review, the NIST standard describes five functions for information security. Within each function, there are several categories of activities that should be presented. These are presented more specific in the subcategories. An example of this is the following: According to the Identification function, Asset management should be performed (category).This is then specified by several subcategories which make it more practically useful, like *"Physical devices and systems within the organization are inventoried"*. The full specification of the NIST categories is presented in Appendix B. Figure 19 shows the activity categories that are defined per function.

FIGURE 19. NIST CATEGORIES PER FUNCTION

3.2 Phase 2: Defining the relations

In the next step, the goal was to find the relationships between Enterprise Architecture and Information. In order to find these connections, a mapping was performed. This was done by looking at a requirements from Information Security and see how Enterprise Architecture could fulfil this.

These relations were not determined solely by the author. During the development of the relations and methodology, several SMEs were involved. These SMEs were consulted during workshops and interviews. The nature of these sessions varied over time. In the first sessions, ideas about this research were shared and developed. As the development moved on, the sessions got more specific. How these sessions were used will be described in the next sections.

During this research four SMEs played a key role. Their experience and knowledge in the fields of Enterprise Architecture and Information Security served as key input for the author. A small profile of each SME is provided in order to provide insights in the domains covered.

Expert 1
Working on Architecture for nearly 20 years in different companies and fields. Has experience in all aspect of EA, from principles to technical implementation. In these assignments, security has played an important role several times. This expert also has provided the Informatiebeveiliging Jaarboek (Information Security Yearbook) with several contributions. His insight and years of experience provide insights in the field of Enterprise Architecture.

Expert 2
Active as a consultant for 4 years, this expert has done several relevant projects. For this research, his experience in incident management and his architecture focus within EA, were of great value. This expert recently co-authored a paper on Disaster recovery and Business Continuity, knowledge that was very relevant to the research.

Expert 3
This expert has almost 10 years of experience in the field of security consulting. Being certified as an Information System Security Professional and an Information Security Manager, this expert clearly has a lot of knowledge of the field of IS. Combining this knowledge with the experience gathered in various assignment, makes this expert a great source of knowledge.

Expert 4
This expert has about 10 years of working experience in different jobs. His jobs had a more technical profile and provide insights in the technical requirements on the enterprise. His knowledge of information security is also demonstrated by certifications as an Information System Security Professional and an Information Security Manager.

As can be derived from the profiles, the experts cover both fields very well. Interesting to notice is the cross field experience. During the introduction talks, it turned out that each expert had experience with the other field. The security experts had worked on architecture related subject, mainly security architecture. The architecture experts were familiar with the incorporation of security in their designs. A basic understanding of the other field, how limited it might have been, made the development process a lot easier.

One might argue that a group of four experts is rather small to cover both subjects. Although this is a valid concern, the group of experts present was considered covering. Combining their views and experiences in the field, most subject could be handled easily. The harder topics were handled carefully. They were left undecided during the meeting. In preparation for the next meeting, these topics were given special attention. If necessary, the SMEs would consult their colleagues that are specialized in this particular subject. This way possible knowledge gaps were mitigated.

Throughout the design process, several set of documentation were used to support the development. Besides the documentation on the chosen descriptions of Enterprise Architecture and Information Security, literature on the relations between the concepts was consulted. The SABSA framework (Sherwood et al., 2009) was used to gain insight in the needed descriptions for certain security aspects. These descriptions were then translated into measurable relations in the

framework. The research conducted by Van den Bosch (2014) was consulted to see how the integrated approach would work and which results could be expected as an outcome of this process. Finally, the idea presented by Pulkkinen et al. (2007) was kept as a guideline. While defining the relations in the framework, their idea of responsibility growing beyond its own enterprise was taken into consideration. This is also an important part of the Identify function in the framework.

3.2.1 Defining and testing the design process

During the introductory talks, the feeling arose that checking all requirements against all artifacts would be impractical. Firstly, because it would take an enormous amount of time. Secondly, it was assumed that for most requirements this was unnecessary. It was assumed that most requirements would be fulfilled with one or two artifacts. Checking all of them would result in an enormous job and most of the relations would stay empty. Therefore another approach was designed.

In a first iteration, for all requirements the relevant layer would be identified. Expectation was that this would result in one or two involved layers per requirement. If it was unsure what connection there would be, all layers would be selected. In the second iteration, the actual artifact would be appointed. Because the architectural layer was already determined, the set of artifacts that needed exploration would be limited. The third round would be used to specify the actual relation between the requirement and artifact.

To test this approach, a small test was performed. Ten random requirements were picked from the list and exposed to the designed approach. It turned out that the expectations were true. By first determining the architectural layer and then looking at the actual artifacts, the relations could be determined accurately.

For the creation of the mapping three types of relations were defined. If an artifact was not involved in meeting a requirement, this was represented by a " - ". If an artifact was involved in meeting the requirements, two types of relations could be appointed. The division was made based on the TOGAF definition of the artifact. In case the standard artifact, as defined by TOGAF, would provide the information needed it was marked as X(S). If the artifact needed a little extension in order to provide the information it was X(E).

3.2.2 Building the framework

The mapping as it is presented now, was not developed all at once. Throughout the creation of the mapping, several sessions with SMEs on both Enterprise Architecture and Security were held. These sessions were used for multiple purposes. First, all newly added assumptions and relations were discussed. These discussions started very openly and as the mapping got more completed, the discussions became more focused. Also the SMEs were asked to give their expectations for the relationships. When the SMEs disagreed, a small meeting was set up to achieve agreement. Through these iterations, the mapping was completed and agreed on (Figure 20).

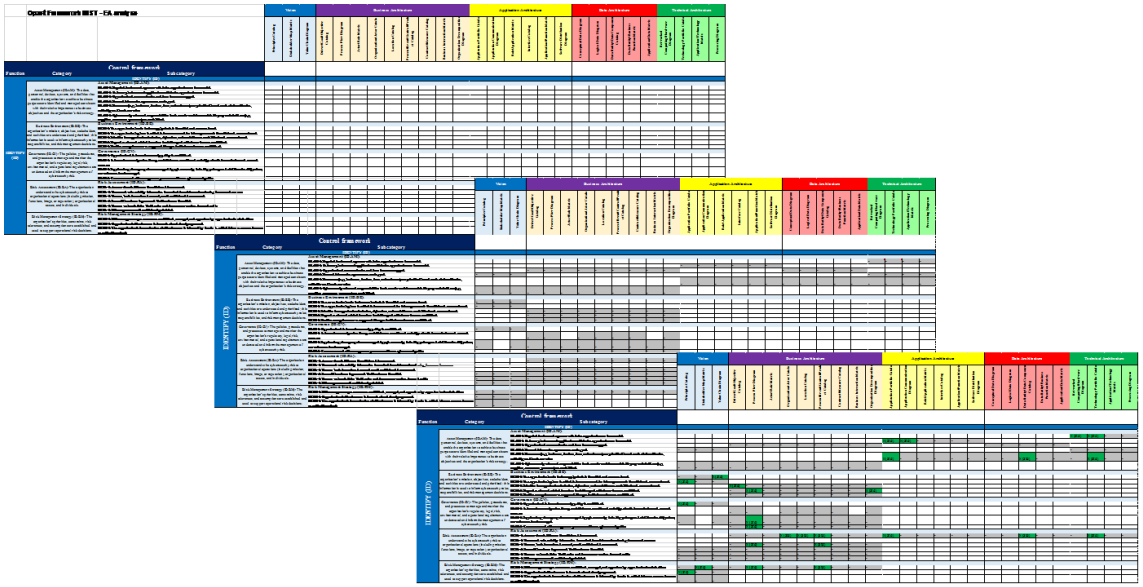

FIGURE 20. FRAMEWORK DEVELOPMENT PHASES

Goal of these iterations was to make the relations as specific as possible. For example, for one requirement to be met, a process is needed. This leads to an intersection with the process flow diagrams and the Process/Event/Control/Product Catalog. A relation stating a process should be in place, is to shallow to use for analysis. Therefore a more extensive description was created. For processes three items are specified: (1) What triggers the process? This can either be an event, a specific moment in time or another process. (2) Are there any milestones in the process that need to be met? These could be a certain step in the process or a decision on a specific subject. (3) What outcome should the process produce? This could be a document with certain contents or the triggering of another process.

A reoccurring discussion in the meetings was about the exact boundaries of Enterprise Architecture. This boundary was determined by making a parallel to building architecture. If looking at the security of a building, one might come up with the idea of an entrance portal. This is then turned into an architecture design. Both the idea generation and design of the solution are part of the architecture process. Once the design is implemented, the architect will check the solution one more time. This test makes sure everything is implemented as planned. When the portal is in use, the architect will not monitor its usage.

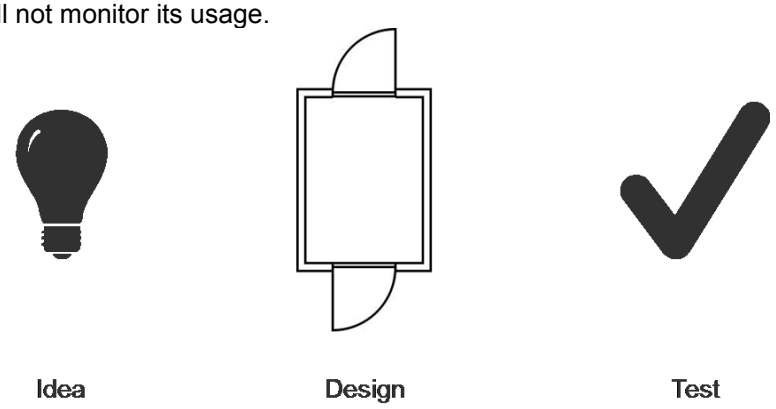

FIGURE 21. BOUNDARY OF EA

This example derived from building architecture can be applied to EA as well. Enterprise architects come up with several ideas and make design how these should be implemented. Once

implementation is finished, a final check is performed. This check assures the implementation is done according to specification. During usage, it might very well be possible that people deviate from the prescribed solution, which might lead to undesirable (side) outcomes. This, however, is no longer in scope of enterprise architecture. An enterprise architect is not considered with the continuous monitoring of the designs he made. The errors/deviations that occur are dealt with in the business of IT department. Of course these errors/deviations are used as input for the next iteration of Enterprise Architecture.

3.2.3 Revising the framework

During the SME sessions, some other interesting points were discovered. The first point of interest is in the empty columns. These columns turned out to have minimal influence in the representation of security in the Enterprise Architecture. This can be explained by the redundancy that is present in the TOGAF. Many aspects are represented in a catalog, matrix and diagram of some sort. When a combination of any of these three is used in this mapping, this gives multiple intersections. In some cases, the different intersections all have their own specific added value and are justified. However, in some cases the added value of one is nihil above the other one. In these situations the relation was concentrated on the smallest set of artifacts possible. This was done in separate iterations, to make sure none of the useful relations was removed.

The second interesting point involves the removed artifacts. In the first phase of the solution design, a subset of the TOGAF artifacts was constructed. During this process several artifact were dismissed from further processing. However, during the mapping several problems occurred. There seemed to be requirements that did not fit any of the selected artifacts well, but fitted precisely in one of the eliminated artifacts. During discussions with the SMEs all of these were traced back to just two artifact: the requirements catalog and the data security diagram. The requirements catalog did not make the first cut, because it is not specified as a layer artifact. This catalog is part of the complete ADM and therefore placed more centrally. It turned out to be of such great value to the developing analysis method, that is was decided to reintroduce the requirements catalog.

The data security catalog was dismissed during the comparison of frameworks. This diagram was only mentioned explicitly by the TOGAF. However many of the data related problems were covered by this diagram. Ignoring its existence would make the final verdict less trustworthy. Thus, although it is not described explicitly by multiple frameworks, it was reintroduced.

In order to provide insight in the meaning of the artifacts mentioned, a list of artifacts descriptions is compiled. These descriptions are based on the official definitions provided by The Open Group. However, in some cases additional assumptions about the artifacts were made. These assumptions are added to the official definitions to make one complete overview. This was done to facilitate the information gathering phase. All information about an artifact is now described in one place. The full list can be found in Appendix B.

By extending the artifacts definitions, the nature of some of the relations was altered. As described earlier, two types of relations were defined (X(S) and X(E)). The difference between these relations was based on an assumption that was added to the artifact. Now these assumptions became part of the definition, the relations all mean the same now. Therefore in the final matrix X(S) and X(E) were replaced with X. Figure 22 provides an overview of the constructed framework. In this figure, the involved artifacts for the fulfillment of a security category are shown. The full version of the matrix can be found in Appendix D. In this appendix, descriptions for each of the relations are provided as well. These descriptions state the content that is needed in an artifact in order to meet a requirement.

		VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTU			TECHNICAL ARCHITECTURE			
		Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control /Product Catalog	Application Portfolio Catalog	Application Communication	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Function	**Control framework Category**																		
IDENTIFY (ID)	**IDENTIFY (ID)**																		
	Asset Management (ID.AM)					x				x	x			x		x	x		
	Business Environment (ID.BE)	x	x	x	x	x	x												
	Governance (ID.GV)	x		x		x	x		x										
	Risk Assessment (ID.RA)					x			x	x	x								
	Risk Management Strategy (ID.RM)	x	x			x			x										
PROTECT (PR)	**PROTECT (PR)**																		
	Access Control (PR.AC)					x	x		x		x	x			x	x	x	x	
	Awareness and Training (PR.AT)					x			x										
	Data Security (PR.DS)	x		x		x		x	x				x	x		x	x		x
	Information Protection Processes and Procedures (PR.IP)	x		x		x			x	x									
	Maintenance (PR.MA)			x			x												
	Protective Technology (PR.PT)	x		x		x	x		x	x		x			x		x		
DETECT (DE)	**DETECT (DE)**																		
	Anomalies and Events (DE.AE)			x		x	x		x	x									
	Security Continuous Monitoring (DE.CM)					x	x		x	x	x	x				x			
	Detection Processes (DE.DP)			x		x	x		x										
RESPOND (RS)	**RESPOND (RS)**																		
	Response Planning (RS.RP)					x			x										
	Communications (RS.CO)	x				x	x		x										
	Analysis (RS.AN)					x			x										
	Mitigation (RS.MI)					x			x										
	Improvements (RS.IM)					x			x										
RECOVER (RC)	**RECOVER (RC)**																		
	Recovery Planning (RC.RP)			x															
	Improvements (RC.IM)			x		x			x										
	Communications (RC.CO)		x			x			x										

FIGURE 22. SUMMARIZED FRAMEWORK

4 SOLUTION DESIGN: METHODOLOGY

The third phase of the research methodology is solution design. This chapter presents the development of the methodology. Based on the on the framework presented in Chapter 3, a methodology for performing the analysis is presented. De design of this methodology is guided by the methodology goals (section 4.1). In section 4.2 the methodology is described step by step. For each step, a rational is presented, a number of alternative methods is suggested and the expected outcome is described.

4.1 Methodology Goals

As described by Peffers et al. (2007), objectives for the solution need to be determined. These objectives serve as guidelines for the design process. In this research, the solution objectives are formulated as methodology goals. These methodology goals were formulated during a workshop with the involved SMEs. We believe that by achieving all goals, a solid analysis method is derived that will fulfill the main research goal.

Goal 1: Provide Enterprise Architects with a method for determining the security level of the Enterprise Architecture.

This goal is the main goal of this methodology and at the same time the main goal of this whole research. However, the methodology should not only be usable for security officers. This drawn extra requirements on the definition of the relations.

Goal 2: Provide insights in the requirements drawn upon Enterprise Architecture by Information Security.

The methodology will be built upon the relations between EA and InfoSec. These relations need to be determined as a basis for this research. The methodology will make clear what is expected from the Enterprise Architecture from an Information Security standpoint.

Goal 3: Determine the overall security level of an Enterprise Architecture.

By providing insight in the fulfillment of each requirement, insight are provided in the state of the integration. The method should be able to determine an overall score for the architecture. Hereby allowing comparison over time and potentially assigning maturity levels to the scores.

Goal 4: Determine the weak spots in the Enterprise Architecture from a security standpoint.

Besides presenting an overall score, the methodology shall also be able to present weak spots in the Enterprise Architecture. By adding this goal, the methodology will provide more insights on this subject. This will allow for better development choices.

Goal 5: Whenever possible the methodology will make use of existing methods.

Using existing methods has two clear benefits. Firstly, the method have proven themselves and therefore don't need additional validation. These methods can be selected based on prove from science, but also from practice. The *best practices* are often known by experts and have earned recognition. Secondly, existing metrics are already known in the organizations. By using existing methods, the methodology will be easier deployable and reduce the chance of incorrect execution.

4.2 Methodology Description

Based on the earlier established relation between EA artifacts and Information Security requirements, a methodology (Figure 23) is designed. The methodology will serve as a guideline for assessing the level of Information Security secured in the Enterprise Architecture. In this section, the steps of the methodology will be described and explained.

All process models shown in this section are created with Bizagi Modeler (Bizagi, 2015). For each step, a sub-process model is presented in the corresponding section.

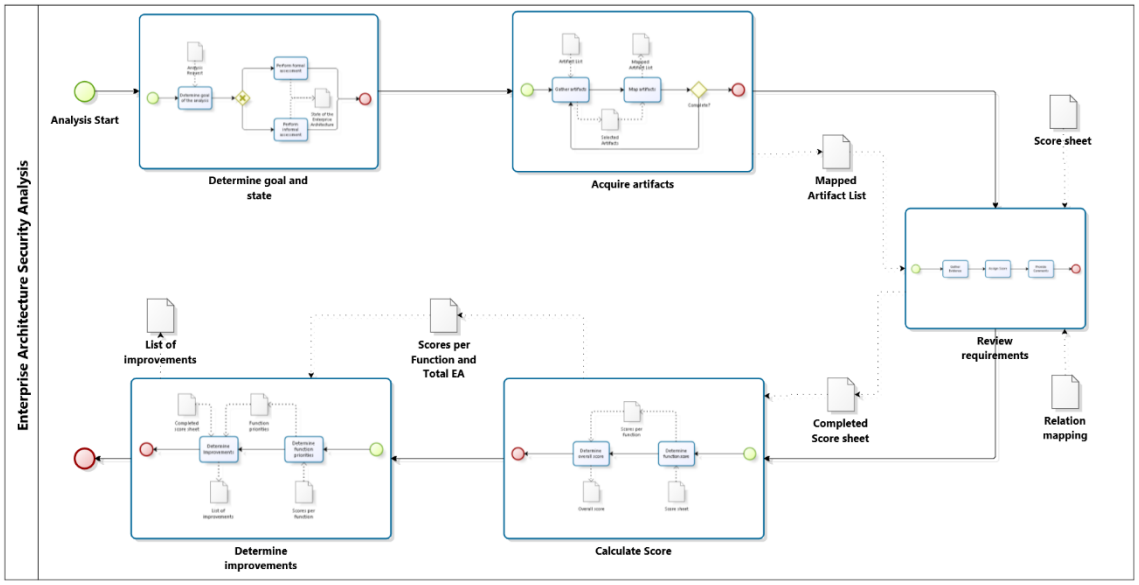

FIGURE 23. OVERALL METHODOLOGY DESCRIPTION

The steps are described using the structure shown by Wielstra (2014). Each step of the methodology consist of one or more tasks. The description for each of these tasks consists of three parts:

1. **Approach**: This parts explains the rationale behind each step. It explains the goal of the task and what's its role in the methodology.
2. **Method**: For each task, a number of alternative methods is suggested. These suggestions are based on literature, but also on best practices. During the development of the methodology, the SMEs were consulted to provide methods for certain activities. While executing this step in the methodology, one of the methods can be used to perform the task. In some situations, it might be useful to combine two or more methods.
3. **Deliverable**: Describes the expected outcome of a task. It provides insight in the form and contents of a deliverable. Most tasks result in an outcome that provides input to another task.

In the remainder of this section, each step is described using this structure. In these descriptions, the person performing the analysis is referred to as the analyst.

4.2.1 Step 1: Determine State and Goal

As stated in section 3.1.1, the first step of the methodology is looking at its context. When the analysis is used to screen the architecture, the difference between the design and the real-life organization can be neglected. The outcome of the analysis will strengthen the design of the enterprise. However, a problem might arise when the analysis results are used to improve the actual organization. When there is a difference between the design and real-life organization, the

wrong conclusion might be drawn. The analysis outcome might identify a problem that is not present in the real-life organization, or the other way around. Awareness of this problem is the most important part of avoiding it. Therefore the goal of the analysis and the state of the architecture influence the interpretation of the analysis results (Figure 24).

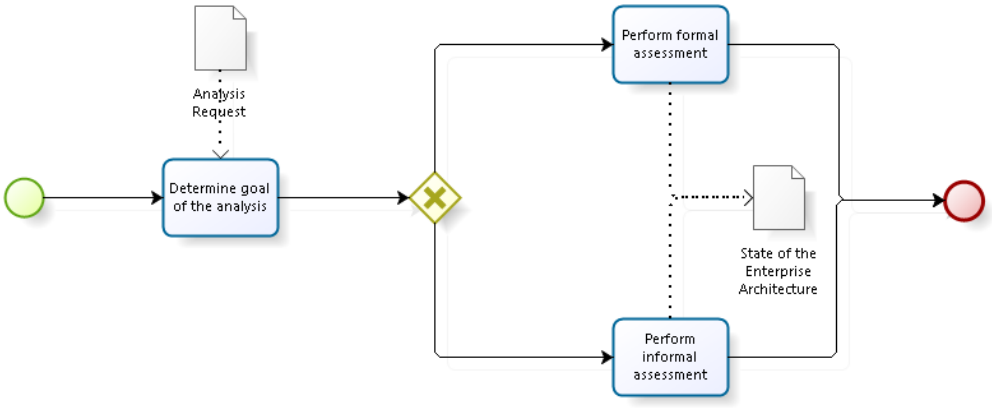

FIGURE 24. PROCESSMODEL STEP 1

DETERMINE GOAL OF THE ANALYSIS

APPROACH:

As stated before, the state of the architecture influences the outcome of the analysis. In order to determine how the outcome of the analysis will be used, the goal of the analysis should be known. This task focuses on finding out whether the results are believed to represent the real-life organization. If this is the case, a formal measurement on the state of the EA is needed. When the analysis is used to test the architecture, a more informal state description will suffice.

METHOD:

ANALYSIS REQUEST: In the request for starting the analysis, the goal might be explicated. The explanation provided with the request might provide enough information. If this is not the case, the interview method should be used.

INTERVIEW: In order to gather the needed information, a small interview could be conducted. The interview should be conducted with the requester. The goal of the interview is to discover the intended use of the outcome. This information is used to choose the right assessment method.

DELIVERABLE:

DECISION ON ASSESSMENT METHOD: When the goal of the assessment is determined, a decision on the next step can be made. If the outcome will be used as representation of the real-life organization, a formal assessment of the enterprise architecture should be conducted. The exact difference with the enterprise architecture will play an important role in the interpretation of the results. If the analysis is used to scan the architecture for improvements, an informal assessment should be conducted. This information will help in determining the reasons for the assigned scores.

PERFORM FORMAL ANALYSIS

APPROACH:

This task will be performed when the outcome will be used as if it represents the real-life organization. To make sure the analysis results are not distorted by shortcomings in the EA

practice, a formal assessment should be performed. This assessment will also provide insight in the gap between the designed organization and the actual one.

METHOD:

EA MATURITY ASSESSMENT: In the field of Enterprise Architecture, measuring the state of the enterprise architecture is a common phenomenon. This measurement is called a maturity assessment. It focuses on the capabilities of the EA department and the work it does. There are several method for performing a maturity assessment. Each of them might have slightly different focus, but there are certain core elements. Based on an analysis of several elements, Lankhorst (2005) provides a generic model for EA maturity (Figure 25)

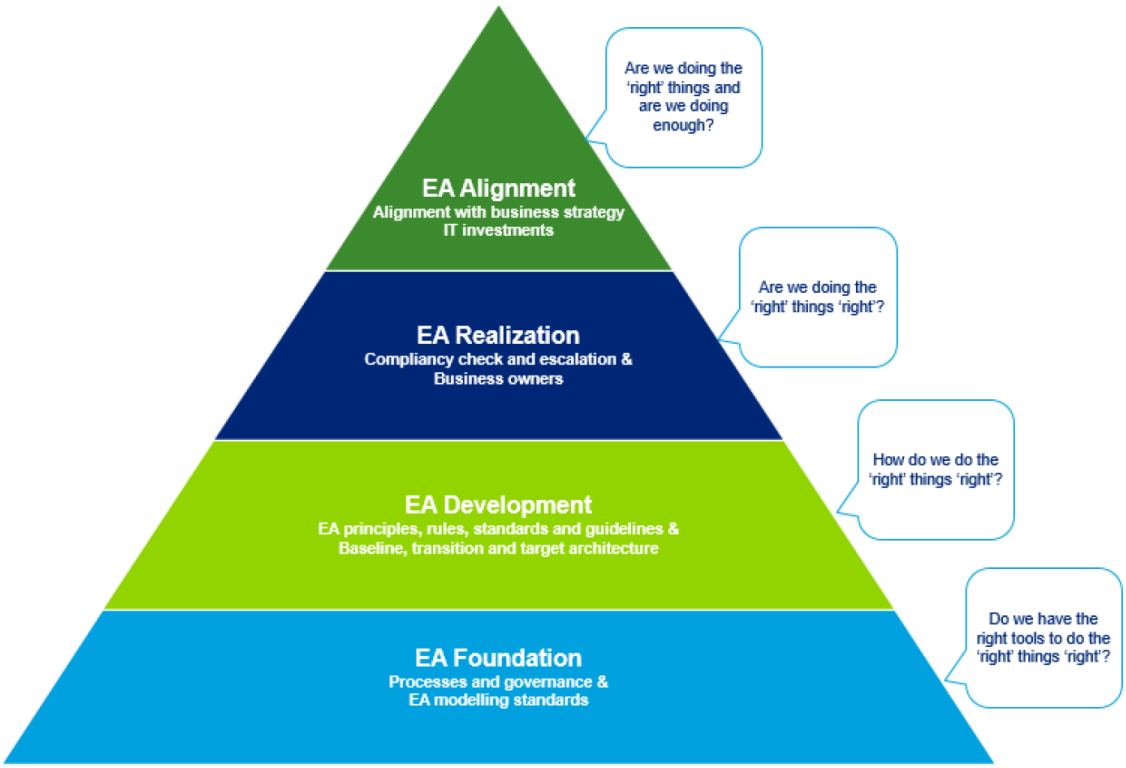

FIGURE 25. GENERIC MATURITY MODEL (VISUALIZATION BY ROEST (2013))

According to this model, EA maturity consists of four parts. A short description is provided based on Roest (2013)The EA foundation looks at the base of the EA department; are all processes and standards in place to perform enterprise architecture? The EA Development looks at the usage of the processes and standards establish in the foundation; are the tools from the foundation put to good use and are EA plans developed according to them? EA Realization is about the actual execution of the plans; Are we doing the things as we should? The EA Alignment enables alignment between IT and the Business Strategy and thus answers the question:" *Are we doing the 'right' things and are we doing enough?"(Roest, 2013)*.

Based on these maturity models, an assessment can be performed. On which model the assessment is based is up to the analyst. Based on experience and current practice within the company, a suitable assessment method can be picked.

In this task, there is a difference in importance for each of these aspects. The EA Foundation, Development and Realization are the most important for this task. These provide a view on how well the EA is managed and how well it does represent the state of the enterprise. Statements on the alignment can be considered bycatch.

DELIVERABLE:

STATE OF THE ENTERPRISE ARCHITECTURE: This document shortly describes the state of the architecture. It shall at least provide a statement on the completeness of the documentation, the quality of the documentation and the expected accuracy of the documentation.

PERFORM INFORMAL ANALYSIS

APPROACH:

This task will be performed when the analysis is used as a scan of the designed organization. To make sure the analysis results are not distorted by shortcomings in the current EA documentation, an informal assessment should be performed. After all, the outcome of the analysis is influenced by the quality and completeness of the EA documentation. Performing the analysis on an up-to-date and maintained architecture will probably provide most useful insights.

METHOD:

For this step, three methods are suggested. Each of them provides an equally usable outcome. However, based on geographical location, time and resources, organizations might prefer one over the other.

INTERVIEW: The quickest method for performing this analysis is conducting a small interview with one or more architects. As this is their daily job, they can provide a lot of information on the available materials. Naturally, this method is easily influence by the opinion and knowledge of the architect at hand. Therefore conducting multiple interviews will provide a better insight in the state of the architecture.

QUESTIONNAIRE: This method is based on the interview method. It allows you to ask the same question to multiple people at once. This will make it easier to approach a bigger group. However, the possibility to address an answer is blocked by this method.

WORKSHOP: This method will help overcome the personal biases. By discussing the state of the enterprise architecture with a group of experts, a more balanced view can be produced. Personal opinions are consolidated by the discussion and the possible knowledge gaps are mitigated by using the combined knowledge of the experts.

DELIVERABLE:

STATE OF THE ENTERPRISE ARCHITECTURE: This document shortly describes the state of the architecture. It shall at least provide a statement on the completeness of the documentation, the quality of the documentation and the expected accuracy of the documentation.

4.2.2 Step 2: Gather Artifacts

In order to start the analysis, the artifacts need to be collected. This is done in the second step (Figure 26) in the methodology.

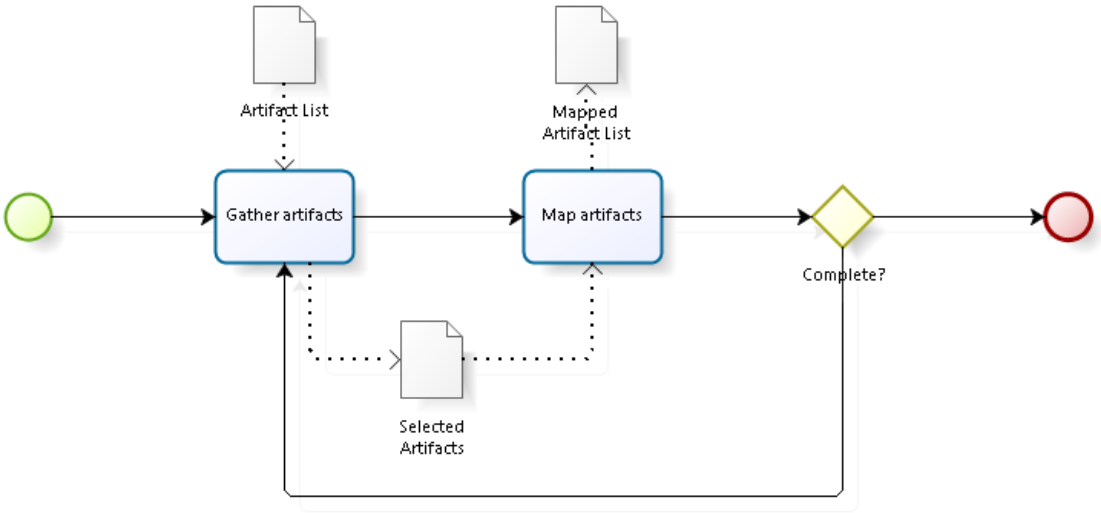

FIGURE 26. PROCESSMODEL STEP 2

GATHER ARTIFACTS

APPROACH:

Basis to this analysis is a set of EA artifacts. These artifacts are described in the artifact list (Appendix B). This list can be used to gather all the needed information. There are three ways of performing this task. Based on security clearance and familiarity with the architecture repository, one (or a combination) of these methods need to be performed.

METHOD:

REQUEST ARTIFACTS: This method will be primarily used by analysts outside the EA team. For these analysts, access to the artifacts and knowledge of the repository is probably limited. Requesting the documentation from an EA team member solves these issues. The request can be done based on the provided artifact list.

PERFORM SEARCH: This method will primarily be used by analysts inside (or very close to) the EA team. As their knowledge of the EA documentation and repository is sufficient, gathering of the artifacts can be performed by the analyst. When a document is unknown to the analyst or cannot be found, he/she can divert to one of the other methods.

COMBINED SEARCH: This method is a hybrid form of the previous methods. In this form, the analyst and a SME will search together. There are two key benefits to this method. First, the chance of misinterpretation is smaller. When requesting the documentation, the possibility of misinterpreting the artifact is present. By searching together this problem is detected immediately. Second, this methodology can also be used when security clearance is insufficient. This might enable the possibility for accessing classified documents, without actually transferring them.

DELIVERABLE:

SET OF SELECTED ARTIFACT: The output of this task is a set of artifacts which is believed to provide the necessary information. If an artifact is not available in the organization, this should be communicated as well.

MAP ARTIFACTS

APPROACH:

In order to perform the analysis, an overview of the available content is needed. Therefore the acquired documents are mapped to the artifacts described in the artifact list. This will enable efficient searching in the next step. It also provides insights in the completeness of the provided set.

METHOD:

COMPARE AND LABEL: In order to perform this task, as basic method is used. Each of the selected documents should match one of the artifacts described in the list. By performing a quick scan on the document, it should be possible to label the artifact.

It is very well possible for a document to provide information on multiple of the expected artifacts. A basic example is a document in which the application landscape is provided as a diagram and a description of the elements. A document of this type will then represent two artifacts; in the example this would be the application communication diagram and the application catalog.

DELIVERABLE:

SET OF MAPPED ARTIFACTS: This set (or list) will provide insight in which organizational documents correspond to the expected artifacts. If for each expected artifact at least one representative is found, the list is marked complete. If not, some further information gathering is needed.

Artifacts being marked as unavailable, should not be considered in the decision to continue. If the artifact does not exist, the analysis can continue. This will be reflected in the outcome.

4.2.3 Step 3: Review Requirements

In this step, the architecture is analysed for each requirement presented in the framework (Appendix D). This step (Figure 27) consist of three tasks. First, evidence for each of the requirements is gathered from the provided documentation. Second, a conclusion is formed based on this evidence. Finally, a rational for the drawn conclusion is provided in comments.

The implementation of these tasks is highly dependent on each other. Therefore, the tasks are combined in the provided methods (shown below). Each method describes the combined implementation of the three tasks.

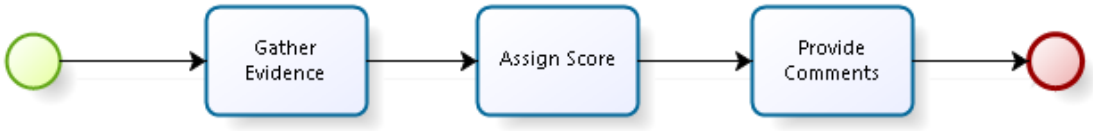

FIGURE 27. PROCESSMODEL STEP 3

APPROACH:

In this step the actual analysis is performed. Basis for the analysis is the framework built in the first phase of the solution design. For each of the requirements, evidence is gathered to show to which extend it is met. Based on the degree to which the requirement is met, a score is provided. This score might come is different forms, depending on the method used. To support the score, comments should be added to explain why this score is assigned. A score sheet (Appendix E) is provided for guidance during this step.

METHOD:

OBSERVING: This qualitative method will not provide a verdict in numbers. Each requirement is subject to a small research. In this research evidence for the fulfillment of requirement is searched for. This is done based on the previously defined relations (Appendix D). Evidence for the fulfillment of a requirement is noted, as are shortcomings that are found. The method however does not provide a scoring in word or number.

SCORING: This qualitative method will provide a verdict in numbers. Each requirement is subject to a small investigation. In this research evidence for the fulfillment of requirement is searched for. This is done based on the previously defined relations (Appendix D). Based on the evidence found, a score is assigned to the requirement. Based on the methodology as it is now, a 3-point scale is suggested:

0. This requirement is not or barely fulfilled by the architecture artifacts.
1. The requirement is partially fulfilled, but not all the expected elements are addressed.
2. The requirement is (almost) fully fulfilled.

One could argue this three point scale lacks refinement. However, this fits the current state of the methodology. The usage of a more detailed scale would suggest a level of accuracy that is not yet present. When the methodology develops, a more detailed scaling could be valuable.

QUANTITATIVE ANALYSIS: Enterprise Architecture often makes use of models. These models could be used to perform a quantitative analysis. Although a tool for this analysis is not yet present, the following research illustrates how this could be done.

This approach is described by Johnson, Lagerström, Närman, and Simonsson (2007). In this paper a formal language is proposed to support the analysis of enterprise architectures. The paper describes an example based on the ISO 17799. The language described is called the Extended Influence Diagram. It is based on the Influence Diagram, of which an example is provided in Figure 28.

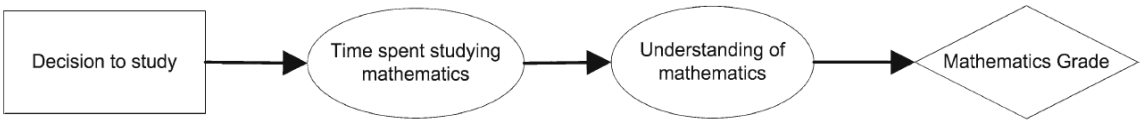

FIGURE 28. INFLUENCE DIAGRAM EXAMPLE

The language as it is now is capable of comparing scenarios based on defined measurement points. If the framework designed in this research would be expressed in this language, this could be used in a tool. This would allow for quantitative analysis based on this research. However this would require all relation to be defined in a binary form. This is (not yet) the case.

DELIVERABLE:

COMPLETED SCORE SHEET: Following one of the methods, a completed score sheet is created. This sheet provides an overview of the scores for each requirement. This scores is based on the evidence found in the documentation.

4.2.4 Step 4: Determine Score

When a score is assigned to each requirement, scores for the functions and complete architecture can be determined. As described in the methodology goals (section 4.1), these scores can be used to provide insights in the architecture. Therefore the scores per function and the overall score are determined separately (Figure 29).

Whether a score is satisfactory or unsatisfactory varies per organization. Therefore scoring on this type of scaling is avoided. Organization could assign scores to e.g. adequate - fair – poor scales.

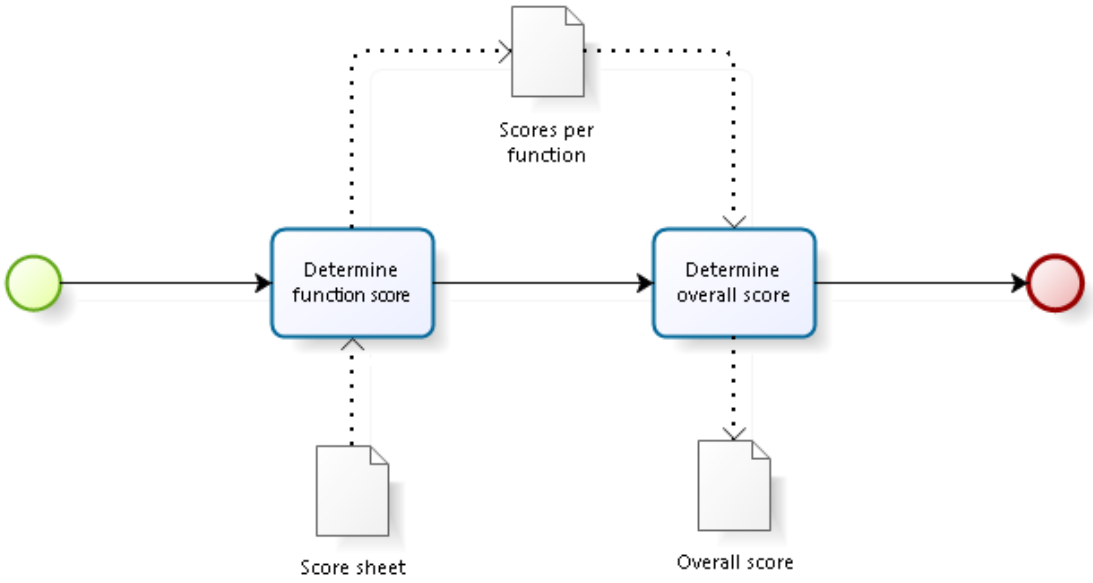

FIGURE 29. PROCESSMODEL STEP 4

DETERMINE FUNCTION SCORE

APPROACH:

As part of the methodology goals and the overall research goal, an expression of the level security in the architecture is determined. This is done by first looking at each of the NIST functions. Looking at the scores provided with every requirements in the function, a scores for the complete function can be created. This is done for each of the five functions. For the composition of these score, several methods can be used.

METHOD:

GENERAL OBSERVATION: If the observation method is chosen in Step 3 (section 4.2.3), this method would be the only possible next step. The comments placed on the requirements need to be observed. Based on these comments, a general observation for each function is formed.

If one of the other methods was chosen in the previous step, this method could also be used. Based on the findings and the scores for each requirement, function level observations can be derived. This, however, will change the quantitative methods in qualitative outcomes.

PERCENTAGES MEASUREMENT: This method cannot be used if the observations method is used in the previous step. In this method, the scores are determined by looking at the points acquired versus the amount that could be scored. This is expressed in a percentage. These percentages provide insight in the functions performance and can be used in determining the overall architecture score.

LOWEST SCORE: This method cannot be used if the observations method is used in the previous step. In this method, the function score is determined by the lowest requirement score in the

particular function. When using this method, a more detailed scoring scheme (than the one suggested) might provide better insights.

This method is much stricter than the previous one. It is based on the principle of *a chain being as strong as its weakest link*. The scoring provided by this method shows the minimal score of each function.

DELIVERABLE:

SCORE PER FUNCTION: The deliverable of this task is a score per function. The form of this score varies per method.

DETERMINE OVERALL SCORE

APPROACH:

As part of the methodology goals and the overall research goal, an expression of the level security in the architecture is determined. This is done by looking at the scores of each of the functions. Looking at the score of each function, a verdict on the complete architecture can be formulated. This can be done using various methods.

METHOD:

GENERAL OBSERVATION: If the observation method is chosen in Step 3 (section 4.2.3) or the previous task, this method would be the only possible next step. The observations made on each of the functions needs to be observed. Based on these observations, a general observation for the complete architecture can be formulated.

If one of the other methods was chosen in the previous step, this method could also be used. Based on the findings and the scores for each function, architecture level observations can be derived. This, however, will change the quantitative methods in qualitative outcomes.

PERCENTAGES MEASUREMENT: This method cannot be used if the observations method is used in the previous step. Following this method, the scores are determined by looking at the points acquired versus the amount that could be scored. Doing this based on the scores provided per function, will result in the score for the overall architecture.

LOWEST SCORE: This method cannot be used if the observations method is used in the previous step. Same as for the function score, in this method the lowest score determines the score. The function that has achieved the lowest score, determines the score for the complete architecture.

DELIVERABLE:

Overall score: The deliverable of this task is a score for the overall architecture. The form of this score varies per method.

4.2.5 Step 5: Determine improvements

Based on the previous steps, recommendations for further improvement can be derived (Figure 30). The recommendations are based on the scores assigned to different requirements and functions. If the purely qualitative observation method was chosen in the previous steps, this step will be harder to perform.

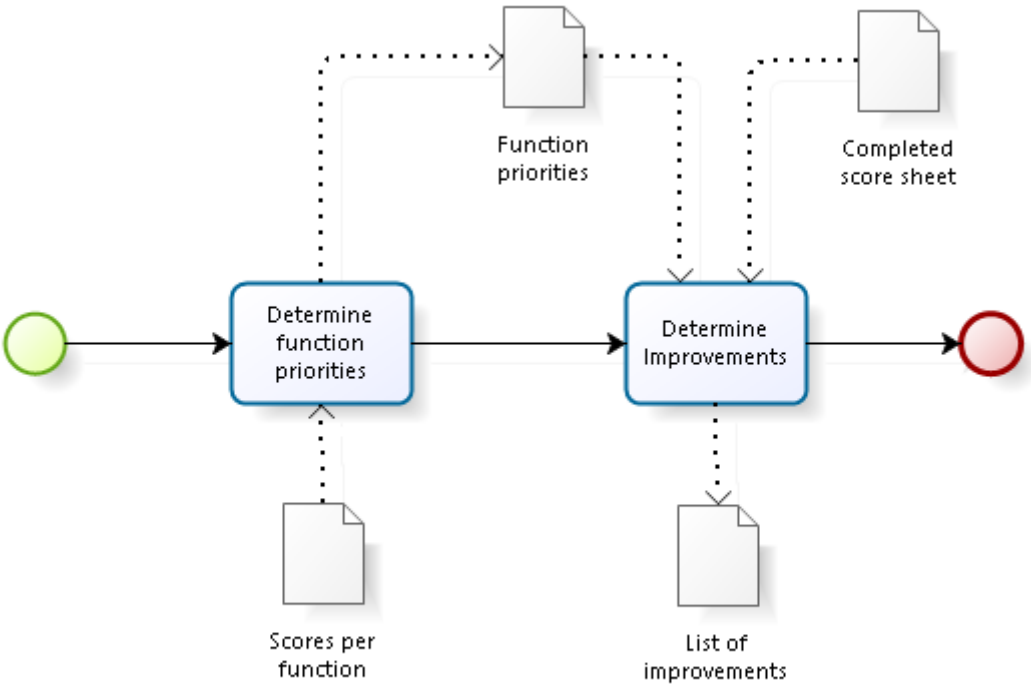

FIGURE 30. PROCESSMODEL STEP 5

DETERMINE FUNCTION PRIORITIES

APPROACH:

Based on the scores provided by the previous step, improvements can be recommended. These improvement recommendations are created based on the function scores. Determining the function that needs attention first, is the first step in creating recommendations for the improvements of the architecture.

METHOD:

For this task, three methods are suggested. The Level method is used when a significant gap between functions is present. However, when the functions have (about) the same score, other methods should be used. These methods, Upgrade 1 and 2, focus on improving the architecture by providing next steps. These methods (patterns) were selected consulting SMEs in the field. They represent the most important streams in the field.

LEVEL: This improvement method is built on the assumption that a chain is as strong as its weakest link. It therefore appoints the lowest scoring function and marks this as the most important area of improvement. By improving the lowest score iteratively, the scores are balanced.

UPGRADE 1: When all scores are (about) the same, this method prescribes a pattern for assigning the most important area of improvement. In determining the improvement opportunities, the functions are observed in the following order:

- Identify
- Protect
- Detect

- Respond
- Recover.

In this order, each function provides a solid basis for the following function. For example, if the identification function is underdeveloped, it is harder to build a rigid protection function. Protecting a set of unknown assets is rather difficult. This line of thinking can be followed through the functions.

In the search for improvements, it is therefore useful to start building foundations from a solid basis. This does not mean that the first layer should score 100% before advancing to the next function. While upgrading the functions, the described pattern should be executed iteratively.

UPGRADE 2: When all scores are (about) the same, this method prescribes a pattern for assigning the most important area of improvement. This method also prescribes small incremental upgrades on the functions, however the order is different than presented in Upgrade 1. This method assigns the following order in prioritizing:

- Identify
- Protect
- Respond
- Recover
- Detect

This method also marks the upgrade of the Identify and Protect functions as the first steps to take. Having a better view on the threats and vulnerabilities and improve protection against them are the first priorities. However, the focus then shifts to Respond and Recover. According to this method the next most important thing is how to handle incidents. If these functions have made a small step, the Detection function should be improved.

DELIVERABLE:

FUNCTION PRIORITIES: A list of the order in which the different functions should be improved.

DETERMINE IMPROVEMENTS

APPROACH:

Based on the priorities assigned in the previous step, the improvements per function are determined. How many of these improvement are executed may vary. This decision will be made based on time and resources available. This step, however, aims for the creation of a prioritized list of possible improvement steps.

METHOD:

LEVEL: This improvement method is built on the assumption that a chain is as strong as its weakest link. It therefore appoints the lowest scoring category and marks this as the most important area of improvement. By improving the lowest score iteratively, the scores are balanced and overall improved. In this procedure upgrading 0 to 1 is considered more useful than 1 to 2.

DELIVERABLE:

PRIORITIZED LIST OF IMPROVEMENT SUGGESTIONS: The list of improvements will provide the company with insight in their architecture. The weakest points are appointed and prioritized based on a combination of methods.

5 DEMONSTRATION

The fourth step of the research methodology is the demonstration. Peffers et al. (2007) describe this step as to *use the artifact to solve one or more instances of the problem*. This can be done is several ways. For this demonstration case studies are used. The case studies are performed based on information provided by three organizations.

Effective knowledge of the use of the artifact is needed (Peffers et al., 2007). As this is an ongoing research, the author is the only person with sufficient knowledge of the methodology. Therefore the analysis was performed by the author. Where needed, organization specific information was collected through person in the organization.

5.1 Case 1: Company A

Company A is a semi public company executing a task on behalf of the National Government. Their task is related to licensing activities and vehicles. In order to perform this task adequately, Company A employs about a 1000 people distributed all over the country.

Case Description is removed because of confidentiality (General observations and conclusions are provided in Chapter 6). Corresponding Appendix F is also confidential

5.2 Case 2: Company B

Company B is a utility company playing an essential role in the distribution of power. Therefore, it plays an important role in the well-being of the Dutch citizens. In order to maintain and operate their assets, Company B employs more than 1500 people. In their work, the continuity of their service is the most important goal.

Case Description is removed because of confidentiality (General observations and conclusions are provided in Chapter 6). Corresponding Appendix Gis also confidential

5.3 Case 3: Company C

Company C is an independent body working under the control of the Dutch Government. One of the key tasks is to make sure Dutch citizens receive money there are entitled too, based on mainly social security related regulations. The reach of their activities is national, therefore their organization is quite substantial. The organization employs 1000-1500 people.

Case Description is removed because of confidentiality (General observations and conclusions are provided in Chapter 6). Corresponding Appendix H is also confidential

6 EVALUATION

The fifth step of the research methodology is the evaluation. Peffers et al. (2007) describe this step as to *Observe and measure how well the artifact supports a solution to the problem. This activity involves comparing the objectives of a solution to actual observed results from use of the artifact in the demonstration.* This can be done is several ways. For this research interviews are used.

In the evaluation a set of interviews is performed to gather insight in the performance of the artifact. For all three cases, two security officers and two enterprise architects of the organization were interviewed. Of these experts, one security officer and one enterprise architect were involved in the demonstration as a contact person. The others were introduced new during the interview. To complement the views presented by the internal experts, experts outside the case organization were consulted. This was done during workshops with the SMEs involved in this research.

6.1 Methodology Evaluation

As mentioned in the previous chapter, the demonstration provided great insight in the usage of the methodology. Following the developed methodology, an assessment is created on the degree to which information security is integrated in the enterprise architecture. During the execution several interesting insights arose.

The first insight concerns the artifacts used in the analysis. As seen in Case 1, a project architecture is less suitable as a basis for this analysis. This can be explained by the scope of the methodology. Assessing the full enterprise, the analysis is looking for evidence of very diverse nature. This can be a process in the HR department, but also a very specific application for Intrusion Detection. As most projects have a smaller scope than the full enterprise, the evidence needed is very unlikely to be found in one project.

The second insight showed a difference between the theoretical world and real life practice. As presented in Figure 31 part 1, the methodology assumes Enterprise Architecture in its widest meaning. It is used as a representation of the complete organization and all its resources, activities and assets. This includes the activities performed by the information security team.

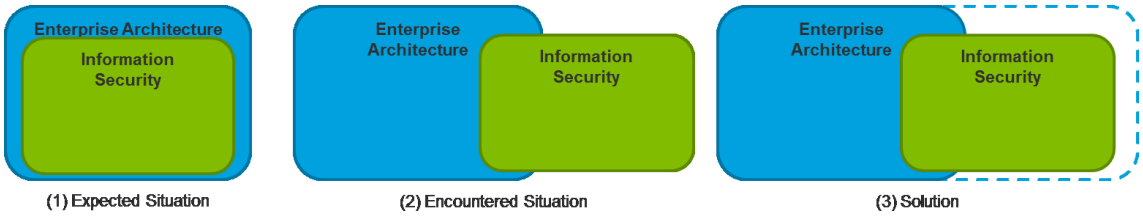

FIGURE 31. PRACTICAL PROBLEM AND SOLUTION

During the demonstration, however, the real situation turned out to be different (Figure 31, part 2). In the organizations participating in this demonstration, a certain overlap was established. In this overlap, the EA team and the information security team were working together and documentation was shared. Both teams, however, also had a lot of unshared activities and documentation. This gap can be dealt with in two ways. The first option is to focus exclusively on the documentation presented by enterprise architecture. This is the most pure form of analysis, but neglects a lot of documentation that is present and known within the organization. Therefore, another option was chosen and used in the demonstrations.

This solution (Figure 31, part 3) mimics the expected situation by incorporation the information security documents. This allows for the creation of a more complete view on the documented security. As most organizations still separate information security from enterprise architecture, this enables the methodology to be executed more widely.

During the analysis, the matrix provided in Appendix D was used frequently. The expectations formulated for each of the intersections were found to be complete most of the time. Describing processes based on their trigger, expected milestone(s) and outcome, turned out to provide enough guidance. However, two points of improvements became clear.

The first improvement focuses on the formulation of the requirements. It was observed several times that one requirement asked for two or more things. An example of this is: *PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained*. This asks for the baseline to be set (1) and managed (2). During the demonstration, this problem was encountered several times. Here, it did not have a big impact on the score, as both parts scored the same. However, it is not hard to imagine a situation where this would a problem. This could be solved in a next version, but this would mean a deviation from the original standard.

The second improvement focusses on the formulation of the expectations for each intersection. All of the expectations are formulated based on an element being present. This caused an interesting situation in one of the cases. Requirement PR.DS-2 prescribes: *Data-in-transit is protected.* This is expected to be fulfilled by encryption on the network connections and software monitoring the data. In one of the cases however, it was explicitly mentioned data was not to be encrypted during transit in a certain environment. In this environment, the monitoring software would perform better on data that was not encrypted. This did not meet our expectations, but it was, in this case, more safe than encrypting. Therefore it was scored 2 points.

How this could be solved in a next version, is still unknown. None of the interviewees could find a way of solving this. The only solution would be to describe several scenarios for each requirement. Not only would this be an enormous job, it was also believed that such a set would never be complete. For now, the best solution seems to leave this to the analyst.

Overall the methodology was found useful. All, except one, would consider using this methodology. It provides them with a clear overview of the situation in their organization. This one person who would not consider to use this methodology, found it useful for others, but not for himself. As his job consisted of working on the edge of enterprise architecture and information security, the methodology did not provide him with a new insights. Nevertheless, he could imagine that someone more focused on one of the two topics, could gain valuable insight from the methodology.

6.2 Outcome Evaluation

During the interviews, a central role was reserved for the outcome of the analysis. Based on these interviews, the correctness of the outcome was determined. This was done by asking people for the score they were expecting for each of the functions at the start of the interview. When the results were presented, the scores were compared with their expectations.

Based on these comparisons, it can be said that the methodology provides a good image. In only two interviews, the expected outcome was notable different from the analysis outcome. The other interviewees estimated their score within 10% below or above the actual score.

The two deviations were explained during the interviews. The first deviation was explained by the way of scoring. The interviewee scored his company high (around 80%) on all of the functions. He based this score based on the activities performed by his coworkers and the activities he performed himself. A lot of active monitoring and proactive event management was performed around him.

However, looking at the documentation, very little of these activities were documented. This was an eye-opener for the interviewee.

The second deviation was explained by the understanding of the research. This interviewee had trouble determining what the scope of the research was. Unfortunately, this was discovered at the end of the interview. The interviewee expected very low scores, as a lot of the documents within the enterprise architecture did not explicitly mention security. During the interview, his understanding of the research grew and his view on the expected scores changed.

It was interesting to see that one of the participants had recently performed a similar analysis. Based on another standard, an audit on the organization was performed. This audit was based on the actual situation in the organization. The outcomes of this audit were (almost) all included in the outcome of the analysis performed based in this research. However, this research found more points of improvement. This was explained by the way the analysis is performed. Apparently, a number of improvements determined by this research, are already implemented in the organization. However, this is done based on personal skill and insight of the employee and therefore undocumented. Therefore, this analysis provided a new insight; the difference between the analysis outcomes is the difference between the designed and actual organization.

This difference, between the designed and the real-life organization, was subject to discussion several times. The organization often was believed to engage in more security activities, than documented in any of the departments. Within team, roles and tasks are perform informally and known by all of them. Explicating these activities in documents, would secure them for the future (generation).

All in all, following the methodology steps, an insight is created in the extent to which information security in integrated in the enterprise architecture. This insight is considered to be valid. The improvements appointed by the methodology, where considered useful. All experts, except two, agreed on the importance of the suggested improvements. The other to two experts supported the conclusion and improvement suggestions, but lived under the impression that far more important things were at hand in their organization.

6.3 Overall discussion

During the methodology design, it was stated that most organizations focus on digital information (Section 3.1.2.). This statement was found to be correct during the demonstrations. In both of the organizations, paper information was equated to information stored on removable media. The security requirements for these items were identical. One of the organizations described the chapter on hardcopy information as follows: *see removable media*. By statements like this one, the digitalization of enterprise information is shown. Enterprise architecture, focusing on the alignment of business and IT, should be able to play an increasingly important role in the security of information.

During the evaluation, the gap between the enterprise architecture and the actual activities in enterprise was discussed. Using the enterprise architecture as a source of the analysis, has advantages and disadvantages. During the interviews, it was mentioned several times that the quality of the architecture descriptions is crucial. We acknowledge this, but this is not considered a problem. The documentation used in this analysis, is also used as a reference in project and as a basis for new development. The quality of the work therefore also has great impact on the future. Therefore low quality architectural descriptions should reflect in a low analysis score.

It was also mentioned that a gap is present between the designed activities and the actual activities. During the evaluations, several of the improvements were believed to be already implemented. It turned out that these activities were performed, based on skill and experience. However in order to secure this knowledge and skill, it should be described in one of the artifacts.

One of the architects explained this gap by his team's focus: *"As we are focusing on supporting projects, extending the architecture to new areas is suspended. In order to see what extensions could be made, we should be able to connect with the other team more often"*. This is in line with observed separation between EA and information security teams. The focus on information security is now staffed by a specific team. Integrating their approaches would strengthen the overall outcome.

In the third step of the research methodology, a set of five methodology goals was composed (section 4.1). Based on the demonstration and evaluation, the fulfillment of these goals can be determined. This is done below.

Goal 1: Provide Enterprise Architects with a method for determining the security level of the Enterprise Architecture.

The designed methodology is capable of reaching this goal. Using EA documentation as input, the enterprise architects can perform this analysis. This was supported by the participating interviewees.

Goal 2: Provide insights in the requirements drawn upon Enterprise Architecture by Information Security.

The matrix provided in Appendix D answers this goal. Using several SME workshops and interviews, this matrix was compiled. It describes the expected elements in enterprise architecture, in order to meet each requirement. During the demonstration these descriptions were used and found to be adequate. Based on the evaluation outcome it can be stated that these description are correct.

Goal 3: Determine the overall security level of an Enterprise Architecture.

The methodology describes several method to provide the enterprise architecture with a score. Based on the needs of the analyst, one of this methods can be chosen.

Goal 4: Determine the weak spots in the Enterprise Architecture from a security standpoint.

Beside the overall score, the methodology provides the analyst with scores per function. This provides a more detailed insight in the weak spots. The methodology also assigns point of improvement based on these scores. By doing this, the actual weak spots are presented.

Goal 5: Whenever possible the methodology will make use of existing methods.

The methodology contains no original methods. All methods are based on literature or best practices. These best practices were collected from the participating SMEs by workshops and interviews.

7 CONCLUSION

This chapter describes the conclusions of this research. The conclusions are based on the literature review, the development of the methodology, its demonstration and the evaluation. Based on these steps, the main research question will be answered:

How can we assess the level of information security within an organization by analyzing the enterprise architecture?

In order to answer this question, several sub question were answered. The answers to all research question is provided in section 7.1. The remainder of this chapter also discusses the contributions to both theory and practice (section 7.2) and the limitations and suggestion for future research (section 7.3)

7.1 Conclusions

In order to provide an answer to the main question, five sub questions are answered.

SQ 1: Which enterprise architecture descriptions are suitable for this analysis??

As shown in the literature review (section 2.2), numerous definitions, frameworks and artifact sets are present for Enterprise Architecture. During the solution design (section 3.1.1), we decided that artifacts are the most suitable representation of enterprise architecture for this analysis. As a result of this design process, the following artifact set was composed:

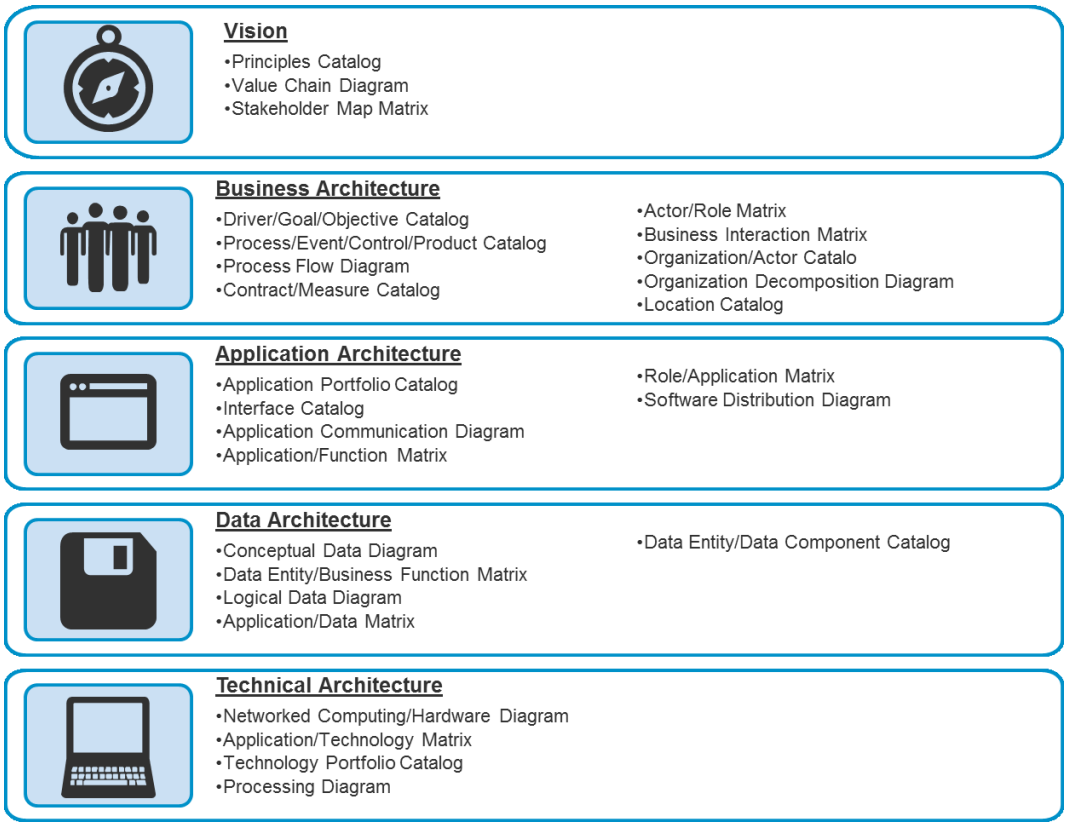

FIGURE 32. SELECTED ARTIFACTS FOR THE REPRESENTATION OF ENTERPRISE ARCHITECTURE

SQ 2: Which information security descriptions are suitable for this analysis?

As shown in the literature review (section 2.3), numerous definitions and standards are present for Information Security. During the solution design (section 3.1.2), it was decided that the framework provided by NIST (NIST, 2013) is the most suitable representation for this analysis. The framework formulates a clear overview of the requirements information security raises. These requirements are categorized as follows:

FIGURE 33. NIST REQUIREMENT CATEGORY OVERVIEW

SQ 3: Which integrated approaches are available?

As presented in the literature review (section 2.4), several authors are mentioning the combination of information security and enterprise architecture. However, the degree to which they specify the combination is often low. Most papers offer high level views and conceptual ideas. The research presented by Van den Bosch (2014) is an exception to this. In this research, an approach for integrated enterprise architecture and security is described.

SQ 4: Which requirements does Information Security impose on Enterprise Architecture?

Based on the representations formulated in SQ1 and SQ2, the relation between the information security requirements and the enterprise architecture artifacts is defined. As described in section 3.2, this was done based on workshops and interviews with a set of four SMEs. In the resulting framework, for each requirement involved the artifacts are determined. For each of these combinations, it is determined what is expected from the artifact in order to meet the requirement.

The resulting framework and the relation descriptions are presented in Appendix D.

SQ 5: Can a methodology be defined to analyze the level of security within an Enterprise Architecture?

Based on the relations established in SQ4, a methodology is designed to analyze an organization. For this analysis, as discussed, the organization is represented by its artifacts. The methodology consists of five steps:

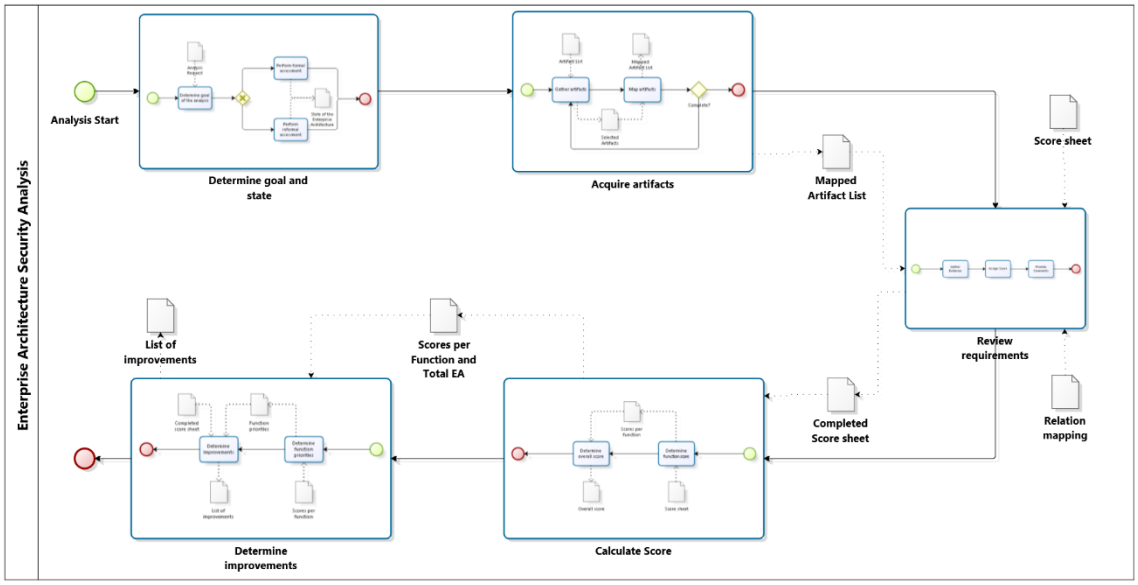

FIGURE 34. OVERALL METHODOLOGY DESCRIPTION

STEP 1: DETERMINE STATE AND GOAL

As stated in section 3.1.1, the first step of the methodology is looking at its context. When the analysis is used to screen the architecture, the difference between the design and the real-life organization can be neglected. The outcome of the analysis will strengthen the design of the enterprise. However, a problem might arise when the analysis results are used to improve the real-life organization. When there is a difference between the design and real-life organization, the wrong conclusion might be drawn. The analysis outcome might identify a problem that is not present in the real-life organization, or the other way around. Awareness of this problem is the most important part of avoiding it. Therefore the goal of the analysis and the state of the architecture influence the interpretation of the analysis results and should therefore be explicated.

STEP 2: GATHER ARTIFACTS

In order to start the analysis, the documents need to be collected. This is done in the second step in the methodology. To check for completeness and make the analysis easier to perform, the collected documents are mapped to the expected artifacts.

STEP 3: PERFORM ANALYSIS

Basis for the analysis is the framework built in the first phase of the solution design. For each of the requirements, evidence is gathered to show to which extend it is met. Based on the degree to which the requirement is met, a score is provided. This score might come is different forms, depending on the method used. A score sheet (Appendix E) is provided for guidance during this step.

STEP 4: DETERMINE SCORE

When a score is assigned to each requirement, scores for the functions and complete architecture can be determined. As described in the methodology goals (section 4.1), these scores can be used to provide insights in the architecture. Therefore the scores per function and the overall score are determined separately.

STEP 5: DETERMINE IMPROVEMENTS

Based on the previous steps, recommendations for further improvement can be derived. The recommendations are based on the scores assigned to different requirements and functions. If the purely qualitative observation method was chosen in the previous steps, this step will be harder to perform.

Based on the demonstration and evaluation of the methodology in practice, it can be stated that the methodology performs well. The methodology provides insight into the level of integration of information security in the enterprise architecture. Based on a set of expert interviews for each case, the scores assigned by the methodology are believed to be correct. The improvements derived from these scores are seen as valuable input for future development, according to the experts.

Based on the answers provided by the sub questions, the main question can be answered:

How can we assess the level of information security within an organization by analyzing the enterprise architecture?

In this research, an enterprise architecture is seen as the formal representation (design) of an organization. This architecture, represented by its artifacts, can be used to perform an analysis on the organization. Based on the established information security requirements, a verdict on the level of information security in the enterprise architecture can be derived.

Through this, the designed analysis methodology can provide insight in the level of information security in the designed organization. It provides insight into the extent to which a *secure by design* architecture is created. Under the assumption the organization is correctly represented by the architecture, we are able to assess the level of information security within an organization by analyzing the enterprise architecture. The designed methodology therefore answers the main question.

7.2 Contributions

This research has both theoretical and practical relevance. In this section, the contributions of this research to theory and practice are discussed.

7.2.1 Contribution to Theory

The first main contribution to theory is the description of the relation between information security and enterprise architecture.

- This thesis describes a set of enterprise architecture artifacts, needed to perform an information security analysis of an enterprise architecture.
- Furthermore, a demonstration is provided of the use of the NIST framework. Its structure of functions, categories and subcategories is used to provide refinement in the outcome of the analysis.
- The relation between each information security requirement and one (or more) enterprise architecture artifact is described. Not only is the existence of the relation appointed, but also is it form explicated.

The second main contribution is the methodology. Based on the first contribution, a methodology is designed to analyze an enterprise architecture. This methodology provides a structured way of performing the analysis and offers tools and methods with it. The used steps and methods are best practices provided by SMEs. Also is the methodology tested in practice and validated with several experts from the enterprise architecture and information security discipline.

7.2.2 Contribution to Practice

The contribution to practice is the methodology. This research presents a usable methodology that serves as a guideline for analyzing the level of information security of an enterprise architecture. It provides a basis which can be used and further developed by consulting companies, such as Deloitte. The methodology is made more practical by combining methods and tool from literature with best practices from practice.

The proposed methodology consists of five steps. The steps are described in such detail that they can be understood and executed right away by various analysts. Each step is described for its approach, methods and outcome. By providing several possible methods, the analyst is allowed some flexibility in executing the analysis. This flexibility is added hoping to enable wider usage of the methodology. This will provide more insight in the performance of the methodology and hopefully stimulate further research into this methodology.

7.3 Limitations and Suggestions for Future Work

A number of limitations of this research are present. This section will outline these limitations and provide suggestions for further research.

The first limitation is the fact that this research is based on qualitative methods. The solution design is based on a group of experts. Although their expertise and experience cover both fields well, more research could be done in the definition of the relations and the implementation of the methodology steps. As stated in the research goals (section 1.3.2), this research aimed for the development of a first version of an analysis method. Based on the research outcome, improvements and developments can be made. One of these actions could involve improvement of the framework. This could be done based on other/more SME input.

Another improvement could be the addition of quantitative analysis tools. The relations defined in this research could be used to engage in such an analysis. In order to prepare for this, the requirements need to be specified even further. As quantitative analysis cannot interpret requirements, their description should be more specific and expressed in a more formal way (e.g. (Johnson et al., 2007)).

The introduction of quantitative analysis will also cope with the second limitation. The methodology is based on the search and interpretation of the analyst. Although the framework describes the expected elements as precise as possible, the analyst determines the verdict. The correctness of the outcome leans of his/her honesty. According to one of the interviewees *the auditor needs to be trusted. If not, all audits become irrelevant.* This is supported by the author, but is something that deserves attention in the future.

The third limitation is a basic assumption for this research: The enterprise architecture describes the complete structure and all activities in the enterprise. The (implemented) design is believed to describe the actual affairs in the enterprise. However, a gap might exist between the design and the actual enterprise. This is not specifically a problem for the proposed methodology, but it impact the way the outcomes should be looked at. A solution for this limitation is incorporated as step 1 of the methodology. Nevertheless, this still is concern while discussing the outcome.

The final point of this section is a suggestion for future work. During the analysis of the case results, the idea arose that a typology for organizations could be derived. One of the organization positioned itself by the phrase “better safe than sorry”. This motto was recognized in the scoring; the scores for the *identify* and *protect* functions were the highest. Another organization characterized itself as being very responsive. This was also recognized in the scores. Therefore, further research in information security typologies for enterprises might be interesting.

8 REFERENCES

Anderson, J. A., & Rachamadugu, V. (2008). *Managing security and privacy integration across enterprise business process and infrastructure.* Paper presented at the 2008 IEEE International Conference on Services Computing, SCC 2008, Honolulu, HI.

Aziz, S., Obitz, T., Modi, R., & Sarkar, S. (2005). Enterprise Architecture: A Governance Framework. *Part I: Embedding architecture into the Organization. InfoSyS Technologies Ltd*.

Bernard, S. A. (2012). *An introduction to enterprise architecture*: AuthorHouse.

Bizagi. (2015). Bizagi - Business Process Management (BPM) software, BPMS and Workflow. Retrieved March 24, 2015, from http://www.bizagi.com/en/bpm-suite

Boster, M., Liu, S., & Thomas, R. (2000). Getting the most from your enterprise architecture. *IT Professional, 2*(4), 43-50. doi: 10.1109/6294.869382

Cieply, M., & Barnes, B. (2014, December 31th, 2014). Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm. *The New York Times,* p. 1. Retrieved from http://nyti.ms/1wzwYDM

Foorthuis, R., Brinkkemper, S., & Bos, R. (2008) An artifact model for projects conforming to Enterprise Architecture. *Vol. 15 LNBIP. 1st IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling, PoEM 2008* (pp. 30-46). Stockholm.

Gartner. (2013). Enterprise Architect - EA - Gartner IT Glossary. Retrieved 23th September, 2014, from http://www.gartner.com/it-glossary/enterprise-architecture-ea/

Hijink, M. (2014, December 10th 2014). Deze 10 lessen moeten alle bedrijven leren van de Sony-hack. Retrieved from http://www.nrcq.nl/2014/12/10/column-marc

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*: Information Systems Audit Control Association.

Iyer, B., & Gottlieb, R. (2004). The four-domain architecture: An approach to support enterprise architecture design. *IBM Systems Journal, 43*(3), 587-597.

Johnson, P., Lagerström, R., Närman, P., & Simonsson, M. (2007). Enterprise architecture analysis with extended influence diagrams. *Information Systems Frontiers, 9*(2-3), 163-180. doi: 10.1007/s10796-007-9030-y

Kaisler, S. H., Armour, F., & Valivullah, M. (2005). *Enterprise architecting: Critical problems.* Paper presented at the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI.

Kissel, R. (2013). NISTIR 7298 -Revision 2 - "Glossary of Key Information Security Terms" (C. S. D. I. T. Laboratory, Trans.): National Institute of Standards and Technology (NIST).

Kreizman, G., & Robertson, B. (2006). Incorporating Security Into the Enterprise Architecture Process: Gartner.

Lankhorst. (2005). Introduction to enterprise architecture. *Enterprise Architecture at Work: Modelling, Communication, and Analysis*, 1-10.

Lankhorst, M. M. (2004). Enterprise architecture modelling - The issue of integration. *Advanced Engineering Informatics, 18*(4), 205-216. doi: 10.1016/j.aei.2005.01.005

McCumber, C. J. R. (1991). *Information Systems Security: A Comprehensive Model.* Paper presented at the 14th National Computer Security Conference, Baltimore.

NIST. (2007). NIST, SP 800-100,"Information Security Handbook for Managers". *Information Security Handbook for Managers*.

NIST. (2013). Preliminary Cybersecurity Framework: National Institute of Standards and Technology (NIST).

Pagliery, J. (2014, December 29th, 2014). 'Sony-pocalypse': Why the Sony hack is one of the worst hacks ever. Retrieved from http://money.cnn.com/2014/12/04/technology/security/sony-hack/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Praxiom Research Group Limited. (2015, September 7th 2014). Plain English ISO IEC 27000 2014 Information Security Definitions. Retrieved Februari 23th 2015, 2015

Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool. *Journal of Systems and Software, 80*(10), 1607-1620. doi: 10.1016/j.jss.2007.01.044

Roest, J. E. (2013). The relationship between enterprise architecture, business complexity and business performance.

Saint-Germain, R., & others. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Sessions, R. (2007). Comparison of the top four enterprise architecture methodologies.

Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise Security Architecture (pp. 25): SABSA.

Tang, A., Han, J., & Chen, P. (2004). *A comparative analysis of architecture frameworks.* Paper presented at the Proceedings - 11th Asia-Pacific Software Engineering Conference, APSEC 2004, Busan.

The International Organization for Standardization. (2014a, 20 October 2014). About us. Retrieved 1 december, 2014, from http://www.iso.org/iso/home/about.htm

The International Organization for Standardization. (2014b). ISO/IEC 27000:2014. 2014-01-15: The International Organization for Standardization,,.

The Open Group. (2011). TOGAF Version 9.1: The Open Group.

The Open Group. (2013). ArchiMate® 2.1 Specification: The Open Group.

Van den Bosch, S. F. (2014). Designing Secure Enterprise Architectures A comprehensive approach: framework, method, and modelling language.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*(2), 99-104.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly, 26*(2), 3.

Whitman, M., & Mattord, H. (2011). *Principles of information security*: Cengage Learning.

Wielstra, B. A. (2014). Assessing the Impact of Business Process Redesign Decisions on Internal Control within Banks: A Methodology.

Wikipedia, C. (2014, 20-9-2014). Security. Retrieved 24 september, 2014, from http://en.wikipedia.org/w/index.php?title=Security&oldid=635213220

Winter, R., & Fischer, R. (2006). *Essential layers, artifacts, and dependencies of enterprise architecture.* Paper presented at the 2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops, EDOCW2006, Hong Kong.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22*(1), 45-55.

Zachman, J. (2002). The zachman framework for enterprise architecture. *Zachman International*.

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal, 26*(3), 276-292.

Zachman, J. A. (1997). Enterprise architecture: The issue of the century. *Database Programming and Design, 10*(3), 44-53.

Appendix A ENTERPRISE ARCHITECTURE ARTIFACT SELECTION

TABLE 4. FRAMEWORK ARTIFACT MATRIX

		The Open Group (2011)	J. Zachman (2002)	Boster et al. (2000)	Winter and Fischer (2006)	Foorthuis et al. (2008)	Total
Vision							
	Principles Catalog	x		x	x		3
	Stakeholder Map Matrix	x	x				2
	Value Chain Diagram	x			x		2
	Solution Concept Diagram	x					1
Business Architecture							
	Driver/Goal/Objective Catalog	x	x	x	x	x	5
	Process Flow Diagram	x	x	x	x	x	5
	Actor/Role Matrix	x			x	x	3
	Organization/Actor Catalog	x			x		2
	Location Catalog	x	x				2
	Process/Event/Control/Product Catalog	x	x				2
	Contract/Measure Catalog	x		x			2
	Business Interaction Matrix	x			x		2
	Organization Decomposition Diagram	x			x		2
	Role Catalog	x					1
	Business Service/Function Catalog	x					1
	Business Footprint Diagram	x					1
	Business Service/Information Diagram	x					1
	Functional Decomposition Diagram	x					1
	Product Lifecycle Diagram	x					1
	Goal/Objective/Service Diagram	x					1
	Business Use-Case Diagram	x					1
	Event Diagram	x					1
Data Architecture							
	Conceptual Data Diagram	x	x		x	x	4
	Logical Data Diagram	x	x		x	x	4
	Data Entity/Data Component Catalog	x	x				2

		The Open Group (2011)	J. Zachman (2002)	Boster et al. (2000)	Winter and Fischer (2006)	Foorthuis et al. (2008)	Total
	Data Entity/Business Function Matrix	x			x		2
	Application/Data Matrix	x			x		2
	Data Dissemination Diagram	x					1
	Data Security Diagram	x					1
	Data Migration Diagram	x					1
	Data Lifecycle Diagram	x					1
Application Architecture							
	Application Portfolio Catalog	x	x		x		3
	Application Communication Diagram	x	x		x		3
	Role/Application Matrix	x	x		x		3
	Interface Catalog	x			x		2
	Application/Function Matrix	x			x		2
	Software Distribution Diagram	x			x		2
	Application/Organization Matrix	x					1
	Application Interaction Matrix	x					1
	Application and User Location Diagram	x					1
	Application Use-Case Diagram	x					1
	Enterprise Manageability Diagram	x					1
	Process/Application Realization Diagram	x					1
	Software Engineering Diagram	x					1
	Application Migration Diagram	x					1
Technology Architecture							
	Networked Computing/Hardware Diagram	x	x	x	x		4
	Technology Portfolio Catalog	x	x		x		3
	Application/Technology Matrix	x			x		2
	Processing Diagram	x	x				2
	Technology Standards Catalog	x					1
	Environments and Locations Diagram	x					1
	Platform Decomposition Diagram	x					1
	Communications Engineering Diagram	x					1

Appendix B NIST CATEGORY SPECIFICATION

Function	Category	Subcategory
IDENTIFY (ID)		
IDENTIFY (ID)	Asset Management (ID.AM)	**Asset Management (ID.AM):**
		ID.AM-1: Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: (cyber)security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment (ID.BE)	**Business Environment (ID.BE):**
		ID.BE-1: The organization's role in the supply chain is identified and communicated
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established
		ID.BE-5: Resilience requirements to support delivery of critical services are established
	Governance (ID.GV)	**Governance (ID.GV):**
		ID.GV-1: Organizational information security policy is established
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3: Legal and regulatory requirements regarding (cyber)security, including privacy and civil liberties obligations, are understood and managed
		ID.GV-4: Governance and risk management processes address (cyber)security risks
	Risk Assessment (ID.RA)	**Risk Assessment (ID.RA):**
		ID.RA-1: Asset vulnerabilities are identified and documented
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
		ID.RA-3: Threats, both internal and external, are identified and documented
		ID.RA-4: Potential business impacts and likelihoods are identified
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized
	Risk Management Strategy (ID.RM):	**Risk Management Strategy (ID.RM):**
		ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

PROTECT (PR)		
PROTECT(PR)	Access Control (PR.AC)	**Access Control (PR.AC):**
		PR.AC-1: Identities and credentials are managed for authorized devices and users
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate
	Awareness and Training (PR.AT)	**Awareness and Training (PR.AT):**
		PR.AT-1: All users are informed and trained
		PR.AT-2: Privileged users understand roles & responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
		PR.AT-4: Senior executives understand roles & responsibilities
		PR.AT-5: Physical and information security personnel understand roles & responsibilities
	Data Security (PR.DS)	**Data Security (PR.DS):**
		PR.DS-1: Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment
	Information Protection Processes and Procedures (PR.IP)	**Information Protection Processes and Procedures (PR.IP):**
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained
		PR.IP-2: A System Development Life Cycle to manage systems is implemented
		PR.IP-3: Configuration change control processes are in place
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
		PR.IP-6: Data is destroyed according to policy
		PR.IP-7: Protection processes are continuously improved
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10: Response and recovery plans are tested
		PR.IP-11: (cyber)security is included in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: A vulnerability management plan is developed and implemented
	Maintenance (PR.MA)	**Maintenance (PR.MA):**
		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	Protective	**Protective Technology (PR.PT):**
		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

		PR.PT-2: Removable media is protected and its use restricted according to policy
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality
		PR.PT-4: Communications and control networks are protected
DETECT (DE)		
	Anomalies and Events (DE.AE)	**Anomalies and Events (DE.AE):**
		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2: Detected events are analyzed to understand attack targets and methods
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
		DE.AE-4: Impact of events is determined
		DE.AE-5: Incident alert thresholds are established
	Security Continuous Monitoring (DE.CM)	**Security Continuous Monitoring (DE.CM):**
		DE.CM-1: The network is monitored to detect potential (cyber)security events
		DE.CM-2: The physical environment is monitored to detect potential (cyber)security events
		DE.CM-3: Personnel activity is monitored to detect potential (cyber)security events
		DE.CM-4: Malicious code is detected
		DE.CM-5: Unauthorized mobile code is detected
		DE.CM-6: External service provider activity is monitored to detect potential (cyber)security events
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.CM-8: Vulnerability scans are performed
	Detection Processes	**Detection Processes (DE.DP):**
		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2: Detection activities comply with all applicable requirements
		DE.DP-3: Detection processes are tested
		DE.DP-4: Event detection information is communicated to appropriate parties
		DE.DP-5: Detection processes are continuously improved
RESPOND (RS)		
	Response Planning	**Response Planning (RS.RP):**
		RS.RP-1: Response plan is executed during or after an event
	Communications (RS.CO)	**Communications (RS.CO):**
		RS.CO-1: Personnel know their roles and order of operations when a response is needed
		RS.CO-2: Events are reported consistent with established criteria
		RS.CO-3: Information is shared consistent with response plans
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader (cyber)security situational awareness
	Analysis (RS.AN)	**Analysis (RS.AN):**
		RS.AN-1: Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		RS.AN-3: Forensics are performed
		RS.AN-4: Incidents are categorized consistent with response plans
	Mitigation (RS.MI)	**Mitigation (RS.MI):**
		RS.MI-1: Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM)	**Improvements (RS.IM):**

		RS.IM-1: Response plans incorporate lessons learned RS.IM-2: Response strategies are updated
RECOVER(RC)		**RECOVER (RC)**
	Recovery Planning	**Recovery Planning (RC.RP):**
		RC.RP-1: Recovery plan is executed during or after an event
	Improvements	**Improvements (RC.IM):**
		RC.IM-1: Recovery plans incorporate lessons learned RC.IM-2: Recovery strategies are updated
	Communications (RC.CO)	**Communications (RC.CO):**
		RC.CO-1: Public relations are managed RC.CO-2: Reputation after an event is repaired RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Appendix C DEFINITION OF ARTIFACTS

These references are selected from the TOGAF (The Open Group, 2011). However, the text has been altered for the sake of this research. Some parts have been deleted and assumptions about the artifact are added.

35.6 ARCHITECTURAL ARTIFACTS BY ADM PHASE

Figure 35-3 shows the artifacts that are associated with the core content metamodel and each of the content extensions.

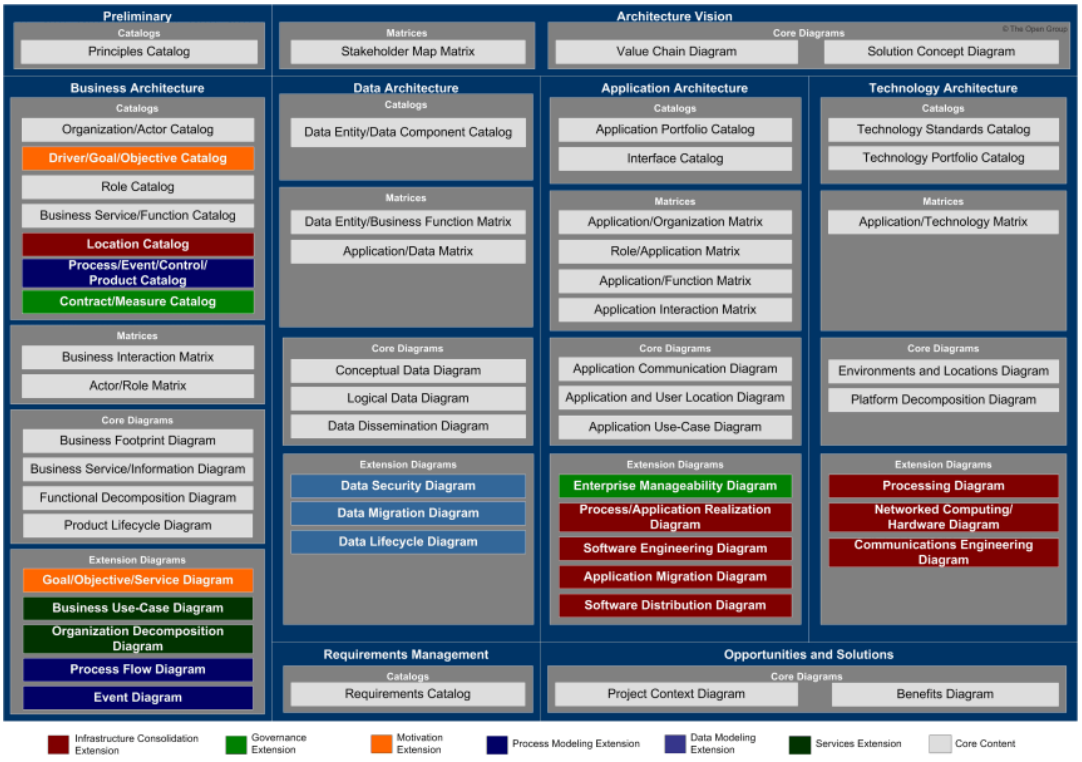

Figure 35-3: Artifacts Associated with the Core Content Metamodel and Extensions

The specific classes of artifact are as follows:

- **Catalogs** are lists of building blocks.
- **Matrices** show the relationships between building blocks of specific types.
- **Diagrams** present building blocks plus their relationships and interconnections in a graphical way that supports effective stakeholder communication.

The recommended artifacts for production in each ADM phase are as follows.

35.6.1 Preliminary Phase (For this research combined with the architecture vision)

PRINCIPLES CATALOG

The Principles catalog captures principles of the business and architecture principles that describe what a "good" solution or architecture should look like. Principles are used to evaluate and agree an outcome for architecture decision points. Principles are also used as a tool to assist in architectural governance of change initiatives.

The Principles catalog contains the following metamodel entities:

- Principle

STAKEHOLDER MAP MATRIX (ORIGINALLY FROM PHASE A: ARCHITECTURE VISION)

The purpose of the Stakeholder Map matrix is to identify the stakeholders for the architecture engagement, their influence over the engagement, and their key questions, issues, or concerns that must be addressed by the architecture framework.

Understanding stakeholders and their requirements allows an architect to focus effort in areas that meet the needs of stakeholders.

Due to the potentially sensitive nature of stakeholder mapping information and the fact that the Architecture Vision phase is intended to be conducted using informal modeling techniques, no specific metamodel entities will be used to generate a stakeholder map.

For this research, it is assumed that the Stakeholder Map will contain stakeholders of the EA outcome as well. These stakeholder may also include security officers or external entities.

REQUIREMENTS CATALOG (ORIGINALLY FROM PHASE E: OPPORTUNITIES AND SOLUTIONS)

The Requirements catalog captures things that the enterprise needs to do to meet its objectives. Requirements generated from architecture engagements are typically implemented through change initiatives identified and scoped during Phase E (Opportunities & Solutions). Requirements can also be used as a quality assurance tool to ensure that a particular architecture is fit-for-purpose (i.e., can the architecture meet all identified requirements).

The Requirements catalog contains the following metamodel entities:

- Requirement
- Assumption
- Constraint
- Gap

35.6.3 Phase B: Business Architecture

ORGANIZATION/ACTOR CATALOG

The purpose of the Organization/Actor catalog is to capture a definitive listing of all participants that interact with IT, including users and owners of IT systems.

The Organization/Actor catalog can be referenced when developing requirements in order to test for completeness.

For example, requirements for an application that services customers can be tested for completeness by verifying exactly which customer types need to be supported and whether there are any particular requirements or restrictions for user types.

The Organization/Actor catalog contains the following metamodel entities:

- Organization Unit
- Actor
- Location (may be included in this catalog if an independent Location catalog is not maintained)

DRIVER/GOAL/OBJECTIVE CATALOG

The purpose of the Driver/Goal/Objective catalog is to provide a cross-organizational reference of how an organization meets its drivers in practical terms through goals, objectives, and (optionally) measures.

Publishing a definitive breakdown of drivers, goals, and objectives allows change initiatives within the enterprise to identify synergies across the organization (e.g., multiple organizations attempting to achieve similar objectives), which in turn allow stakeholders to be identified and related change initiatives to be aligned or consolidated.

The Driver/Goal/Objective catalog contains the following metamodel entities:

- Organization Unit
- Driver
- Goal
- Objective
- Measure (may optionally be included)

LOCATION CATALOG

The Location catalog provides a listing of all locations where an enterprise carries out business operations or houses architecturally relevant assets, such as data centers or end-user computing equipment.

Maintaining a definitive list of locations allows change initiatives to quickly define a location scope and to test for completeness when assessing current landscapes or proposed target solutions. For example, a project to upgrade desktop operating systems will need to identify all locations where desktop operating systems are deployed.

Similarly, when new systems are being implemented, a diagram of locations is essential in order to develop appropriate deployment strategies that comprehend both user and application location and identify location-related issues, such as internationalization, localization, timezone impacts on availability, distance impacts on latency, network impacts on bandwidth, and access.

The Location catalog contains the following metamodel entities:

- Location

PROCESS/EVENT/CONTROL/PRODUCT CATALOG

The Process/Event/Control/Product catalog provides a hierarchy of processes, events that trigger processes, outputs from processes, and controls applied to the execution of processes. This catalog provides a supplement to any Process Flow diagrams that are created and allows an enterprise to filter, report, and query across organizations and processes to identify scope, commonality, or impact.

For example, the Process/Event/Control/Product catalog allows an enterprise to see relationships of processes to sub-processes in order to identify the full chain of impacts resulting from changing a high-level process.

The Process/Event/Control/Product catalog contains the following metamodel entities:

- Process
- Event
- Control
- Product

ACTOR/ROLE MATRIX

The purpose of this matrix is to show which actors perform which roles, supporting definition of security and skills requirements.

Understanding Actor-to-Role relationships is a key supporting tool in definition of training needs, user security settings, and organizational change management.

The Actor/Role matrix shows the following metamodel entities and relationships:

- Actor
- Role
- Actor *performs* Role relationships

In this matrix, parts of the role catalog are assumed. These description might often be found in this document or a document like the Role Catalog

> ***ROLE CATALOG***
>
> *The purpose of the Role catalog is to provide a listing of all authorization levels or zones within an enterprise. Frequently, application security or behavior is defined against locally understood concepts of authorization that create complex and unexpected consequences when combined on the user desktop.*
>
> *If roles are defined, understood, and aligned across organizations and applications, this allows for a more seamless user experience and generally more secure applications, as administrators do not need to resort to workarounds in order to enable users to carry out their jobs.*
>
> *In addition to supporting security definition for the enterprise, the Role catalog also forms a key input to identifying organizational change management impacts, defining job functions, and executing end-user training.*
>
> *As each role implies access to a number of business functions, if any of these business functions are impacted, then change management will be required, organizational responsibilities may need to be redefined, and retraining may be needed*

PROCESS FLOW DIAGRAM

The purpose of the Process Flow diagram is to depict all models and mappings related to the process metamodel entity.

Process Flow diagrams show sequential flow of control between activities and may utilize swim-lane techniques to represent ownership and realization of process steps. For example, the application that supports a process step may be shown as a swim-lane.

In addition to showing a sequence of activity, process flows can also be used to detail the controls that apply to a process, the events that trigger or result from completion of a process, and also the products that are generated from process execution

.

Process Flow diagrams are useful in elaborating the architecture with subject specialists, as they allow the specialist to describe "how the job is done" for a particular function. Through this process, each process step can become a more fine-grained function and can then in turn be elaborated as a process

.

35.6.4 Phase C: Data Architecture

The following describes catalogs, matrices, and diagrams that may be created within Phase C (Data Architecture).

DATA ENTITY/BUSINESS FUNCTION MATRIX

The purpose of the Data Entity/Business Function matrix is to depict the relationship between data entities and business functions within the enterprise. Business functions are supported by business services with explicitly defined boundaries and will be supported and realized by business processes. The mapping of the Data Entity-Business Function relationship enables the following to take place:

- Assign ownership of data entities to organizations
- Understand the data and information exchange requirements business services
- Support the gap analysis and determine whether any data entities are missing and need to be created
- Define application of origin, application of record, and application of reference for data entities
- Enable development of data governance programs across the enterprise (establish data steward, develop data standards pertinent to the business function, etc.)

The Data Entity/Business Function matrix shows the following entities and relationships:

- Data Entity
- Business Function
- Data Entity relationship to owning Organization Unit

APPLICATION/DATA MATRIX

The purpose of the Application/Data matrix is to depict the relationship between applications (i.e., application components) and the data entities that are accessed and updated by them.

Applications will create, read, update, and delete specific data entities that are associated with them. For example, a CRM application will create, read, update, and delete customer entity information.

The data entities in a package/packaged services environment can be classified as master data, reference data, transactional data, content data, and historical data. Applications that operate on the data entities include transactional applications, information management applications, and business warehouse applications.

The mapping of the Application Component-Data Entity relationship is an important step as it enables the following to take place:

- Assign access of data to specific applications in the organization
- Understand the degree of data duplication within different applications, and the scale of the data lifecycle
- Understand where the same data is updated by different applications
- Support the gap analysis and determine whether any of the applications are missing and as a result need to be created

The Application/Data matrix is a two-dimensional table with Logical Application Component on one axis and Data Entity on the other axis.

CONCEPTUAL DATA DIAGRAM

The key purpose of the Conceptual Data diagram is to depict the relationships between critical data entities within the enterprise. This diagram is developed to address the concerns of business stakeholders.
Techniques used include:

- Entity relationship models
- Simplified UML class diagrams

DATA SECURITY DIAGRAM

Data is considered as an asset to the enterprise and data security simply means ensuring that enterprise data is not compromised and that access to it is suitably controlled.

The purpose of the Data Security diagram is to depict which actor (person, organization, or system) can access which enterprise data. This relationship can be shown in a matrix form between two objects or can be shown as a mapping.

The diagram can also be used to demonstrate compliance with data privacy laws and other applicable regulations (HIPAA, SOX, etc.). This diagram should also consider any trust implications where an enterprise's partners or other parties may have access to the company's systems, such as an outsourced situation where information may be managed by other people and may even be hosted in a different country.

35.6.5 Phase C: Application Architecture

The following describes catalogs, matrices, and diagrams that may be created within Phase C (Application Architecture).

APPLICATION PORTFOLIO CATALOG

The purpose of this catalog is to identify and maintain a list of all the applications in the enterprise. This list helps to define the horizontal scope of change initiatives that may impact particular kinds of applications. An agreed Application Portfolio allows a standard set of applications to be defined and governed.

The Application Portfolio catalog provides a foundation on which to base the remaining matrices and diagrams. It is typically the start point of the Application Architecture phase.

The Application Portfolio catalog contains the following metamodel entities:

- Information System Service
- Logical Application Component
- Physical Application Component

ROLE/APPLICATION MATRIX

The purpose of the Role/Application matrix is to depict the relationship between applications and the business roles that use them within the enterprise.

People in an organization interact with applications. During this interaction, these people assume a specific role to perform a task; for example, product buyer.

The mapping of the Application Component-Role relationship is an important step as it enables the following to take place:

- Assign usage of applications to the specific roles in the organization
- Understand the application security requirements of the business services and processes supporting the function, and check these are in line with current policy
- Support the gap analysis and determine whether any of the applications are missing and as a result need to be created
- Define the application set used by a particular business role; essential in any move to role-based computing

The Role/Application matrix is a two-dimensional table with Logical Application Component on one axis and Role on the other axis.

The relationship between these two entities is a composite of a number of metamodel relationships that need validating:

- Role *accesses* Function
- Function *is bounded by* Service
- Services are *realized by* Logical/Physical Application Components

APPLICATION COMMUNICATION DIAGRAM

The purpose of the Application Communication diagram is to depict all models and mappings related to communication between applications in the metamodel entity.

It shows application components and interfaces between components. Interfaces may be associated with data entities where appropriate. Applications may be associated with business services where appropriate. Communication should be logical and should only show intermediary technology where it is architecturally relevant.

35.6.6 Phase D: Technology Architecture

The following section describes catalogs, matrices, and diagrams that may be created within Phase D (Technology Architecture) as listed in *12.5 Outputs*.

TECHNOLOGY PORTFOLIO CATALOG

The purpose of this catalog is to identify and maintain a list of all the technology in use across the enterprise, including hardware, infrastructure software, and application software. An agreed technology portfolio supports lifecycle management of technology products and versions and also forms the basis for definition of technology standards.

The Technology Portfolio catalog provides a foundation on which to base the remaining matrices and diagrams. It is typically the start point of the Technology Architecture phase.

Technology registries and repositories also provide input into this catalog from a baseline and target perspective.

The Technology Portfolio catalog contains the following metamodel entities:

- Platform Service
- Logical Technology Component
- Physical Technology Component

APPLICATION/TECHNOLOGY MATRIX

The Application/Technology matrix documents the mapping of applications to technology platform.

This matrix should be aligned with and complement one or more platform decomposition diagrams.

The Application/Technology matrix shows:

- Logical/Physical Application Components
- Services, Logical Technology Components, and Physical Technology Components
- Physical Technology Component *realizes* Physical Application Component relationships

PROCESSING DIAGRAM

The Processing diagram focuses on deployable units of code/configuration and how these are deployed onto the technology platform. A deployment unit represents grouping of business function, service, or application components. The Processing diagram addresses the following:

- Which set of application components need to be grouped to form a deployment unit
- How one deployment unit connects/interacts with another (LAN, WAN, and the applicable protocols)
- How application configuration and usage patterns generate load or capacity requirements for different technology components

The organization and grouping of deployment units depends on separation concerns of the presentation, business logic, and data store layers and service-level requirements of the components. For example, presentation layer deployment unit is grouped based on the following:

- Application components that provide UI or user access functions
- Application components that are differentiated by location and user roles

There are several considerations to determine how application components are grouped together. Each deployment unit is made up of sub-units, such as:

- **Installation**: Part that holds the executable code or package configuration (in case of packages).
- **Execution**: Application component with its associated state at run time.
- **Persistence**: Data that represents the persistent state of the application component.

Finally, these deployment units are deployed on either dedicated or shared technology components (workstation, web server, application server, or database server, etc.). It is important to note that technology processing can influence and have implications on the services definition and granularity.

NETWORKED COMPUTING/HARDWARE DIAGRAM

Starting with the transformation to client-server systems from mainframes and later with the advent of e-Business and J2EE, large enterprises moved predominantly into a highly network-based

distributed network computing environment with firewalls and demilitarized zones. Currently, most of the applications have a web front-end and, looking at the deployment architecture of these applications, it is very common to find three distinct layers in the network landscape; namely a web presentation layer, an business logic or application layer, and a back-end data store layer. It is a common practice for applications to be deployed and hosted in a shared and common infrastructure environment.

So it becomes highly critical to document the mapping between logical applications and the technology components (e.g., server) that supports the application both in the development and production environments. The purpose of this diagram is to show the "as deployed" logical view of logical application components in a distributed network computing environment. The diagram is useful for the following reasons:

- Enable understanding of which application is deployed where in the distributed network computing environment
- Establishing authorization, security, and access to these technology components
- Understand the Technology Architecture that support the applications during problem resolution and troubleshooting
- Isolate performance problems encountered by applications, determine whether it is application code-related or technology platform-related, and perform necessary upgrade to specific physical technology components
- Identify areas of optimization as and when newer technologies are available which will eventually reduce cost
- Enable application/technology auditing and prove compliance with enterprise technology standards
- Serve as an important tool to introduce changes to the Technology Architecture, thereby supporting effective change management
- Establish traceability and changing application end-point address while moving application either from a shared environment to a dedicated environment or *vice versa*

The scope of the diagram can be appropriately defined to cover a specific application, business function, or the entire enterprise. If chosen to be developed at the enterprise level, then the network computing landscape can be depicted in an application agnostic way as well.

Appendix D EA - INFORMATION SECURITY FRAMEWORK

This appendix contains the EA - Information Security Framework. This framework is presented on the next page. For each Information Security requirement, the artifact(s) contributing to the fulfillment of the requirement are identified. These are marked by an X in the framework. For each of the identified combinations, a description is provided to explicate what is expected of an artifact in order to meet the requirement. These descriptions are presented in sections D.1 till D.5.

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTUR			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Function	**Category**	**Subcategory**																		
IDENTIFY (ID)		**IDENTIFY (ID)**																		
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**Asset Management (ID.AM):**																		
		ID.AM-1: Physical devices and systems within the organization are inventoried															X	X	-	-
		ID.AM-2: Software platforms and applications within the organization are inventoried									X	X	-							
		ID.AM-3: Organizational communication and data flows are mapped				-	X	-	-	-				-	-	-				
		ID.AM-4: External information systems are catalogued									X	X	-				X	X	-	-
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value									X	-	-	-	X	-	-	X	-	-
		ID.AM-6: (cyber)security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established				-	-	X	-	-										
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform (cyber)security roles, responsibilities, and risk management decisions.	**Business Environment (ID.BE):**																		
		ID.BE-1: The organization's role in the supply chain is identified and communicated	-	X	-															
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	X	-	-															
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated				X	-	-	-	-										
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established				-	X	X	-	-										
		ID.BE-5: Resilience requirements to support delivery of critical services are established	-	-	X															
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of (cyber)security risk.	**Governance (ID.GV):**																		
		ID.GV-1: Organizational information security policy is established	X	-	X															
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners				-	-	X	-	-										
		ID.GV-3: Legal and regulatory requirements regarding (cyber)security, including privacy and civil liberties obligations, are understood and managed	-	-	X	-	X	-	-	X										
		ID.GV-4: Governance and risk management processes address (cyber)security risks				-	X	-	-	X										
	Risk Assessment (ID.RA): The organization understands the (cyber)security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Risk Assessment (ID.RA):**																		
		ID.RA-1: Asset vulnerabilities are identified and documented	-	-	-	-	X	-	-	X	-	-	-	-	-	-	-	-	-	-
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	-	-	X						X	X	-							
		ID.RA-3: Threats, both internal and external, are identified and documented				-	X	-	-	X										
		ID.RA-4: Potential business impacts and likelihoods are identified				-	X	-	-	X										
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk				-	X	-	-	-										
		ID.RA-6: Risk responses are identified and prioritized				-	X	-	-	X										
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**Risk Management Strategy (ID.RM):**																		
		ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	-	X	-	-	X	-	-	X										
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	X	-	-															
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	X	-	-															
PROTECT (PR)		**PROTECT (PR)**																		
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**Access Control (PR.AC):**																		
		PR.AC-1: Identities and credentials are managed for authorized devices and users				-	X	-	-	X							X	-	-	-
		PR.AC-2: Physical access to assets is managed and protected				-	-	-	-	X							X	X	-	-
		PR.AC-3: Remote access is managed				-	X	-	-	X	-	X	-				X	X	-	-
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties				-	-	X	-	X	-	-	X	-	-	X	-	-	X	-
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate															X	X	-	-
	Awareness and Training (PR.AT): The organization's personnel and partners are provided (cyber)security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**Awareness and Training (PR.AT):**																		
		PR.AT-1: All users are informed and trained					X			X										
		PR.AT-2: Privileged users understand roles & responsibilities					X			X										
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities					X			X										
		PR.AT-4: Senior executives understand roles & responsibilities					X			X										
		PR.AT-5: Physical and information security personnel understand roles & responsibilities					X			X										
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**Data Security (PR.DS):**																		
		PR.DS-1: Data-at-rest is protected				-	-	-	X	-				-	X	-	X	X	-	-
		PR.DS-2: Data-in-transit is protected				-	-	-	X	-				-	X	-	-	X	-	X
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition				-	X	-	-	X										
		PR.DS-4: Adequate capacity to ensure availability is maintained	-	-	X															
		PR.DS-5: Protections against data leaks are implemented	-	-	X						X	X	-				X	X	-	-
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity									X	X	-	X	-	-				
		PR.DS-7: The development and testing environment(s) are separate from the production environment	X	-	-												X	-	-	X
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**Information Protection Processes and Procedures (PR.IP):**																		
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	-	-	X															
		PR.IP-2: A System Development Life Cycle to manage systems is implemented				-	X	-	-	-										
		PR.IP-3: Configuration change control processes are in place				-	X	-	-	X										
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically				-	X	-	-	X	X	-	-							
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	X	-	-	-	X	-	-	X										
		PR.IP-6: Data is destroyed according to policy				-	X	-	-	-										
		PR.IP-7: Protection processes are continuously improved				-	X	-	-	X										
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	-	X	X	-	-	-	-	-										
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	-	-	X	-	X	-	-	X										
		PR.IP-10: Response and recovery plans are tested				-	X	-	-	-										
		PR.IP-11: (cyber)security is included in human resources practices (e.g., deprovisioning, personnel screening)				-	X	-	-	X										
		PR.IP-12: A vulnerability management plan is developed and implemented	-	-	X															
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**Maintenance (PR.MA):**																		
		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	-	-	X	-	-	X	-	-										
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	-	-	X	-	-	X	-	-										
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**Protective Technology (PR.PT):**																		
		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	-	-	X	-	X	X	-	X										
		PR.PT-2: Removable media is protected and its use restricted according to policy	X	-	-															
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality									-	-	X	-	X	X				
		PR.PT-4: Communications and control networks are protected									X	-	-				-	X	-	-
DETECT (DE)		**DETECT (DE)**																		
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**Anomalies and Events (DE.AE):**																		
		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	-	-	X	-	-	X	-	-										
		DE.AE-2: Detected events are analyzed to understand attack targets and methods				-	X	-	-	X										
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors									X	-	-							
		DE.AE-4: Impact of events is determined				-	X	-	-	X										
		DE.AE-5: Incident alert thresholds are established	-	-	X	-	-	X	-	-										
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify (cyber)security events and verify the effectiveness of protective measures.	**Security Continuous Monitoring (DE.CM):**																		
		DE.CM-1: The network is monitored to detect potential (cyber)security events									X	-	-				X	-	-	-
		DE.CM-2: The physical environment is monitored to detect potential (cyber)security events				-	X	X	-	X										
		DE.CM-3: Personnel activity is monitored to detect potential (cyber)security events				-	X	-	-	X	X	X	X							
		DE.CM-4: Malicious code is detected									X	-	-							
		DE.CM-5: Unauthorized mobile code is detected									X	-	-							
		DE.CM-6: External service provider activity is monitored to detect potential (cyber)security events									X	X	-							
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed				-	X	-	-	-	X	X	-							
		DE.CM-8: Vulnerability scans are performed	-	-	X															
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**Detection Processes (DE.DP):**																		
		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability				-	-	X	-	-										
		DE.DP-2: Detection activities comply with all applicable requirements				-	X	-	-	-										
		DE.DP-3: Detection processes are tested	-	-	X															
		DE.DP-4: Event detection information is communicated to appropriate parties				-	X	-	-	X										
		DE.DP-5: Detection processes are continuously improved	-	-	X															
RESPOND (RS)		**RESPOND (RS)**																		
	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected (cyber)security events.	**Response Planning (RS.RP):**																		
		RS.RP-1: Response plan is executed during or after an event				-	X	-	-	X										
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**Communications (RS.CO):**																		
		RS.CO-1: Personnel know their roles and order of operations when a response is needed				-	-	X	-	-										
		RS.CO-2: Events are reported consistent with established criteria				-	X	-	-	X										
		RS.CO-3: Information is shared consistent with response plans				-	-	X	-	-										
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans				-	X	-	-	X										
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader (cyber)security situational	X	-	-															
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**Analysis (RS.AN):**																		
		RS.AN-1: Notifications from detection systems are investigated				-	X	-	-	X										
		RS.AN-2: The impact of the incident is understood				-	X	-	-	X										
		RS.AN-3: Forensics are performed				-	X	-	-	X										
		RS.AN-4: Incidents are categorized consistent with response plans				-	X	-	-	X										
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**Mitigation (RS.MI):**																		
		RS.MI-1: Incidents are contained				-	X	-	-	X										
		RS.MI-2: Incidents are mitigated				-	X	-	-	X										
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks				-	X	-	-	X										
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**Improvements (RS.IM):**																		
		RS.IM-1: Response plans incorporate lessons learned				-	-	-	-	X										
		RS.IM-2: Response strategies are updated				-	X	-	-	X										
RECOVER (RC)		**RECOVER (RC)**																		
	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by (cyber)security events.	**Recovery Planning (RC.RP):**																		
		RC.RP-1: Recovery plan is executed during or after an event	-	-	X	-	-	-	-	-										
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**Improvements (RC.IM):**																		
		RC.IM-1: Recovery plans incorporate lessons learned	-	-	X	-	X	-	-	X										
		RC.IM-2: Recovery strategies are updated	-	-	X	-	X	-	-	X										
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**Communications (RC.CO):**																		
		RC.CO-1: Public relations are managed	-	X	-															
		RC.CO-2: Reputation after an event is repaired				-	X	-	-	X										
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	-	X	-	-	-	-	-	-										

D.1 Comments on Identify Function

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/ Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Control framework																				
Function	**Category**	**Subcategory**																		
IDENTIFY (ID)		**IDENTIFY (ID)**																		
	Asset Management (ID.AM)	**Asset Management (ID.AM):**																		
		ID.AM-1: Physical devices and systems within the organization are inventoried															Diagram should provide an overview of all technical components and their relations.	The catalog should provide an overview of all technical component in the enterprise.		
		ID.AM-2: Software platforms and applications within the organization are inventoried									A description of all applications should be present.	This diagram should provide an overview of the available applications and their relations.								
		ID.AM-3: Organizational communication and data flows are mapped					Process steps imply the communication flow. It is required for process steps to be assigned to a role.													
		ID.AM-4: External information systems are catalogued									A description of all external applications should be present.	This diagram should provide an overview of the available applications (including external) and their relations.					Diagram should provide an overview of all internal and external technical components and their relations.	The catalog should provide an overview of all technical component in the enterprise and the external components that are connected.		
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value									Applications should be described from a CIA viewpoint. These scores can be used for prioritization of the applications.				Data shall be provide with a CIA score. This score can be used to prioritize them.			These component descriptions shall be extended by use of a CIA score.		
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established						The roles should be described. At least thay should express the expected activities of a role, its right and responsibilities.												
	Business Environment (ID.BE)	**Business Environment (ID.BE):**																		
		ID.BE-1: The organization's role in the supply chain is identified and communicated		The external stakeholders are recognized. Also is their role described.																
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	The prinicples provide insight in the role the organization has in its environment. Also they define the role the organization want to have.																	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated				Through this catalog the Driver, Goals and Objectives are communicated. In order to fulfill this requirement there need to be a priorization to these goals and objectives.														
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established					Critical processes should be identiefied.	Critical roles should be identiefied.												
		ID.BE-5: Resilience requirements to support delivery of critical services are established			A document describing the threats faced by the organization is expected.															
	Governance (ID.GV)	**Governance (ID.GV):**																		
		ID.GV-1: Organizational information security policy is established	Leadership indicates what their risk appetite is.		Some requirement might be formulated to further specify the principles.															
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners						Provides a certain actor with a defined role.												
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed			The requriement catalog shall contain security requirements. These shall describe how to handle legal and regulatory requirements and privacy requirements.		A process is described for updating the requirements.			A process is described that is triggered based on time or regulatory change. This process will uodate the requirements and output an updateed version of the requiremetns catalog.									
		ID.GV-4: Governance and risk management processes address cybersecurity risks					A process describing the governance and risk management is expected.			A process for governance and risk management is expected. This process will be triggered on a timely basis. No explicit outcome is expected.										

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/ Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Control framework																				
Function	Category	Subcategory																		
	Risk Assessment (ID.RA)	**Risk Assessment (ID.RA):**																		
		ID.RA-1: Asset vulnerabilities are identified and documented					A process for vulnerability analysis is described.			A process for vulnarebility analysis is described. This process is triggered timely. The outcome of this process will be a report identifing and documenting all vulnarebilities in the enterprise.										
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources			As a process or part of a process, information gathering should be explicated. It should state what information is gathered, who does this and how it is processed into the organization. This could be done by both software and employees.						An application gathering this information should be described in the catalog. It should be connected to several sources.	An application with this funtion should be represented in the diagram. This application should be connected to several different sources.								
		ID.RA-3: Threats, both internal and external, are identified and documented					A process for identifing threats should be present. Also, the documenting of threats should be described.			There should be a threat identification process. Also, an "Threat Identified" event should be present triggering a process.										
		ID.RA-4: Potential business impacts and likelihoods are identified					There should be a process for analysing the impact and likelihood of a threat. This process is triggered when a new threat arises, but preferably also periodically to reassess all threats.			If a threat is identified, an assessment of impact and likelihood should be performed.										
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk					In the process of determining risk Threats, vulnerabilities, likelihoods, and impacts are taken into account.													
		ID.RA-6: Risk responses are identified and prioritized					A process for identifing responses is present.			There is a process for identifing responses to several kinds of risks. The output of this process will at least contain a prioritized list of responses.										
	Risk Management Strategy (ID.RM)	**Risk Management Strategy (ID.RM):**																		
		ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders		This matrix describes the level of influence a stakeholder has on a specific part of the enterprise. This also goes for the Risk Management processes.			Risk management process is described.			A process for risk management is established. This porcess will be executed continously or in triggered by a timer.										
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Leadership explicates the risk they are willing to take. This can be expressed in a monetary value, but there are several options available.																	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	An explanation for the risk tolerance stement should be provided.																	

D.2 Comments on Protect Function

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/ Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Function	Category	Subcategory																		
PROTECT (PR)																				
	Access Control (PR.AC)	Access Control (PR.AC):																		
		PR.AC-1: Identities and credentials are managed for authorized devices and users					A process is described for adding new users. This process contain an element ensuring the account is handed to the right user. Also a process is needed for the deletion of user accounts.			A process is described for the creation of user accounts. This process is triggered by the entry of a new actor. Also a process for deletion is described. This is trigger on exit.										
		PR.AC-2: Physical access to assets is managed and protected								Processes need authorizations for certain actions. These are documented.							Might include access gates or door scanner in the architecture.			
		PR.AC-3: Remote access is managed					There is a process for changing the access right of employees.			Access right change process is called when an employee leaves the organization or changes roles. Also upon request from the organization.		An application for enabling access and managing access is in place.					A component for allowing external access is in place.	A component for enabling external access is in place and connected to both the outside world and the access managing server.		
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties						Role description contains a edscription of the privileges this role needs.		Process is described for evaluations of the user right. This is trigger on entry and exit of an actor. Also when an actor changes roles.			This matrix describes the access of roles to applications. A better solution is to explicate the level of access for example in the form of CRUD. Also, there should be a component monitoring and managing access rights.			This matrix describes the access of roles to applications. A better solution is to explicate the level of access for example in the form of CRUD.			Should described what application is located where. A better solution would be to specify the the actions a application is allowed to perform on a specific piece of technology.	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate															Switch for disconnecting certain servers of data centers is in place.	Segregation is applied where possible.		
	Awareness and Training (PR.AT)	Awareness and Training (PR.AT):																		
		PR.AT-1: All users are informed and trained					Informing and training should be part of the onboarding process. On assignment of a new role, new and existing knowledge should be changed.			Informing and training should be part of the onboarding process. On assignment of a new role, new and existing knowledge should be changed										
		PR.AT-2: Privileged users understand roles & responsibilities					On the assignment of a new role, empolyees are informed on their responsibilities regarding security.			On the assignment of a new role, empolyees are informed on their responsibilities regarding security.										
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities					On the assignment of a new role, empolyees are informed on their responsibilities regarding security.			On the assignment of a new role, empolyees are informed on their responsibilities regarding security.										
		PR.AT-4: Senior executives understand roles & responsibilities					On the assignment of a new role, empolyees are informed on their responsibilities regarding security.			On the assignment of a new role, empolyees are informed on their responsibilities regarding security.										
		PR.AT-5: Physical and information security personnel understand roles & responsibilities					During onboarding, training should be integrated. If changed into on of the security roles, training on the new role and responsibilities should be provided.			During onboarding, training should be integrated. If changed into on of the security roles, training on the new role and responsibilities should be provided.										

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/ Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Control framework																				
Function	**Category**	**Subcategory**																		
PROTECT (PR)	Data Security (PR.DS)	**Data Security (PR.DS):**																		
		PR.DS-1: Data-at-rest is protected							For each loaction the data can be in , the level of security needed is determined.						Describes how the protection is implemented.		Datastores are expected to be duplicated in any way.	Information on the implemented security measures should be provided. At least, encryption of the data is expected.		
		PR.DS-2: Data-in-transit is protected							For each loaction the data can be in , the level of security needed is determined.						Describes how the protection is implemented.			Information on the implemented security measures should be provided. At least, encryption of the data is expected.		During processing, data should be encrypted (or otherwise protected).
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition					An asset management process is described.			An asset management process is described. It is triggered on every movement of the asset. This process will be involved in these movements.										
		PR.DS-4: Adequate capacity to ensure availability is maintained			A measure for the needed and provided capacity is present and managed.															
		PR.DS-5: Protections against data leaks are implemented			Project and Architectural requirements should providede statements on the expected measures.						A firewall and scanning software are described in the catalog.	A firewall and scanning software are placed at central points in the architecture.					Protection from intruders should be in place.	Protection against intruders should be in the landscape and connected to the incoming connections.		
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity									There should be a piece of software designed for checking integretey of software, firmware and information	The targeted piece of software should have a place in the landscape connected to at least the main flows.		Constraints bijv. int, string, foreign key						
		PR.DS-7: The development and testing environment(s) are separate from the production environment	As a priciple, testing and production should be seperated.														A clear seperation is visible between the production and development environment is notable.			In the processing of application there is no overlap between the two environment.
	Information Protection Processes and Procedures (PR.IP)	**Information Protection Processes and Procedures (PR.IP):**																		
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained			It should be required in the use of detection methods, that a baseline is set to distinguish normal from abnormal traffic.															
		PR.IP-2: A System Development Life Cycle to manage systems is implemented					The Life cycle can be recognized in the process(es) describing system management.													
		PR.IP-3: Configuration change control processes are in place					A process model describing this process should be present.			This process should be described and linked to the right triggering events.										
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically					There should be a process describing the testing of backups and their restoring as well as one describing the maintanance on the backups.			A timely trigger should be in place for triggering the backup processes.	An application coordinating the backup procedure is described.									
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	Policies and regulations for the physical operation environment should be described.				A process for checking the execution of these policies should be described.			A process for checking the execution of these policies should be described and lined to the right events.										
		PR.IP-6: Data is destroyed according to policy					Data destruction policy is followed in this process.													
		PR.IP-7: Protection processes are continuously improved					A process for improving protection processes is descibed. Or the detection process itself has a trigger for this.			A process for improving protection processes is descibed. Or the detection process itself has a trigger for this.										
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties		The stakeholder document should indicate which are the appropriate parties.	For each process regarding protection it should be required to share information. How this is done and what information is shared, is decided per process.															
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed			It should be required for such a plan to be in place.		A process for managing the response plan is described.			A process for the management of response plans is described. It is triggered on a timely bases.										
		PR.IP-10: Response and recovery plans are tested					A plan describing the testing of response and recovery plans is in place. This process also triggers another process to solve errors found.													

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/ Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Control framework																				
Function	**Category**	**Subcategory**																		
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)					As part of the onboarding process, people receive security training fit for their role. This is also triggerd on role changes.			As part of the onboarding process, people receive security training fit for their role. This is also triggerd on role changes.										
		PR.IP-12: A vulnerability management plan is developed and implemented			This plan should be required.															
	Maintenance (PR.MA)	**Maintenance (PR.MA):**																		
		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools			A requirement should describe which activities are to be logged, which information about the activity and which tools are to be ued.			There should be at least one role responsable for this.												
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access			A requirement should describe which activities are to be logged, which information about the activity and which tools are to be ued.			There should be at least one role responsable for this.												
	Protective Technology (PR.PT)	**Protective Technology (PR.PT):**																		
		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy			A requirement should describe which activities are to be logged, which information about the activity and which tools are to be ued.		At least a process for the reviewing of the records is in place. Others might needs processes dependant on their implementation.	There should be at least one role responsable for this.		At least a process for the reviewing of the records is in place. This process is triggered based on time. Others might needs processes dependant on their implementation.										
		PR.PT-2: Removable media is protected and its use restricted according to policy	Leadership should provide high level guidance for this policy.																	
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality											Only to those who need it, access will be granted.		For each data assets, it should be known which processes and roles make use of it. (e.g. CRUD matrix)	Data can only be used by applications that really need it (and therefor users that really need it.). These applications shall only have access to exactly the data they need.				
		PR.PT-4: Communications and control networks are protected									A protective application is in place.							Network protecting components are in place.		

D.3 Comments on Detect Function

Control framework			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
Function	Category	Subcategory	Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control/ Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
DETECT (DE)		DETECT (DE)																		
	Anomalies and Events (DE.AE)	**Anomalies and Events (DE.AE):**																		
		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed			It should be required for IPDS installation to have this baseline			There should be at least one role responsable for this.												
		DE.AE-2: Detected events are analyzed to understand attack targets and methods					A process for the analysis of detected events is in place.			When an event is detected, the analysis process is triggered. This process produces an overview of the assumed target and used method.										
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors									A component for the collection and analysis of event data is in place.									
		DE.AE-4: Impact of events is determined					The process determines the impact of an event.			Upon detection of an event, the impact of the event is determined. Outcome of the proces is an overview of the estimated risk.										
		DE.AE-5: Incident alert thresholds are established			Based on the baseline, incident alerts should be determined and documented.			There should be at least one role responsable for this.												
	Security Continuous Monitoring (DE.CM)	**Security Continuous Monitoring (DE.CM):**																		
		DE.CM-1: The network is monitored to detect potential cybersecurity events									A component for the collection and analysis of event data is in place						Network monitoring devices are placed in such way, tempering the logs becomes (almost) impossible.			
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events					A process description for monitoring the physical environment is provided.	One or more roles should be made responsible for the proper execution of this process.		A process description for monitoring the physical environment is provided. This process should be exeuted continuously.										
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events					A process description for the monitoring of activity is described.			A process description for the monitoring of activity is described. This process should be executed continuously. In the cyber realm, this can be done by software.	A software component for (network) activity monitoring is described.	A software component for (network) activity monitoring is described. This component should be connected to (at least) the main infrasctructure.	In order to determine abnormal behaviour, the rights for each role to applications should be known.							
		DE.CM-4: Malicious code is detected									An application for the detection of unwanted code is in place.									
		DE.CM-5: Unauthorized mobile code is detected									An application for the detection of unwanted code is in place.									
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events									A software component for (network) activity monitoring is described. This component also monitors the activity from external parties.	A software component for (network) activity monitoring is described. This component should be connected to (at least) the main infrasctructure.								
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed					A process for the detection of unauthorized personnel should be described. Also, processes check on the monitoring software should be described.				An application for the detection of unwanted behaviour (from digital or physical agents) is in place.	An application for the monitoring of unwanted behaviour is in place.								
		DE.CM-8: Vulnerability scans are performed			Implementation determines further options (paper or digital)															
	Detection Processes (DE.DP)	**Detection Processes (DE.DP):**																		
		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability						Persons are linked to roles and roles have a description of their responsebilities.												
		DE.DP-2: Detection activities comply with all applicable requirements					Processes checking the compliance are in place.													
		DE.DP-3: Detection processes are tested			As part of the process implementation, the process should be tested.															
		DE.DP-4: Event detection information is communicated to appropriate parties					The process of event detection handling results in a report with sharable information.			The product of the process will consist of a sharable report containing information about the detected										
		DE.DP-5: Detection processes are continuously improved			The detection process should contain a reflective/evaluating step.															

D.4 Comments on Respond Function

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control /Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Function	**Category**	**Subcategory**																		
RESPOND (RS)		**RESPOND (RS)**																		
	Response Planning (RS.RP)	**Response Planning (RS.RP):**																		
		RS.RP-1: Response plan is executed during or after an event					In this case the response plan is the process			The process is triggered by an event.										
	Communications (RS.CO)	**Communications (RS.CO):**																		
		RS.CO-1: Personnel know their roles and order of operations when a response is needed						People are assigned to roles and roles have a clear description. Also are these roles linked to the process.												
		RS.CO-2: Events are reported consistent with established criteria					A reviewing process should be in place.			A process for reviewing this should be in place. This process is triggered on all or some of the reported events.										
		RS.CO-3: Information is shared consistent with response plans						There should be at least one role responsable for this.												
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans					The response plan prescibes the communication and has a checking mechanism for it.			The process should contain a mechanism for checking this.										
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Information sharing with other parties is prescribed from the highest level.																	
	Analysis (RS.AN)	**Analysis (RS.AN):**																		
		RS.AN-1: Notifications from detection systems are investigated					In the response process, a step describing the analysis is the system notfication should be described.			A process step for the investigation of system notifications should be part of the response process. This process should be triggered by notifications from the detection system.										
		RS.AN-2: The impact of the incident is understood					This should be a step in the response process.			This should be a step in the response process.										
		RS.AN-3: Forensics are performed					Performing deep analysis on the root of a notfications should be a step in the response process.			Performing deep analysis on the root of a notfications should be a step in the response process. The process should be triggered by a notification from the detection system. As forensics can be quite complicated, this step could be a process on its own aswell.										
		RS.AN-4: Incidents are categorized consistent with response plans					This should be a step in the response process.			This should be a step in the response process.										
	Mitigation (RS.MI)	**Mitigation (RS.MI):**																		
		RS.MI-1: Incidents are contained					This should be a step in the response process.			This should be a step in the response process.										
		RS.MI-2: Incidents are mitigated					This should be a step in the response process.			This should be a step in the response process.										
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks					This should be a step in the response process.			This should be a step in the response process.										
	Improvements (RS.IM)	**Improvements (RS.IM):**																		
		RS.IM-1: Response plans incorporate lessons learned								Outcome of the process contains at least a report of the events that occured and lessons learned from this incident.										
		RS.IM-2: Response strategies are updated					A revision process is in place. This can be triggered based on timing or on triggering events.			If new lessons learned become available, the current plans will be revised.										

D.5 Comments on Recover Function

			VISION			BUSINESS ARCHITECTURE					APPLICATION ARCHITECTURE			DATA ARCHITECTURE			TECHNICAL ARCHITECTURE			
			Principles Catalog	Stakeholder Map Matrix	Requirement Catalog	Driver/Goal/Objective Catalog	Process Flow Diagram	Actor/Role Matrix	Location Catalog	Process/Event/Control / Product Catalog	Application Portfolio Catalog	Application Communication Diagram	Role/Application Matrix	Conceptual Data Diagram	Data Security Diagram	Application/Data Matrix	Networked Computing/Hardware Diagram	Technology Portfolio Catalog	Application/Technology Matrix	Processing Diagram
Function	Category	Subcategory	Control framework																	
RECOVER (RC)		RECOVER (RC)																		
	Recovery Planning (RC.RP)	Recovery Planning (RC.RP):																		
		RC.RP-1: Recovery plan is executed during or after an event			Should be a requirement.															
	Improvements (RC.IM)	Improvements (RC.IM):																		
		RC.IM-1: Recovery plans incorporate lessons learned			Should be requirement for the process.		This should be a step in the response process.			This should be a step in the response process.										
		RC.IM-2: Recovery strategies are updated			Should be requirement for the process.		This should be a step in the response process.			This should be a step in the response process.										
	Communications (RC.CO)	Communications (RC.CO):																		
		RC.CO-1: Public relations are managed		Importance of different stakeholders is made explicit and agreed on.																
		RC.CO-2: Reputation after an event is repaired					A process for handling public relations in events is present.			Afer an event a process for reputation investigation is started.										
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams		Provide an overview of who need to be kept informed.																

Appendix E SCORE SHEET – EMPTY

Function	Category	Subcategory	Involved Artifacts	Score	Comment
IDENTIFY (ID)					
IDENTIFY (ID)	Asset Management (ID.AM)	**Asset Management (ID.AM):**			
		ID.AM-1: Physical devices and systems within the organization are inventoried			
		ID.AM-2: Software platforms and applications within the organization are inventoried			
		ID.AM-3: Organizational communication and data flows are mapped			
		ID.AM-4: External information systems are catalogued			
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value			
		ID.AM-6: (cyber)security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established			
	Business Environment (ID.BE)	**Business Environment (ID.BE):**			
		ID.BE-1: The organization's role in the supply chain is identified and communicated			
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated			
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated			
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established			
		ID.BE-5: Resilience requirements to support delivery of critical services are established			
	Governance (ID.GV)	**Governance (ID.GV):**			
		ID.GV-1: Organizational information security policy is established			
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners			
		ID.GV-3: Legal and regulatory requirements regarding (cyber)security, including privacy and civil liberties obligations, are understood and managed			
		ID.GV-4: Governance and risk management processes address (cyber)security risks			
	Risk Assessment	**Risk Assessment (ID.RA):**			
		ID.RA-1: Asset vulnerabilities are identified and documented			
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources			
		ID.RA-3: Threats, both internal and external, are identified and documented			

		ID.RA-4: Potential business impacts and likelihoods are identified			
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk			
		ID.RA-6: Risk responses are identified and prioritized			
	Risk Management	**Risk Management Strategy (ID.RM):**			
		ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders			
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed			
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis			
PROTECT(PR)		**PROTECT (PR)**			
	Access Control (PR.AC)	**Access Control (PR.AC):**			
		PR.AC-1: Identities and credentials are managed for authorized devices and users			
		PR.AC-2: Physical access to assets is managed and protected			
		PR.AC-3: Remote access is managed			
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties			
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate			
	Awareness and Training (PR.AT)	**Awareness and Training (PR.AT):**			
		PR.AT-1: All users are informed and trained			
		PR.AT-2: Privileged users understand roles & responsibilities			
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities			
		PR.AT-4: Senior executives understand roles & responsibilities			
		PR.AT-5: Physical and information security personnel understand roles & responsibilities			
	Data Security (PR.DS)	**Data Security (PR.DS):**			
		PR.DS-1: Data-at-rest is protected			
		PR.DS-2: Data-in-transit is protected			
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition			
		PR.DS-4: Adequate capacity to ensure availability is maintained			
		PR.DS-5: Protections against data leaks are implemented			
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity			
		PR.DS-7: The development and testing environment(s) are separate from the production environment			
	Information Protection Processes and Procedures	**Information Protection Processes and Procedures (PR.IP):**			
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained			
		PR.IP-2: A System Development Life Cycle to manage systems is implemented			
		PR.IP-3: Configuration change control processes are in place			
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically			
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met			
		PR.IP-6: Data is destroyed according to policy			

		PR.IP-7: Protection processes are continuously improved			
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties			
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed			
		PR.IP-10: Response and recovery plans are tested			
		PR.IP-11: (cyber)security is included in human resources practices (e.g., deprovisioning, personnel screening)			
		PR.IP-12: A vulnerability management plan is developed and implemented			
	Maintenance (PR.MA)	**Maintenance (PR.MA):**			
		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools			
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access			
	Protective Technology (PR.PT)	**Protective Technology (PR.PT):**			
		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy			
		PR.PT-2: Removable media is protected and its use restricted according to policy			
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality			
		PR.PT-4: Communications and control networks are protected			
DETECT (DE)		**DETECT (DE)**			
	Anomalies and Events (DE.AE)	**Anomalies and Events (DE.AE):**			
		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed			
		DE.AE-2: Detected events are analyzed to understand attack targets and methods			
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors			
		DE.AE-4: Impact of events is determined			
		DE.AE-5: Incident alert thresholds are established			
	Security Continuous Monitoring (DE.CM)	**Security Continuous Monitoring (DE.CM):**			
		DE.CM-1: The network is monitored to detect potential (cyber)security events			
		DE.CM-2: The physical environment is monitored to detect potential (cyber)security events			
		DE.CM-3: Personnel activity is monitored to detect potential (cyber)security events			
		DE.CM-4: Malicious code is detected			
		DE.CM-5: Unauthorized mobile code is detected			
		DE.CM-6: External service provider activity is monitored to detect potential (cyber)security events			
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed			
		DE.CM-8: Vulnerability scans are performed			
	De	**Detection Processes (DE.DP):**			

		DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability			
		DE.DP-2: Detection activities comply with all applicable requirements			
		DE.DP-3: Detection processes are tested			
		DE.DP-4: Event detection information is communicated to appropriate parties			
		DE.DP-5: Detection processes are continuously improved			
RESPOND (RS)					
	Resp	**Response Planning (RS.RP):**			
		RS.RP-1: Response plan is executed during or after an event			
	Communications (RS.CO)	**Communications (RS.CO):**			
		RS.CO-1: Personnel know their roles and order of operations when a response is needed			
		RS.CO-2: Events are reported consistent with established criteria			
		RS.CO-3: Information is shared consistent with response plans			
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans			
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader (cyber)security situational awareness			
	Analysis (RS.AN)	**Analysis (RS.AN):**			
		RS.AN-1: Notifications from detection systems are investigated			
		RS.AN-2: The impact of the incident is understood			
		RS.AN-3: Forensics are performed			
		RS.AN-4: Incidents are categorized consistent with response plans			
	Mitigation (RS.MI)	**Mitigation (RS.MI):**			
		RS.MI-1: Incidents are contained			
		RS.MI-2: Incidents are mitigated			
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks			
	Improveme	**Improvements (RS.IM):**			
		RS.IM-1: Response plans incorporate lessons learned			
		RS.IM-2: Response strategies are updated			
RECOVER (RC)					
	Reco	**Recovery Planning (RC.RP):**			
		RC.RP-1: Recovery plan is executed during or after an event			
	Improveme	**Improvements (RC.IM):**			
		RC.IM-1: Recovery plans incorporate lessons learned			
		RC.IM-2: Recovery strategies are updated			
	Communications (RC.CO)	**Communications (RC.CO):**			
		RC.CO-1: Public relations are managed			
		RC.CO-2: Reputation after an event is repaired			
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams			

Appendix F SCORE SHEET – COMPANY A

Appendix is removed because of confidentiality

Appendix G SCORE SHEET - COMPANY B

Appendix is removed because of confidentiality

Appendix H SCORE SHEET - COMPANY C

Appendix is removed because of confidentiality