Leiden University

Master ICT in Business

An Enterprise Architecture Approach to Implementing the NIST Cyber Security Framework.

Name: Cedric Hoogenboom
Date: 03-04-2019
Supervisor: Bas Kruiswijk
2nd supervisor: Mohamed Atef

MASTER THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Abstract

In February 2013, an Executive Order was signed by the U.S. to increase the state of cyber security of critical infrastructure, which was tasked the National Institute of Standards and Technology (NIST) to create a cyber security framework. In its core this framework consists of five functions: identify, protect, detect, respond and recover. Since its introduction in 2014, the NIST Cyber Security Framework (CSF) has been adopted by more and more organizations in different sectors around the world. The NIST framework is considered a useful, but complex system. Due to this complexity a simplification or guidance is needed, which we introduce in this thesis.

The link between enterprise architecture and information security has long been separated with security architecture as a separate domain. The Open Group Architecture Framework (TOGAF) handles security separately, as it is infrastructure that is rarely visible to the business function. Security architecture has its own methodologies, views and frameworks, of which the Sherwood Applied Business Security Architecture (SABSA) is the most popular.

This thesis introduces an enterprise architecture viewpoint that can assist organizations using enterprise architecture with the implementation of the NIST Cyber Security Framework. We have performed literature research to provide background and conducted expert interviews to gather the input for the viewpoint. Candidates with experience advising clients as experts and candidates carrying the responsibility themselves have been interviewed, to find out what processes, technologies and elements take place in which category of the NIST framework.

The final viewpoint is constructed by going through each subcategory of the NIST framework's core to see how enterprise architecture could assist in those steps. The resulting modeling techniques and example elements can be used to document and visualize steps in the framework, or parts of the existing or to-be architecture. Due to the considerable size of this viewpoint it is split into parts for each function of the framework. The relevant architectural elements, relationships, and actors are shown for each subcategory of the framework. This results in guidance how enterprise architecture can help with the implementation of the framework. All modeling is performed in ArchiMate, an open modeling language specifically developed for enterprise architecture.

Besides this viewpoint a combined process for the implementation has been introduced. NIST has provided seven steps for implementing this framework, which we have mapped onto TOGAF's Architecture Development Method (ADM). Using this combined process, organizations can implement the framework in a single architecture development cycle.

The NIST Cyber Security Framework is a large and complex framework for improving cyber security management. The viewpoint and process introduced in this thesis help to reduce this complexity and make it more applicable for organizations using enterprise architecture. Organizations can follow the process to adopt the NIST CSF within an architecture development cycle, and use elements in the viewpoint to clarify the output, steps taken, and the changes to be made in the architecture. The viewpoint introduced in this thesis has grown quite large. To this end, organizations implementing it should not strive to implement all elements, but use them where necessary.

For demonstration, this viewpoint has been applied to the ArchiSurance case study. Three views of the existing enterprise architecture of the case study have been modified using elements as described by our viewpoint.

Acknowledgements

First and foremost I would like to express my thanks to my first supervisor Bas Kruiswijk for his support, patience, and guidance throughout the process of this thesis. I would also like to thank Mohamed Atef as second supervisor, who has been more and more involved near the end of the process to get me in the right direction. Without their help this thesis would not have been what it is today.

This thesis has been written in the context of an intership at PwC's Cyber, Forensics & Privacy business unit. I would like to thank PwC for the opportunity, support and means to write my thesis there. Special thanks go out to Pablo Gonzales Soto, who has guided me throughout the internship, and Abdullah Rasool for all the support and help.

This research would have never been possible without the people who have made time to be interviewed: Jan Visscher, Silvia Knitl, Bart Spijkervet, Dennis Switzer, Fred Wijnsma and Jessica Conquet. To them I would also like to express my thanks.

Lastly I would like to thank all of my family and friends who have supported me throughout my studies, and have had the patience allowing me to finish them with this thesis.

Contents

1 Introduction

Over the past years, more and more organizations have appeared in worldwide media with coverage of security breaches, often with Distributed denial-of-service attacks (DDoS) or attacks resulting in the leaking of end users' passwords, credit card information or personal data. Due to the large effect of these breaches and regulations forcing organizations to disclose breaches to the public, highly visible breaches occur with growing regularity. This leads most technology executives to believe they are losing ground to attackers (Bailey, Miglio, & Richter, 2014).

As Ekstedt and Sommestad (2009) have pointed out, "security is inherently suffering from a weakest-link syndrome" (p. 1), as often only a single weakness might be needed to cause a significant cyber breach. If one link is missing altogether, the entire chain becomes useless (Sherwood, Clark, & Lynas, 2009). There are two approaches to developing a secure architecture, a 'built-it-in' and a 'bolt-it-on' approach (The Open Group, n.d.). Although the latter is implemented more often, security professionals agree that the built-in approach is far more effective.

With executive order 13636, U.S. President Obama directed the National Institute of Standards and Technology (NIST) to form standards, procedures and guidelines to develop a voluntary framework to reduce cyber risk to critical industries (NIST, 2018). This NIST Cyber Security Framework (CSF) consists of three parts: the framework core, the framework implementation tiers and the framework profiles. Since its introduction, the framework has also been implemented by many organizations outside of U.S. critical industries, and is slowly becoming the de facto standard for implementing cyber security controls (Greenwald, 2017).

Wrenn (2017) note the importance of the NIST CSF, but also it's complexity: "the NIST Cybersecurity Framework is by far the most comprehensive framework, but it is also the most complex to navigate". This complexity notes that a simplification or guidance might be desired.

2 Objectives

The Open Group (2018) have stated that "security concerns are pervasive throughout the architecture domains and in all phases of the architecture development. Security is called out separately because it is infrastructure that is rarely visible to the business function". Furthermore, security architectures generally have their own methodology, views and viewpoints (The Open Group, 2018). It appears however, that security concerns nowadays might not be rarely visible to the business function anymore. Cyber security is no longer just an IT issue; it is a risk management and board issue that cuts across every organization

(Saito, 2016). This claim is supported by a large study performed by McKinsey, in which 70 percent of the respondents in an executive function within a financial institution believe that cyber security is a strategic risk for their companies (Bailey et al., 2014). With the overall business security landscape changing and the fact that The Open Group states that security concerns are pervasive in all architecture domains and phases of development, one could argue that it can no longer be seen as “rarely visible to the business function” (The Open Group, 2018). In this research this claim will also be checked by expert interviews.

The ‘language’ that security architects speak is most often that of the SABSA (Sherwood Applied Business Security Architecture) Framework (Sherwood et al., 2009), an architecture framework that is very similar to, but developed independently of, the Zachman framework (John A. Zachman, 1987). For most management functions and consultancy purposes, these frameworks can be considered too technical or abstract. To this end, The Open Group Architecture Framework (TOGAF) provides views and viewpoint as a way to elaborate complex architectures to different types of stakeholders, such as top management (The Open Group, 2018).

The NIST CSF operates at a high level within the governance of organizations, which directly affects technical components, tools and processes. Because enterprise architecture can act as a bridge between IT and governance, it is a perfect tool to make this adoption clear. At the moment of writing however, no translation or link to TOGAF as an enterprise architecture framework has been published.

The goal of this research is to use enterprise architecture to assist organizations in implementing this framework. Based on the different functions of the NIST framework core (identify, protect, detect, respond and recover), we will create a viewpoint to help visualize what types of processes, components, technologies and principles take place at what point in the architecture. Organizations can use this viewpoint to reduce the complexity of implementation mentioned by Wrenn (2017).

This study fits into the field of enterprise architecture and security architecture, but also the fields of information security and risk management. The research consist of literature review and expert interviews.

The outcome of this research could be used to help organizations arrange or revise their enterprise architecture in a way that it is protected from external cyber threats, based on their maturity or desired tier of protection. These tiers will reflect the implementation tiers of the NIST framework, ranging from partial to adaptive. This does not necessarily reflect an organization’s maturity, but the required level of protection. For example, financial institutions should be in a higher tier of protection than a local sports club, as the chances of advanced threats against financial institutions are much higher than most other types of organizations. The outcome of this thesis should help implementing the NIST framework for organizations by simplifying it, providing ways of making the progress, goals and elements clear to stakeholders. By doing so, we help to protect organizations’ data, intellectual property, reputation, and equally important: the end users’ private data.

2.1 Research Questions

To address the issues presented in the previous section, the following research question (RQ) will be analyzed:

RQ 1. *What does an enterprise architecture viewpoint and process for implementing the NIST Cyber Security Framework within enterprise architecture look like?*

As mentioned in section 2, the goal of this research is to use enterprise architecture to assist organizations with implementing the NIST CSF, which is encompassed in this research question. In order to answer this research question, the following sub-question (SQ) will be researched:

SQ 1. *What processes take place within the different functions identify, protect, detect, response & recover of the NIST Cyber Security Framework?*

SQ 2. *What does a TOGAF enterprise architecture viewpoint look like as a reference to implement the NIST Cyber Security Framework?*

SQ 3. *What does the combined process for implementing the NIST Cyber Security Framework and the TOGAF Architecture Development Method look like?*

The final output of RQ 1, and therefore of this thesis, is a TOGAF viewpoint that can assist organizations with the adaption of the NIST framework. The goal of SQ 1 is to find out what steps organizations have taken or would like to take with unlimited resources in each of the categories of the framework, which will be answered by performing expert interviews and literature research. In these expert interviews we will find what the adoption of the NIST framework means in practice. Together with literature research, this should provide us with an idea of what technologies and tools are available, what measures are to be taken and what organizations should take into account for this adaption.

The knowledge and information we have gathered in answering SQ 1 will be used as input for answering SQ 2. In that phase, we will design the viewpoint itself. The output of SQ 1 will be categorized and translated to architecture. For the visualization and modelling, we will use and extend the ArchiMate modelling language. This will result in an enterprise architecture viewpoint, which answers SQ 2.

This viewpoint alone will not be enough to answer the main research question. Essential to this is the process, of how an organization can adopt this viewpoint. By analyzing literature from NIST (2018) as well as TOGAF (The Open Group, 2018), we will combine processes into one. The resulting process will be a mapping of steps NIST provides to implement the framework (NIST, 2018), with TOGAF's Architecture Development Method (ADM) (The Open Group, 2018). This will result in a process that can be used to develop an enterprise architecture with NIST Cyber Security Framework adopted.

As this thesis will be written within the context of an internship at the cyber security department of PwC, its outcome will be (mostly) confidential. The cyber security department resides within the business unit Cyber, Forensics & Privacy.

3 Method

In this section, each of the steps in answering the research questions will be elaborated upon. Each research question represents a phase in the research. The first phase will be to provide background and the current state of the art, which will be done by performing literature research. The output of this phase will be used in the next phase, which is to conduct interviews. After these interviews some additional literature research may be required. The output of the literature research phase and of the interviews will both be used as input for the third phase: the construction of a viewpoint and a process. After this is completed the final phase will be to validate this viewpoint in practice. This process is visualized in figure 1.

3.1 Literature Research

First we will provide background using literature research. This will provide insight *why* we use certain frameworks and standards, such as the NIST CSF itself, but also TOGAF for enterprise architecture and SABSA for security architecture. We will provide definitions for subjects that we use throughout the thesis, such as cyber- and information security and enterprise architecture. The frameworks will be analyzed and compared. This will provide us with a state-of-the-art, from where we can determine which frameworks and what literature to use in the following phases. We will gather the required literature mostly digitally by means of Google Scholar, Google, Leiden University's catalogue and PwC's intranet, but some paperback books will also be utilized.

3.2 Interviews

In this phase we will answer SQ 1 using qualitative research in the form of semi-structured expert interviews. Afterwards, the interviews will be processed, encoded and reviewed. The goal is to get an idea of how the NIST CSF would be used in practice, and how enterprise architecture can be of value to its implementation. We will find examples of principles and in what categories these can be divided, and find what types of tools and systems are used in practice. This phase will add to the literature research in the first phase, as the related domains generally are rooted more in practice than in theory or literature. Figure 1 also shows a flow going back from the interviews-phase to the literature research-phase. This is because at some points, subjects will come up in the interviews that will need further literature research. The output of that research can be used in the next round of interviews, creating continuous flow between literature research and interviews.

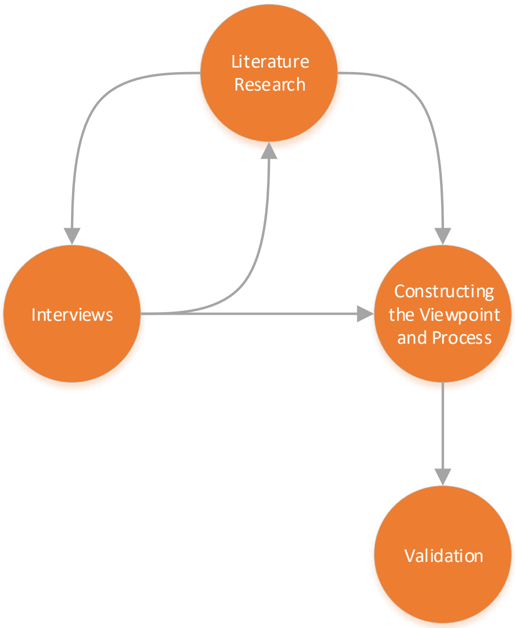


Figure 1: Research process visualized as phases providing input to other phases.

3.2.1 Selection of candidates

The success of this phase depends highly of which subjects will be interviewed. To collect the required data, potential interview candidates are selected based on experience with assisting clients as expert with- or carrying the responsibility of architecture or information security within an organization.

The first set of interviews has focused on the link between enterprise- or security architecture and information security. During these interviews a second strategy for selecting candidates quickly arose. As elaborated upon in section 5, these interviews focused on top management as a stakeholder and quickly identified a differentiation in the candidates to come. The need for a risk-based approach arose, and from literature we have later identified the NIST Cyber Security Framework as a risk-based approach to managing information security. As the NIST framework cannot be seen as a purely technical implementation or purely risk management framework, input from both sides is needed. Candidates who have experience in enterprise architecture often do not have experience with information security or the NIST framework. This created a differentiation in the further selection of candidates: ones that focus on enterprise- or security architecture combined with information security (group A.), and ones that focus on the NIST framework and its elements in practice (groups B.).

Both groups of interviews are aimed at candidates that have experience with assisting clients as an expert in these areas. However, a different side of this experience will be with the people not advising organizations, but leading the process within the organization themselves. Therefore we have added a third group of interview candidates, one that focuses on people who have carried the responsibility themselves (group C.). This group will be arranged under the group focused on the NIST framework in practice, as we will go into details on their current, intended or desired measures for each of the framework's categories. The whole selection procedure is visualized in figure 2. In order to gather qualifying candidates, before the selection a list of qualifications has been made to ensure the quality of the output and the amount of experience. This list can be found in annex A.

3.2.2 Interview questions

The questions used for interviewing are listed in appendix B, with a general and a specific set of questions for each group of interviewees. The idea is to follow a natural flow, and to let the interviewees first talk about their experience in the fields. Listing experiences will likely already point out some practical

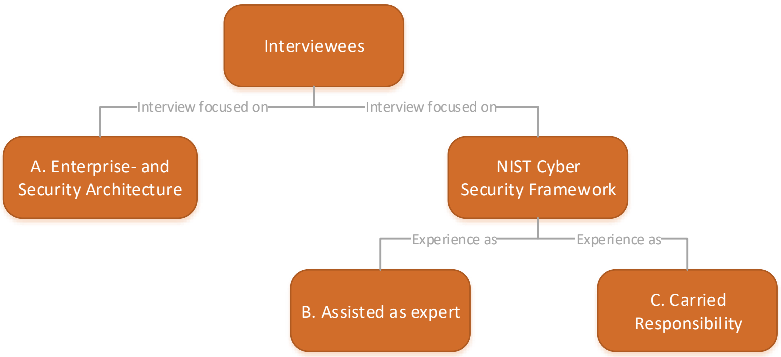


Figure 2: Differentiation in interview candidates.

problems within the field, as well as general opinions. We will start with enterprise architecture, then move to security architecture and the relationship between the two fields. Here we also check if the frameworks found in the first phase correspond with practice.

For the interviews in group B and C, the core questions are question 10 and its sub-questions in the second page of appendix B. This is where the we can gather the interviewee's experience needed to answer the technical parts of SQ 1. The interviews in group A focus more on the governance and risk management side of implementing the NIST framework. In group C we have tried to gather both types of data. For interview 5, the fact that we have interviewed a security officer with a technical background helped to make this possible.

Finally the interview addresses another point that followed from the literature research phase, focuses on the stand of TOGAF that security is infrastructure that is pervasive throughout the architecture development process, but should be considered separately as it does not provide value. Some doubts on this stance are identified in the literature research phase, in the interviews we will analyze the stance of the interviewees.

3.2.3 Analysis

After the interviews have been conducted, we will analyze them using the Grounded Theory (Martin & Turner, 1986). We will use the steps provided by Grounded Theory Online (2016):

1. **Identify substantive area** or the area of interest or expertise. In this thesis this step is described in section 4, and to a lesser extend in sections 1 and 2. In our research design, this step takes place in phase 1.

2. **Collect data** related to the area described above. This is the conduction of interviews in this thesis, or the start of phase 2. After we have conducted interviews we will transcribe the results, which also happens within this step.

3. **Open code** the transcriptions of the interviews. This identifies concepts, themes and subjects within the transcript. According to Grounded Theory Online (2016), this step happens simultaneously as the collection of data. The *open* part of open coding means you code for anything and everything you can find.

4. **Write memos** to identify possible theories, concepts, relationships or other things that may come to mind during coding.

5. **Selective code** follows when the open coding phase has stopped, and core categories and main concerns should be identified. This should lead towards conclusions based on the data.

6. **Find theoretical codes** by sorting memos and forming the theory in a repeated process.

7. **Integrate with theory.** In our research design, this is where phase three begins. Using the output from the literature research and the output of the previous steps of Grounded Theory, we can start to form a viewpoint. This is where the arrows from phase 1 and 2 come together in phase 3 of figure 1.

8. **Write up theory**, and form the final viewpoint, conclusions and report.

3.3 Construction of a viewpoint and process

The output of this thesis will be in two parts, a viewpoint and a process, both aimed at assisting organizations in adopting the NIST Cyber Security Framework. In the third phase, this output will be created based on input from the literature research and the interviews. This phase reflects RQ 2 and SQ 3.

3.3.1 Viewpoint

To answer SQ 2, we will analyze the output of the interviews and literature research and create the first part of the output of the research: a viewpoint for assisting organization in adopting the NIST Cyber Security Framework. We will model in the ArchiMate language (The Open Group, 2017), where will will first identify the viewpoint's stakeholders, their concerns, the purpose of the viewpoint (deciding, designing or informing) and the scope (overview, coherence or detail). Based on the output of the literature research and of the interviews (see figure 1), we can then determine the components of the viewpoint. We will not only introduce the concepts and notations used for creating a view, we will introduce a practical example of how such a view might look. It will highlight the relationships between the NIST CSF functions and the technology or governance that achieves those functions. To get an example that can be easily understood and generalized for organizations to apply, we will use the ArchiSurance case study by ArchiMate (Jonkers, Band, Quartel, & Lankhorst, 2016).

3.3.2 Process

Assisting organizations in adopting the NIST CSF would not be complete by just providing a viewpoint, guidance on how to get there is also needed. We will introduce a process that organizations can use, given they already have a TOGAF enterprise architecture in place. This will, just as the viewpoint itself, be done with output from the literature research- and interview phase. NIST provides steps in its literature on implementing the cyber security framework, in the background literature these steps as well as TOGAF's Architecture Development Method (ADM) are elaborated upon. In this phase we analyze and compare these two processes. By mapping the steps from NIST onto the ADM, we will show where the activities of NIST take place within the architecture development process. This allows organizations working with the ADM to adopt the framework within the known architecture development process. This provides us with a high level overview, we will also go more into detail on adopting the viewpoint. These two processes are not the same, as the NIST framework is much more extensive than the viewpoint we provide.

In the interviews, we will also inquire on how to implement the framework. The insight gained there will also provide input for the process.

3.4 Validation

Ideally, we would implement this viewpoint on an organization within the financial sector that intends to adopt the NIST framework. If this does not turn out to be possible, we will apply this viewpoint onto the ArchiSurance case study by Jonkers et al. (2016), in which ArchiMate is applied to a fictional organisation in the financial sector. This will allow us to check if RQ 1 has been answered.

4 Background

In this section, the background of this thesis is sketched by providing an integrative literature study. In the previous sections, we have mentioned a number of frameworks such as the NIST CSF, TOGAF and SABSA. In this section we will elaborate on them, and define why we have chosen to use these frameworks.

4.1 Architecture

Before conceptualizing security- and enterprise architecture, we first need to look at its context and origins. The most well-known and widely used definition of architecture is that of ISO/IEC 1471:2000: "The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" (p.3). This standard has however been superseded by ISO/IEC 42010:2011, in which it is slightly altered: "(system) fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution" (p. 2). Besides the phrasing and order of elements these definitions can mostly be considered as the same.

The Open Group (2018) adds the following to the definition of ISO/IEC 42010:2011: "The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time". With this, a differentiation is made between the design of the system itself and of the components making up that system, both encompassed in the concept of architecture. This is reflected in the different architectures, layers and views that TOGAF encompasses, in which components making up the architecture and their relationships and evolution can be specified just as detailed as the architecture in general.

One definition that is also not to be overlooked is that of John. A. Zachman (1997), who was the first to handle the concept of enterprise architecture. He describes architecture as a "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)" (p. 5). This definition focuses on the goals, where the definition from TOGAF focuses on the content making up the architecture. The Open Security Architecture combine the definition of Zachman with that the second part of the TOGAF definition: "The design artifact describe the structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time".

4.1.1 Enterprise Architecture

When we make the link from architecture to Enterprise Architecture (EA), we will also need a good definition of an enterprise itself. The Open Group (2018) defines an enterprise as "the highest level (typically) of description of an organization and typically covers all missions and functions. An enterprise will often span multiple organizations".

When we apply the definition of architecture to an enterprise as a whole, we can form an idea of the concept enterprise architecture. According to The Open Group (2018), "the purpose of enterprise architecture is to optimize across the enterprise the often fragmented legacy of processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the delivery of the business strategy". This allows organizations to stay adaptive and in line with the business strategy and goals. Lankhorst (2009) defines enterprise architecture as "a coherent whole of principles, methods, and models that are used in the design and realization of an enterprise's organizational structure, business processes, information systems, and infrastructure" (p. 3). Literature such as (Kotusev, 2016), (Gosselt, 2012) and (Umeh, Dagli, & Miller, 2007) agree that the de facto standard enterprise architecture framework is TOGAF (The Open Group, 2018), which we will go more into detail on further in this section.

By combining the dimensions business, technology, application and infrastructure, enterprise architecture is often used as a tool to achieve alignment between business- and IT mission, vision and goals. IT and business alignment remains a pressing concern for IT practitioners (Chan & Reich, 2007), to which EA has always been relevant as solution (Clark, Barn, & Oussena, 2012). EA is specifically useful to this end as it enforces an architect to think from the business (or IT in some cases) goals, and creates blueprints to achieve those goals.

4.1.2 Security Architecture

Thorn, Christen, Gruber, Portman, and Ruf (2008) have defined Security Architecture (SA) as "a cohesive security design, which addresses the requirements (e.g. authentication, authorization, etc.) – and in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied where. The design process should be reproducible" (p. 1).

As mentioned in section 2, enterprise- and security architecture are often separated from each other. The Open Group (2018) state that "security concerns are pervasive throughout the architecture domains and in all phases of the architecture development. Security is called out separately because it is infrastructure that is rarely visible to the business function". Basically, as expected from the term, security architecture is like enterprise architecture but applied to security in general. This includes all types of security, of which for example information security, physical access gates and the encryption of customer data. Just like enterprise architecture, this results in many different architectures and views for different stakeholders and concerns. In section 4.2.5 we will go more into details about one of the most popular security architecture framework, SABSA (Sherwood et al., 2009).

The difference between enterprise- and security architecture lies, as the names suggest, that security architecture focuses on the security of an organization and all of its components. Enterprise architecture deals with as-is and to-be states of the organization, security architecture makes sure that the security of all components is up to the task. Security architecture goes beyond just cyber- or information security, risk management for example is also an important part of a security design.

4.1.3 Stakeholders and concerns

The term stakeholder is defined by The Open Group (2018) as "an individual, team, organization, or class thereof, having an interest in a system". This very wide definition in this context basically means anyone or anything who could be involved with, could influence or will have to work with the architecture. The architect and top management are of course important stakeholders, but a user who will eventually work with it should also be considered. Along with views, viewpoints and concerns stakeholder management is an important process within TOGAF's Architecture Development Method.

ISO/IEC/IEEE 42010 (2013) uses the term concern as any topic of interest pertaining to the system, which are held by one or more stakeholders. Stakeholders themselves can hold one or more concerns. A concern of an end user could for example be the usability and the degree of user-friendliness, while for the CFO the cost implication will be much more important.

4.1.4 Reference Architecture

The Open Group (2018) defines a reference model as "an abstract framework for understanding significant relationships among the entities of an environment, and for the development of consistent standards or specifications supporting that environment". It is a more high-level model of what it references, used as a basis for education and explaining standards to non-specialists (The Open Group, 2018). OSA (n.d.) define a reference architecture as "something that describes a 'to be' state and should reflect accepted best practices". In a document created for to define the concept reference architecture, the U.S. Department of Defence defined it as "an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions" (Department of Defense, 2010). In that sense, when we talk about an enterprise reference architecture, we refer to a higher-level, more abstract framework of an enterprise architecture that can be applied to multiple organizations by implementing the details, like a blueprint for which the details can be filled in for implementation. A reference architecture will often be targeted towards a certain type or group of use cases, which can be for example for information management within the Dutch government (NORA) or for municipalities (GEMMA).

4.1.5 Views and Viewpoints

The downside of an enterprise architecture is that it can become a large, complex whole of models and principles, which in the end can be hard to comprehend for anyone but the architect. To that end, most architecture frameworks make use of views and viewpoints as an abstraction of the architecture tailored to certain concerns or stakeholders. In a view an architect can elaborate parts of the architecture relevant to specific stakeholders and their concerns while leaving out unnecessary information (Lankhorst, 2009). In this section we will elaborate on the definition of and the difference between views and viewpoints.

According to ISO/IEC/IEEE 42010 (2013), an architecture view "addresses one or more of the concerns held by the system's stakeholders. An architecture view expresses the architecture of the system-of-interest in accordance with an architecture viewpoint (or simply, viewpoint)" (p. 6), where a viewpoint prescribes how the view addresses particular concerns of the stakeholders within the architecture (Lankhorst, 2009, p. 48). In other words, a viewpoint describes a way of looking at an architecture, where a view is what you would see from where you are looking (Lankhorst, 2009, p. 49). For example, the architecture viewpoint of a user can be comprised of the all the ways that user interacts with a system, without any technical details where the viewpoint of a developer might contain more technical details and tools, and will not contain things as live data and customers (The Open Group, 2018). A viewpoint can be seen as a reference or abstraction of a view: "viewpoints define abstractions on the set of models representing the enterprise architecture, each aimed at a particular type of stakeholder and addressing a particular set of concerns" (Lankhorst, 2009, p. 171)

In the specification of the ArchiMate modelling language, The Open Group (2017) helps architects select the purpose and content relevant for the stakeholder's concern while defining and classifying viewpoints (p. 107). The purpose dimension is supported by the categories designing, deciding and informing, indicating if the viewpoint will be used to respectively support architects and designers in the design process, assist managers with decision-making or to inform any other stakeholder about the enterprise architecture (The Open Group, 2017, p. 108). The content dimension is supported by the categories details, coherence and overview, specifying the relevant aspect and layers. Views on the detailed level typically contain only one level and one aspect and is mostly used for the design and implementation. On the coherence abstraction level a view spans multiple layers or aspect, typically for operational management stakeholders. Finally on the overview level a viewpoint addresses both multiple layers and multiple aspects, and provides an overview of the view to top-level management and decision-making (The Open Group, 2017, p. 108). Previous versions of ArchiMate included a visualization technique to indicate the classification, but this has been removed as of ArchiMate 3.0.1. The structure of this visualization can be seen in figure 3.

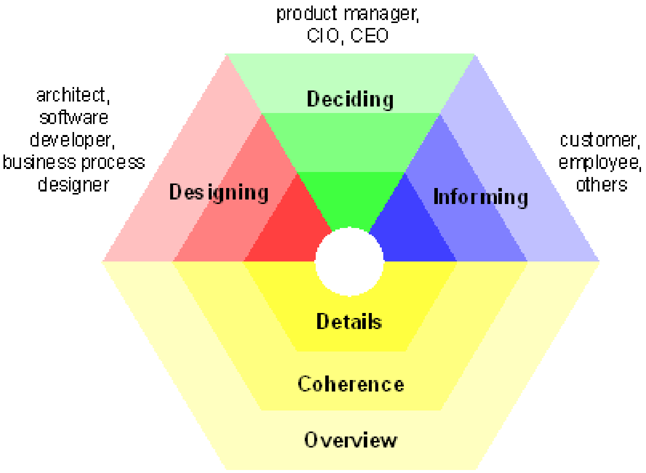

product manager, CIO, CEO
architect, software developer, business process designer
customer, employee, others
Deciding
Designing
Informing
Details
Coherence
Overview

Figure 3: ArchiMate viewpoint classification (The Open Group, 2017).

4.1.6 Zachman Framework

The first mention of an enterprise architecture framework is that of Zachman (John A. Zachman, 1987). This framework has evolved heavily since its introduction in 1987, and is still in use in many organizations worldwide.

The centre of the Zachman Framework is a 6 by 6 matrix, with each cell representing a design artifact for the corresponding view and aspect. Its main advantage is that it is easy to understand, but there are some drawbacks. One of the biggest drawbacks is that the relationships between the cells are not well specified, and in comparison to for example TOGAF, it is only a content framework which does not really cover governance (Lankhorst, 2009). TOGAF is nowadays however more widely used than the Zachman Framework, as it is much simpler to implement and understand with fewer perspectives.

4.1.7 TOGAF

The Open Group Architecture Framework (The Open Group, 2018), or often abbreviated as TOGAF, is an enterprise architecture framework developed by The Open Group in 1995. Since then many different versions have been released, at the moment of writing the current version is TOGAF 9.2, released in 2018 (The Open Group, 2018).

TOGAF consists of the following main components: an Architecture Capability Framework, an Architecture Development Method (ADM), an Architecture Content Framework, and an Enterprise Continuum (Lankhorst, 2009). Figure 4 shows the relationship between these components.

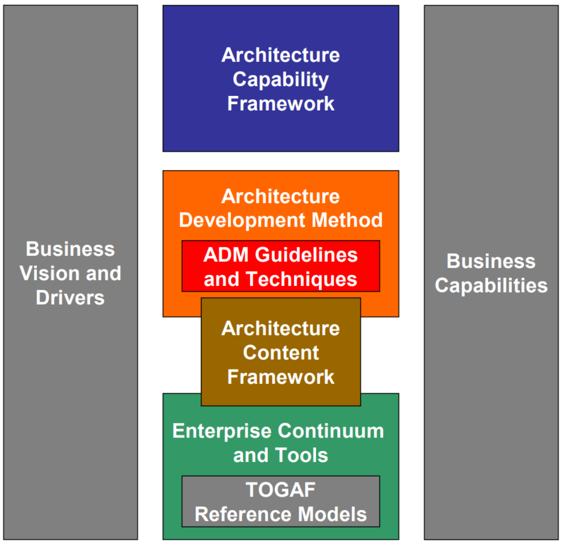

Business Vision and Drivers
Architecture Capability Framework
Architecture Development Method
ADM Guidelines and Techniques
Architecture Content Framework
Enterprise Continuum and Tools
TOGAF Reference Models
Business Capabilities

Figure 4: TOGAF 9 (Lankhorst, 2009, p. 26).

The TOGAF Architecture Capability Framework "addresses the organization, processes, skills, roles and responsibilities required to establish and operate an architecture function within an enterprise" (Lankhorst, 2009, p. 25). This framework helps to establish an architecture function within an organization (The Open Group, 2018). By first understanding the organization's structure, skills and capabilities architects can better understand and model it.

At the core of TOGAF is the ADM, its Architecture Development Method. This method describes the Architecture Development Cycle, a continuous process that is iterative between and within phases. An overview of the structure of the Architecture Development Cycle can be seen in figure 5, which is elaborated upon in further in this section. At the centre of this cycle is the Requirements Management phase, which is a continuous phases to ensure that at each phase the appropriate governance processes are handled and reflected (The Open Group TOGAF-SABSA Integration Working Group, 2011). The other phases follow an iterative order, each using the output of the previous steps as input:

Preliminary. Before the process starts, an architect should first define the context and scope. This is done by asking where, what, why, who, and how the architecture process is done.

A. Architecture Vision. In the first 'real' phase, an aspirational vision of the capabilities and business value of the result is developed. Among others stakeholders, concerns, business requirements are identified, and a statement of work is gathered from the organization's management.

B. Business Architecture. The first layer of the architecture itself is the business layer, as it is a prerequisite for architecture work in any other domain (data, application, technology). TOGAF recommends creating it by following the steps:

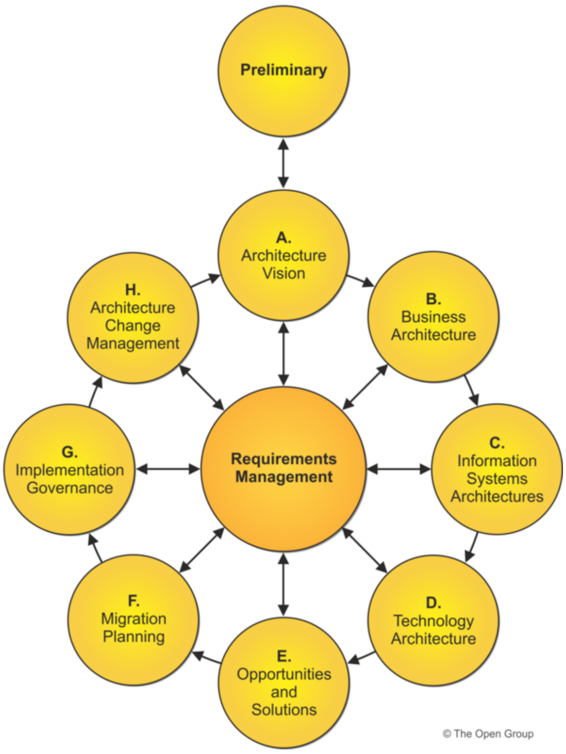

Preliminary
A. Architecture Vision
B. Business Architecture
C. Information Systems Architectures
D. Technology Architecture
E. Opportunities and Solutions
F. Migration Planning
G. Implementation Governance
H. Architecture Change Management
Requirements Management
© The Open Group

Figure 5: TOGAF Architecture Development Cycle (The Open Group, 2018).

1. Select reference models, viewpoints, and tools
2. Develop baseline business architecture description
3. Develop target business architecture description
4. Perform gap analysis
5. Define candidate roadmap components
6. Resolve impacts across the architecture landscape
7. Conduct formal stakeholder review
8. Finalize the business architecture
9. Create the architecture definition document

C. **Information Systems Architecture.** This step creates two architecture layers at once: the data- and the application architecture, both to support the business architecture developed in the previous step. The process to develop these is the same as mentioned in step B, with 'business architecture' substituted by the corresponding architecture.

D. **Technology Architecture.** The last architecture layer to be developed is the technology layer, which is also developed using the process in step B. The technology layer is developed last as it supports the data and application architecture.

E. **Opportunities and Solutions.** In steps B to D, a baseline and a target architecture was developed. In this phase a gaps between these are analyzed. This is also the initial step on the creation of the implementation and migration plan, which is completed in Phase F.

F. **Migration Planning.** The implementation and migration plan are completed in this phase, by among others estimating required resources and project timings.

G. **Implementation Governance.** All the information for successful management of the various implementation projects is brought together in this phase. All implementation projects are started parallel to this phase, it is important that this process is governed in a defined way.

H. Architecture Change Management. In the last phase, the goal is to ensure that the original target business value is achieved. This is done by among others monitoring, managing, and implementing new requirements.(The Open Group, 2018)

Throughout the Architecture Development Cycle, deliverables and other outputs are created. The Architecture Content Framework specifies which phases produce what deliverables, and provides a Content Metamodel. In the Architecture Content Framework three categories to describe architectural work products are used: deliverables, artifacts and building blocks. The Content Metamodel describes which building blocks exist, in what form, and how the building blocks relate to each other (The Open Group, 2018). The Architecture Content Framework also considers an architecture to be composed of a business architecture, data architecture, application architecture and a technology architecture (Lankhorst, 2009). In the ArchiMate modelling language, these architectures are referenced in the layers business, application and technology.

4.1.8 Modeling

As modeling is a large part of the output of this thesis, the type and language of the model needs to be formally determined as well.

In software engineering, the standard for modeling is the Unified Modeling Language (UML). Since it has been adopted as standard by the Object Management Group in 1997, it has been applied to many other disciplines than just software engineering. Sousa, Caetano, Vasconcelos, Pereira, and Tribolet (2007) have applied UML to enterprise architecture to model business roles, activities and entities in a organization-, business-, and information architecture.

Another popular modeling language is BPML, which (as the name Business Process Modeling Language suggests) origins from business process design. For the modeling of enterprise architecture the scope of BPML is however too narrow, as it is restricted to business processes and therefore only the business domain.

A modeling language specifically designed for enterprise architecture has been introduced by Lankhorst (2004) named ArchiMate. Now adopted as standard by The Open Group, ArchiMate is still under development with version 3.0 introduced in 2016 (The Open Group, 2017). Although the ArchiMate and TOGAF standard are both maintained by The Open Group, the two are not explicit to each other. TOGAF can easily be modeled in other languages or standards, and other architecture frameworks can easily be modeled in ArchiMate. The two are naturally compatible. Where TOGAF has the main dimensions of business-, application-, technology and infrastructure, ArchiMate uses business-, application- and technology. With ArchiMate 3.0, a physical layer has been introduce which aligns more with the TOGAF dimensions (The Open Group, 2017).

Given the choice for TOGAF as an enterprise architecture framework in section 4.1.9, the logical choice for a modeling language or standard would be ArchiMate. ArchiMate also has very clear and extensive documentation for modelling viewpoints, which we will use in section 6.2.

4.1.9 Conclusion

In this section, four enterprise architecture frameworks are described, all of (slightly) different categories. The Zachman framework is historically the first framework to handle the enterprise as a whole, but can be overly complex and only provides a content framework. TOGAF is an open standard that uses a content framework, architecture development method, enterprise continuum, and fewer dimensions than the Zachman framework.

For this thesis, we will build upon TOGAF as it covers by far most of the enterprise. Although Zachman is a comprehensive framework as well, the power of TOGAF lies in its process: “Zachman tells you how to categorize your artifacts. TOGAF gives you a process for creating them” (Sessions, 2007). Besides the ADM, TOGAF also has the benefit of it being an open standard. This simplifies adaption for organizations, as all documentation is openly available. We will build upon this process and unify it with the steps for implementing the NIST Cyber Security Framework (see section 4.2.6). This will result in a process using which an organization can adopt the NIST framework within a TOGAF ADM cycle. These results are specified in section 14.

For the modelling part of the viewpoint we will use ArchiMate, as it is a formally defined modelling language specifically created for enterprise architecture. It is framework-independent, so the final output will be created for TOGAF but can easily be ported to another framework such as the Zachman Framework.

4.2 Cyber Security

The term *cyber security*, or often abbreviated as simply *cyber* has nearly gained buzzword status over the past few years. When people talk about for example cyber security, a cyber breach, or cyber warfare, the definition of the word 'cyber' is often vague and undefined.

Many scientific publications also use the terms cyber security and information security interchangeably, while the two are not synonymous (Von Solms & Niekerk, 2013). In this section we will conceptualize a definition and elaborate on the difference between the two concepts.

4.2.1 Information Security

ISO/IEC 27002 (2013) defines information security as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (p. ix). If we split the term into 'information' and 'security', the term information itself is defined in ISO/IEC 27000 (2012) as "an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected" (ISO/IEC 27000, 2012, p. 12). Information can be stored both digital as material, as well as in the form of knowledge of employees, and can be transmitted by means of for example courier, transmission or verbal communication (p. 12). Whitman and Mattord (2011) uses the Merriam-Webster definition of the term security: "the quality or state of being secure—to be free from danger" (p. 8). In their paper they name the following six layers of security that organizations should have to protect its information: physical security, personnel security, operations security, communications security, network security and information security. This last layer, information security, is then defined as "to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology" (Whitman and Mattord, 2011, p. 8). In this definition, we can see the terms confidentiality, integrity and availability central to the protection of information assets. These terms are often referred to as the as the information security 'CIA triad' or 'CIA triangle' (Cherdantseva & Hilton, 2013). This CIA triad is a model based on a paper by Saltzer and Schroeder (1975), in which the terms confidentiality, integrity and availability are named as respectively 'unauthorized information release', 'unauthorized information modification' and 'unauthorized denial of use'. The term CIA triad first appeared around 1986-1987, when it rapidly gained popularity among information security practitioners (Cherdantseva & Hilton, 2013, p. 3). According to Whitman and Mattord (2011), "the C.I.A. triangle model no longer adequately addresses the constantly changing environment" (p. 8). They add accuracy, authenticity, utility and possession to the list of concepts (p. 12-15).

In this CIA triad, confidentiality refers to the core of what most people think about with breaches, basically who has access to what systems. A breach in confidentiality could for example be the leaking of credit card data because a web application is not secure. Integrity reflects not if the information is there or not, but the fact that the information itself is *correct*, and not modified by a third (unauthorized) party. ISO/IEC 27000 (2012) define integrity as the "property of protecting the accuracy and completeness of assets" (p. 5), indicating the focus on the information itself, not the way it is accessed or who has access to it. Finally availability refers to whether or not the information can be accessed. It has become common for websites to be attacked by means of Distributed Denial of Service (DDoS) attacks, which directly affects the availability of the information. When a website is suffering from a DDoS attack, the information might still be valid and no unauthorized people may have access. However, due to the website itself not being online, the information is not available anymore.

ISO/IEC 27000 (2012) note that in addition to confidentiality, integrity and availability, properties such as authenticity, accountability and non-repudiation could also be involved. While some may seem to overlap with the 'original' C.I.A. triad, they do provide some different views. An obvious overlap would be between authenticity and confidentiality, as both deal with user access management. If we take for example email messages, we assume that the sender is who the `from` field says he is. A breach in authenticity would be if for example by means of email spoofing a third party pretends to send an email as someone else (Whitman & Mattord, 2011), while a breach in confidentiality in such case would be that a third party reads an email he or she is not supposed to. Another example of attacks based on authenticity are `phishing` attacks, in which attackers attempt to obtain personal or financial information by posing as organizations such as banks (Whitman & Mattord, 2011), for example by creating a fake log-in page. Cherdantseva and Hilton (2013) have reviewed and compared different information security goals, among other the ones named in this section. They define accountability as the ability of the system to hold users responsible for their actions in case of misuse of information (Cherdantseva & Hilton, 2013, p. 7). While this might not directly impact the security of information, employees handling that information might be more aware with high levels of accountability in place. The same could be said for auditability, which Cherdantseva and Hilton (2013) define as a system's ability to "conduct persistent, non-bypassable monitoring of all actions performed by humans or machines within the system" (p. 7).

The only aspects proposed by Whitman and Mattord (2011) we have not yet described in this section are accuracy, utility and possession. They describe that information has accuracy when it is what the user expects it to be, and is free of errors. Information that is intentional or unintentional altered would not be accurate. This could be because of a breach in confidentiality and a third party has had the ability to alter the data, but could also be the result of human error. Utility determines the quality or state of having value of the data (Whitman & Mattord, 2011, p. 15), where for example U.S. Census data can be hard to comprehend or overwhelming for private citizens, but can have great value to politicians planning their campaign.

4.2.2 Cyber Security

Von Solms and Niekerk (2013) state that cyber security and information security are related to one another, but not analogous. Often cyber security is viewed as a subset of information security or vice versa, but according to Von Solms and Niekerk (2013) they are intersecting sets with "information based assets stored or transmitted using ICT" (p. 101) at the intersection. Von Solms and Niekerk (2013) list cyber bullying, disruptions of home automation systems, lost revenue due to illegal file sharing and cyber terrorism as examples of cyber security events that do not affect information's confidentiality, integrity, or availability. Information security is also not a subset of cyber security, as information not stored or transmitted using ICT are not part of cyber security (p. 100-101). For protecting a paper archive with a physical lock (with an old-fashioned key) could not be counted as cyber security but would classify as information security. The relationship between these fields can be seen in figure 6, with in the intersection between the two fields information and communication technology security. This intersection handles the security of information based assets stored or transmitted using ICT.

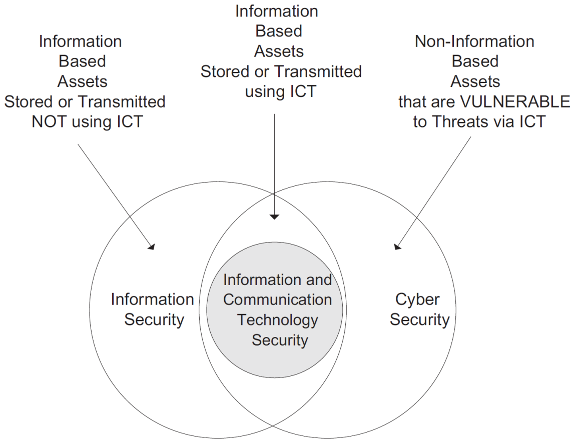

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Figure 6: The relationship between information- and cyber security (Von Solms & Niekerk, 2013).

In this thesis, the focus lies mainly on the intersection between information- and cyber security, visualized in figure 6 as information and communication technology security. Although the NIST Cyber Security Framework (see section 4.2.6) has *cyber* security in its name, it is partly based on the ISO 27000 family. The ISO standards do focus on information security rather than cyber security, as clearly defines it focuses on information security: “Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation” (ISO/IEC 27002, 2013, p. ix). This thesis utilizes the ISO 27000 family and NIST Cyber Security Framework extensively, which is why we will focus on information security rather than cyber security.

4.2.3 Threat Intelligence

Interview 3 and 4 noted the use of threat intelligence, as knowing what threat actors are active in your sector and how they work can be vital to the information security of an organization. As specified in section 3, this section (and the next) were added after interesting topics came up in the interviews that require additional literature research.

Shackleford (2015) defines threat intelligence, or Cyber Threat Intelligence (CTI), as “the set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators”. CTI helps security practitioners with recognizing the indicators of cyber threats and attack methods in order to respond in a timely manner (Conti, Dargahi, & Dehghantanha, 2018). The higher implementation tiers of the NIST Cyber Security Framework (section 4.2.6) also focus on if information on threats and attacks is shared with other organizations and services.

Within threat intelligence the protection against Advanced Persisitent Threats (APT’s) is key. Bejtlich (2010) defines the term APT in three terms: it is *advanced* in the sense that the adversary is conversant with computer intrusion tools and techniques and is capable of developing custom exploits, *persistent* in that the intend of the threat is to achieve a mission and that the adversary receives directives and works towards goals, and a threat in the sense that the adversary is organized, funded, and motivated. For defence against APT’s, Hutchins, Cloppert, and Amin (2011) have developed the Cyber Kill Chain model to identify patterns and phases that attackers might go through. Understanding these phases of an attack can give more insight in how that attack can be stopped or detected. The phases of the Cyber Kill Chain are reconnaissance, weaponization, delivery, exploitation, installation, command & control (C2) and action on objectives. According to interview 4, the goal of threat intelligence is to provide knowledge on these attack actors and methods, and share that knowledge with organizations to provide better information security.

4.2.4 Security Operations Center

Another topic that arose in interview 4 and led to additional literature research was that of a Security Operations Center (SOC). According to Bidou (2005), a security operations center is a “generic term describing part or all of a platform whose purpose is to provide detection and reaction services to security incidents” (p. 1). In that article he describes five operations that a SOC performs: the generation, collection, storage, analysis, and reaction of security events. Interview 4 described how a SOC can perform operations from the NIST CSF’s protect, detect and response categories, which fits with those five operations.

The term SOC originates from physical security of an organization’s premise on a technical level, where it is mostly concerned with access monitoring, physical barriers and alarms (Nadel, 2004). In this thesis, when we mention a SOC we refer to the information security type of SOC, sometimes referred to as an ISOC or CSOC (for Information- or Cyber Security Operations Center). A different term is a Network Operations Center, which Hernandez (2018) describes as “a command center designed to manage, control and monitor one or more network infrastructures” (p. 2). The difference between a NOC and a SOC is that the NOC is more occupied with the day-to-day network operations and management, such as DDoS Attacks, power outages, network failures and port management, where the SOC handles real-time monitoring, cyber intel collection (as described in the previous section), threat assessment and forensics (Hernandez, 2018).

4.2.5 SABSA

For security architecture, the most used and well-known framework is the SABSA (Sherwood Applied Business Security Architecture) Framework (Sherwood et al., 2009). Although SABSA was originally based on the Zachman Framework (John A. Zachman, 1987), a white paper has been published on integrating SABSA with TOGAF by The Open Group TOGAF-SABSA Integration Working Group

(2011). This White Paper tries to combine the best of both frameworks. SABSA mainly focuses on risk management and on business requirements, as the model enforces that all steps return to requirements engineering.

SABSA is an open standard, consisting of the SABSA framework, model, methodologies and processes (Sherwood et al., 2009). The SABSA model comprises six layers, corresponding with six different views for stakeholders. These layers contain the conceptual, logical and implementation levels of abstraction mentioned by Oda, Fu, and Zhu (2009) and adds three additional levels for different stakeholders. Which views correspond with what layers and stakeholder can be seen in table 1. In this model, the security service management architecture is often placed vertically across the other five layers, as "security service management issues arise at each and every one of the other five layers" (Sherwood et al., 2009, p. 8). The schematic model of the layers of can be seen in figure 7.

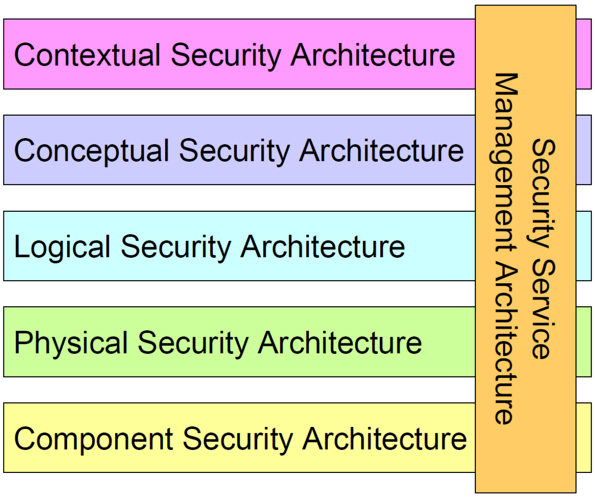

Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

Figure 7: The SABSA model for security architecture (Sherwood, Clark, & Lynas, 2009, p. 9).

Just as in the Zachman framework, the horizontal axis of the 6 × 6 matrix is formed by asking the questions what, why, how, who, where and when for each layer. These questions result in respectively the assets, motivation, process, people, location and time relevant to the layer. Besides the model and matrix, SABSA consists of the a development process indicating which steps should follow which while developing a security architecture, a life cycle to provide context in which the development process can be seen, and a business attributes profile to provide linkage between the business requirements and the technology- or process design (Sherwood et al., 2009).

Business View	Contextual Security Architecture
Architect's View	Conceptual Security Architecture
Designer's View	Logical Security Architecture
Builder's View	Physical Security Architecture
Tradesman's View	Component Security Architecture
Service Manager's View	Security Service Management Architecture
Service Manager's View	Security Service Management Architecture

Table 1: SABSA views and corresponding architectures (Sherwood, Clark, & Lynas, 2009, p. 9).

SABSA also provides a unique requirements engineering technique, which ensures that security architects do not necessarily have to start with a 'blank slate'. This Business Attribute Profile provides an extensive list of security requirements examples encountered in many real-world situations. At first these were mostly ICT focused, later Sherwood et al. (2009) added a second set of more high-level business-focused attributes. The attributes are listed figure 8, and organised under seven group headings.

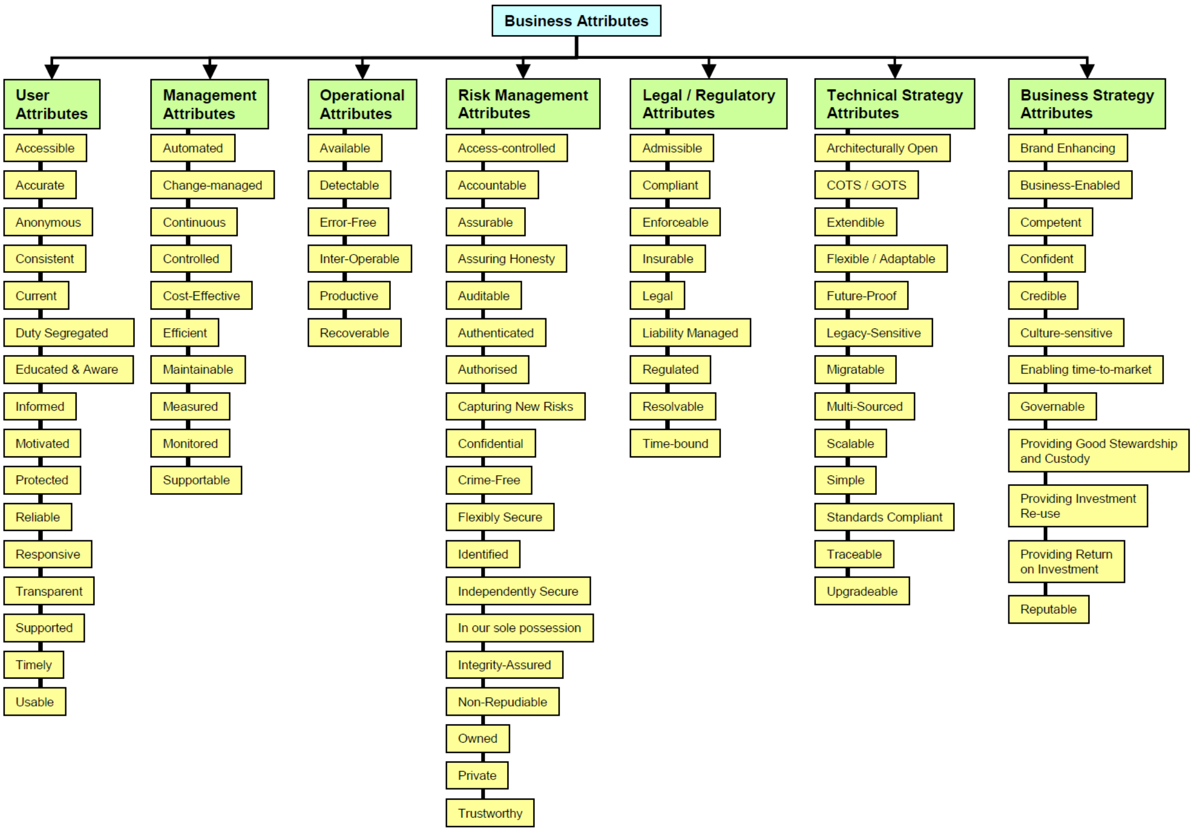


Figure 8: The SABSA Business Attribute Profiles (Sherwood, Clark, & Lynas, 2009, p. 20).

4.2.6 NIST Cyber Security Framework

With Executive Order 13636, U.S. President Obama directed the National Institute of Standards and Technology (NIST) to form standards, procedures and guidelines to develop a voluntary framework to reduce cyber risk to critical industries (NIST, 2018). This NIST Cyber Security Framework (CSF) consists of three parts: the framework core, the framework implementation tiers and the framework profiles. Since its introduction the framework has been implemented by many organizations, and is slowly becoming the de facto standard for implementing cyber security controls (Greenwald, 2017).

The Core of the NIST Framework "provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes" (NIST, 2018, p. 6). It consists of four functions: identify, protect, detect, respond and recover, that can be used by companies to manage their cyber security risk. The functions themselves consist of categories (such as identity management, asset management and detection process), subcategories (supporting the outcomes of the categories), and informative references (standards, guidelines and practices illustrating the outcomes of the subcategories) (NIST, 2018).

The NIST framework implementation tiers "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk" (NIST, 2018, p. 8). The four tiers range from partial to adaptive, and are determined by an organization's risk management process, integrated risk management program and external participation. Organizations can also check the implementation tiers of other organizations, to find possible weakest links within their supply chain.

An organization's profile is "the alignment of the functions, categories, and subcategories with the business requirements, risk tolerance, and resources of the organization" (NIST, 2018, p. 11). The profile is the part that can be customized to the organization's goals and resources, and can describe the current or the desired cyber security management state.

When looking at the NIST framework core[1], we can see that each subcategory is supported by a number of informative references (NIST, 2018, Appendix A.). These references indicate the standards or frameworks the subcategory was based on, which can be one or more of the following standards, frameworks and best practice guides (NIST, 2018):

- NIST SP 800-53 Rev. 4
- ISO/IEC 27001:2013 (see section 4.2.7)
- COBIT 5
- CIS CSC
- ISA 62443-2-1:2009
- ISA 62443-3-3:2013

The SABSA initiative have responded to the popularity of the NIST framework by forming a working group to create a SABSA Enhanced NIST Cybersecurity Framework (SENC). This framework however still seems to be in development at the moment of writing.

In order to implement or improve a cyber security program NIST (2018) provides seven steps that can be repeated to continuously improve cyber seurity capabilities. We will elaborate on these steps here, and link them to the ADM in section 6.4.

1. **Prioritize and scope.** In the first phase an organization determines its business goals and high-level priorities. With the business goals in mind, the scope of the implementation can be set and a target implementation tier can be selected.

2. **Orient.** Once the scope has been set, systems and assets, regulatory requirements and an overall risk approach can be identified. In this phase an organization can also identify threats and vulnerabilities applicable to those systems and assets.

3. **Create a current profile.** The categories and subcategories of the framework core contain many assets, some of which the organization might have already implemented. In this phase a current profile is made to establish the as-is state.

4. **Conduct a risk assessment.** Different types of industries bring very different levels of cyber security risks. To that end an organization should analyze the environment, identify threats and use internal and external sources to gather information about the likelihood of an event.

5. **Create a target profile.** In step three a profile for the as-is state of cyber security management was established, in this step the to-be state is defined. Besides the existing categories and sub-categories in the framework core, organizations are free to define new ones. This target profile should reflect the implementation tier set in step 1.

6. **Determine, analyze, and prioritize gaps.** After the as-is and to-be states are defined, it is time to analyze the differences between the two and create a prioritized action plan to address the gaps. The organization should determine resources, budgets and workforce necessary to implement within the plan.

7. **Implement action plan.** When the plan is made and the resources are determined, the last step is to execute that plan. The Framework provides further guidelines for each sub-category in the informative references of the framework core. (NIST, 2018)

[1] Excel sheet available at https://www.nist.gov/sites/default/files/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx

4.2.7 ISO 27000 Series

Besides the frameworks mentioned in this section, the security standards of ISO/IEC themselves are also intended to be used as guidelines or framework for managing information security, and many other frameworks are based on or compatible with the ISO 27000 family of standards (often abbreviated as ISO 27K). The goal of this family of standards is to help organizations implement an Information Security Management System (ISMS). In this section we will elaborate on these standards. The essence of and the relationship between the different standards within the ISO/IEC Information Security Management Systems family can be seen in figure 9. This figure also differentiates the standards into four levels: terminology, general requirements, general guidelines and sector-specific guidelines. Here we will go into detail on the first two levels, handle two of the general guidelines and leave the sector specific guidelines.

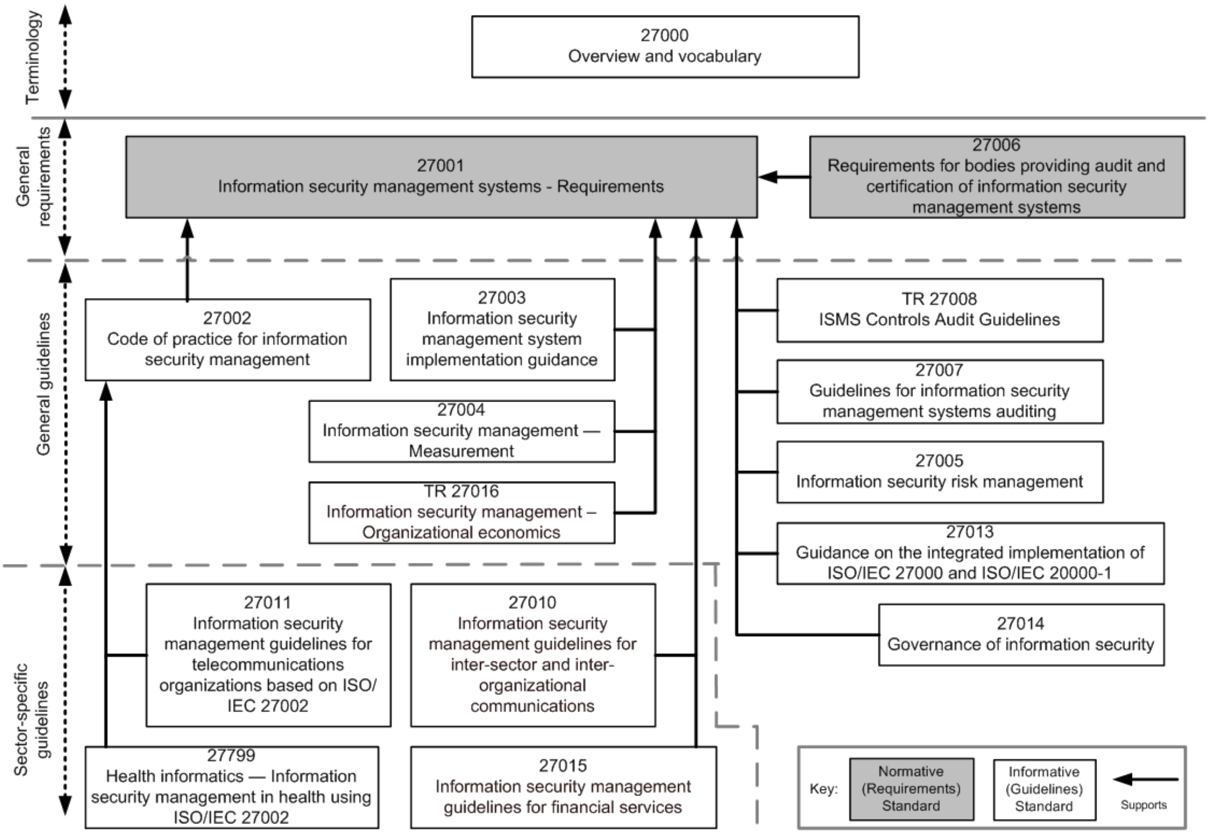

Terminology
General requirements
General guidelines
Sector-specific guidelines
27000 Overview and vocabulary
27001 Information security management systems - Requirements
27006 Requirements for bodies providing audit and certification of information security management systems
27002 Code of practice for information security management
27003 Information security management system implementation guidance
27004 Information security management — Measurement
TR 27016 Information security management – Organizational economics
TR 27008 ISMS Controls Audit Guidelines
27007 Guidelines for information security management systems auditing
27005 Information security risk management
27013 Guidance on the integrated implementation of ISO/IEC 27000 and ISO/IEC 20000-1
27014 Governance of information security
27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
27010 Information security management guidelines for inter-sector and inter-organizational communications
27799 Health informatics — Information security management in health using ISO/IEC 27002
27015 Information security management guidelines for financial services
Key:
Normative (Requirements) Standard
Informative (Guidelines) Standard
Supports

Figure 9: ISO 27k family of standards (ISO/IEC 27000, 2012).

In figure 9 it can be seen that the terminology level is formed by only ISO 27000, titled Overview and vocabulary. This standard contains (beside figure 9 itself) mostly definitions and background and introduces Information Security Management Systems. An ISMS contains all procedures, policies, guidelines and associated resources and activities organizations can use to protect it's information assets (ISO/IEC 27000, 2012, p. 12). As is often the case with ISO standards, the approach for implementing an ISMS is based on the Plan-Do-Check-Act cycle, also known as the Deming cycle. To establish and maintain an ISMS, organizations need to undergo the following steps: identify information assets and associated information security requirements, asses and treat information security risks, select and implement controls to manage unacceptable risks, and monitor, maintain and improve the effectiveness of controls associated with information assets (ISO/IEC 27000, 2012, p. 15).

In the ISO 27001 standard, the requirements relevant to the ISMS introduced in ISO 27000 are elaborated upon. The design and implementation of these systems are influenced by an organization's "needs and objectives, security requirements, the processes employed and the size and structure of the organization" (ISO/IEC 27001, 2005, p. v). Organizations can be certified within the scope of ISO

27001, allowing them to show that they have successfully implemented an ISMS. Guidance and additional requirements for third parties to audit and certify organizations can be found in ISO 27006. An important part of ISO 27001 is Annex A., which is essentially a large list of objectives and controls that can be used to improve information security within an organization. These directives are not very elaborated, mostly formed up from one or more sentences, for example A.5.1.1: “An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties” (ISO/IEC 27001, 2005, p. 13). These controls directly relate to ISO 27002, which as can be seen in figure 9 provides guidance to ISO 27001. ISO 27002 has the same structure and numbering as Annex A., but provides much more details and information on the controls.

Another interesting standard within the guidance-level of figure 9 is ISO 27003, titled Information security management system implementation guidance. As the name suggests, this standards guides organizations with the implementation of an ISMS itself. ISO 27005 is focused on risk management, and introduces an information security risk assessment and treatment process. This process follows the following steps: asset identification, risk identification, risk assessment, risk evaluation and risk treatment. We will handle risk management somewhat more extensively in section 4.3.

Many frameworks exist that guide organizations in implementing a ISMS, often this process is based on the ISO 27000 family. One of these is the NIST Cyber Security Framework, which is described in section 4.2.6 of this thesis.

4.2.8 Other Frameworks

There are many other information- or cyber security frameworks available, so we will not go into details on all of them. One which does deserve attention within the context of this research is the Open Enterprise Security Architecture (O-ESA), created by The Open Group themselves. O-ESA is described as a “framework and template for policy-driven security” (Wahe and Petersen, 2011), indicating that it handles security on the level of the organization as a whole, driven by policies set by the business. Besides the frameworks described in this section, many other frameworks are out there such as one by Gartner, Rise, COBIT , and many more. To analyze and compare all of these would go beyond the scope of this thesis, so we will keep it at this.

In section 4.2.6, we have described the NIST Cyber Security Framework, which originates from U.S. legislation. In Europe, there are comparable legislations and standards in use or in development. The European Network and Information System Agency (ENISA) is tasked within the European Union to improve network and information security. Comparable with the U.S. executive order that led to the NIST CSF, the European Union has adopted the Network and Information Security (NIS) directive in 2016, for which the deadline to translate into national law was in May 2018. This directive is the first piece of EU cyber security legislation, it is expected to be expanded further in the near future (ENISA, n.d.). ENISA has published four guidelines to assist organizations on the NIS directive. This thesis however focuses on the U.S. NIST Cyber Security Framework, as this is much more practical, applied and in use by organizations. Enisa also has more applied frameworks, but these are often directed towards a more focused implementation — such as a framework for IoT security. The same applies for the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany.

4.2.9 Comparison of Frameworks

In this section, the word *framework* has been used often, and many times with different meanings. Some indicate an architectural framework, others are formed more of best-practices or principles. In this section the most used cyber security frameworks will be elaborated upon and a comparison will be made.

Oda et al. (2009) have reviewed some commonly used enterprise information security architecture frameworks, namely SABSA, the Gartner EISA framework, the Zachman framework and a framework by the Oakland University. In their analysis, they identify three common levels of abstraction used in all frameworks (in some frameworks under a different name): conceptual, logical and implementation. At the conceptual level an architecture a framework describes how it handles the confidentiality, integrity and availability (see earlier in section 4.2). The logical level of abstraction defines methods, strategies and techniques to accomplish the goals set in the conceptual level, and the implementation level defines resources needed to apply the other layers of abstraction (Oda et al., 2009).

Another review of enterprise security architecture solutions has been performed by Mees (2017) for military purposes, combining SABSA with TOGAF as "unfortunately, information security has long been considered a separate discipline, isolated from the enterprise architecture" (Mees, 2017, p. 9). As previously mentioned, in the relationship between the frameworks mentioned in this section the ISO 27000 framework forms a basis for many other frameworks. This applies for the NIST Cyber Security Framework, but does not apply for SABSA.

In this section we have described three frameworks of different types; one architecture framework, one ISO standard framework and one high level framework based on multiple other standards. As a security architecture framework, SABSA comprises the security measures of the entire organization. It is based on the Zachman framework, and is very extensive and can be hard to implement. The NIST Cyber Security Framework is not an architecture framework, but as it's name suggests a framework for improving critical infrastructure cyber security. The framework tries to accomplish this by combining many different best-practice guides, standards and frameworks into five categories to simplify implementation. The ISO 27000 family (as other families of standards mentioned, such as ISA) is not only meant for guidance and helping organizations improve their information security but provides certification that organizations can use to show their status and progress. NIST uses its implementation tiers as a guideline, which is not a checklist organizations can comply to and get a certification to show the outside world they comply. But as the framework is based on other standards, if organizations implement NIST successfully the step to certify against these standards is quite small.

The intend of this research is to introduce an architectural approach to adopting the NIST framework. Due to the fact that the NIST CSF is high level enough, we think that enterprise architecture can be of value in the implementation of the framework by introducing a way of modeling the output in each category. This method will be introduced in section 6.3.

4.3 Risk Management

Although risk management is a much broader field than we will handle here, some definitions are required for the final construction of the viewpoint. The NIST Cyber Security Framework states to identify vulnerabilities and threats within the risk assessment category, here we will define those concepts.

Spencer Pickett (2006) uses the following definition for the concept of risks: "any uncertainty about future events that impact an organization's ability to achieve its objectives. Risk is measured in terms of its impact and the likelihood that it materializes" (p. 42). Risk management is, as the name suggests, a management process of those risks to the enterprise. A basic risk management cycle that Spencer Pickett (2006) uses has the steps objectives, context, risk identification, risk assessment, risk management, and formal disclosures in a cycle with risk appetite in the center (Spencer Pickett, 2006). This process is of course simple an example, many risk management frameworks exist which may handle this differently. Risk appetite is a preference of an organization that determine how much risk it is willing to take, accept or avoid.

ISO/IEC 27000 (2012) defines a vulnerability as weakness of an asset or control that can be exploited by one or more threats (p. 17). ISO/IEC 27000 (2012) in turn defines a threat as a "potential cause of an unwanted incident, which may result in harm to a system or organization" (p. 16). These definitions shows that the concepts of assets, vulnerabilities, risks and threats are inherited linked: vulnerabilities in assets can pose a threat to an organization, which in turn introduces risks. Vulnerabilities can be seen as internal threats to the organization, but threats can also come from outside of the company, for example in the form of threat actors. Many different types of threats and vulnerabilities can be named, these are just a small sample to get an idea of the concepts and relationships. As Allen and Derr (2015) describes the relationship between the terms: an asset is what we're trying to protect, a threat is what we're trying to protect against, a vulnerability is a weakness or gap in our protection efforts and risk is the intersection of assets, threats and vulnerabilities (p. 12).

For risk response, there are basically four types of responses generally agreed upon: to accept, avoid, mitigate or transfer (Joint Task Force, 2018). Some sources and frameworks have the same types of responses under different names, avoid is for example also referenced as control, mitigate, reduce or modify, and accept can also be referred to as retain. Although to share the risk is not a synonym for transfer, we have chosen to group it under the same concept.

Interview	**Function**	**Years of experience**	**Expertise**	**Consultancy**	**Carried Responsibility**	**EA or SA**
1	Senior Manager	13	Cyber Security Governance, & Privacy, eID, Smart Mobility	Yes	No	Revised EA
2	Senior Manager	12	IAM, Security Architecture, Enterprise Architecture	Yes	No	Implemented SA
3	Senior Associate	4/14[2]	Offensive Security (Windows networks), Red team	Yes	No	No
4	Manager	9	Blue Team, Cyber Security Governance, SOC, Security Monitoring	Yes	No	No
5	Global Cloud Platform Director	18	Global Cloud Platform, Security Officer, Audit Framework	No	Yes	No
6	Global IT Security Officer	20	Security Officer, Security Management, Firewall Management, ISMS Implementation, Security Architecture	Not currently	Yes	Implemented SA

Table 2: Qualifications of interviewees.

5 Results

In this section we show the notable results from the interviews before we process the results into the viewpoint. All the results used to construct the viewpoint are handled in the next section, and fully shown in appendix C and D.

5.1 Interviewees

After the first and second interview, we quickly noticed that the comprehension of information security of top management will not be easily improved with enterprise architecture. Interview 1 and 2 however note that this might also not be necessary. Top management should not need to understand all the details, but should be aware of the risks each measure introduces or mitigates. These first interviews were aimed at finding out how enterprise architecture can be of value to the information security of an organization, the candidates however did not have experience with the NIST framework. Therefore we have divided the interviewees into ones that have knowledge of enterprise- and/or security architecture (group A.), and ones that have in-depth knowledge of the NIST framework or in-depth knowledge of its functions identify, protect, detect, respond & recover (group B.). As explained in section 3.2.1, we have also made a division between candidates that have advised as an expert and candidates that have carried the responsibility themselves. The latter makes up group C. To get a balance between these three groups, we have selected two candidates for each group. According to the research design, we have also made sure each of the candidates fits the qualifications in appendix A. Each candidate fit the qualifications amply, as can be seen in table 2. In the end, group A is made up of interviews 1 and 2, group B of interviews 3 and 4, and group C of interviews 5 and 6.

5.2 Questions

With that differentiation in candidates, the interview questions differed somewhat per group. For the enterprise- and security architecture focused interviews, the goal was to get an idea of the understanding and involvement of information security in management. Then we could find if and how our viewpoint could improve that understanding. For the second group of candidates the interviews had a more technical

[2] 4 years of experience in this field, 14 years in IT operations.

focus, where we tried to find out what examples of technologies and other implementation level elements are important in each NIST CSF function. With all questions we have tried to by as non-biased as possible.

To get the most creativity out of the interviewees, we have chosen to ask the candidates to imagine they are designing an organization from scratch, with no limitations such as budget or bureaucracy. How would they design the information security for that organization, where would they start, what components would they use? After that, we ask what difficulties they may face. Why is the scenario they have just described a 'perfect world' scenario? Then we can ask if these difficulties can be overcome by usage of architecture or other methods.

In each interview we have asked about experiences with the frameworks introduced in section 4: TOGAF, SABSA and NIST. As to be expected, none of the interviewees were experienced in all three, but we have gotten the required input on all of them. These results are elaborated upon more in section 4.1 and 4.2.

Lastly, we have put the following statement of TOGAF to the test: "security concerns are pervasive throughout the architecture domains and in all phases of the architecture development. Security is called out separately because it is infrastructure that is rarely visible to the business function" (The Open Group, 2018). We have asked all interviewees if they agree with this statement and compared their responses. In this, *visible to the business function* was translated as *has value to the business function.* We give an elaboration on these answers in section 5.3.3.

5.3 Notable findings

Besides the data we have gathered that we have used to develop the viewpoint, many other interesting topics were discussed in the interviews. In this section we will elaborate on some and compare the results between candidates.

5.3.1 Risk management

As mentioned in the beginning of this section, the first set of questions we have asked were aimed at finding out what the involvement and understanding of information security of top management is to get more insight on the governance side of the NIST framework. What we found in the interviews aimed at candidates group A, was that overall, this understanding is often low. Out of interview 1 followed that management should be more interested in the associated risks by means of business impact analyses. This can provide management with an understanding that if for example an organization's website is down for 5 minutes, exactly how much income they will miss. What technical measures have to be taken in order to reduce the risk to a certain level matters less to management than how much it will cost and what the effects will be to the risk. Interview 2 also highlighted the gap between the business and IT. When asked if our intended solution could help bridge that gap, the interviewee responded that some sort of translation is needed between the two worlds. For security the same need was identified, where the business needs to know the risk in order to understand the measures and costs, and the technical security specialists needs to translate the technical details into risk and costs.

Both interview 1 and interview 2 indicated that for the implementation, you should always start with the business. In interview 1 this was in the sense that when implementing an information security program, you should start at the highest level, with the organization's mission, vision and goals. Interview 2 pointed out that you should always find out the business goals behind a new technology or solution, as this is often overlooked. These two statements are much in line with TOGAF, in which the ADM also advises to start by finding the organization's mission, vision and goals, and create the business architecture before the technology architecture. This indicates that the choice for enterprise architecture linked to the NIST CSF, a high level framework for cyber security, is not far fetched.

One good example of where risk management and technical implementations meet is in Business Continuity Management (BCM), which was an interesting topic of interview 5. BCM is defined in ISO 22301 (2012) as "the process of identifying potential threats to an organization's business operations", and as a process "which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities" (p. 2). BCM deals with procedures as Disaster Recovery (DR), which is for example planning what needs to be done in case a large hack has occurred, or if a datacentre has been flooded and all data has been lost. The reason this falls under risk management is that it deals with risks an organization hopes to never encounter, but has to plan for them. The technical part can for example be the failover service of a datacentre. This allows an organization to switch all of their data and services from a datacentre for example in Germany to one in the United States almost instantly. Technically, this requires all data to be replicated in the second datacentre, which naturally increases the costs significantly. Management of the organization does not need to know exactly what techniques are used for the replication, but they should know what the costs are, that certain risks (e.g., the loss of data due to the flooding of a datacentre) are mitigated, and what risks are *not* mitigated (e.g., the leaking of customer data due to a hack). In the NIST framework the recover function deals with the restoring part of business continuity, the preparing (planning, making a failover technically possible) take place in the protect function.

5.3.2 Frameworks

In the literature research some frameworks offered much potential to be combined, referenced or used: TOGAF for enterprise architecture, SABSA for security architecture and NIST for cyber security. Although no one subject was proficient with all of these frameworks, we could get expert input for each of the frameworks for at least one of the subjects. The only exception here is TOGAF, which many interviewees know and had some experience with, but no subject has implemented or extensively used. There we can also rely on literature and own experience. We will go into detail her on SABSA and NIST, where most new insight was gained.

5.3.2.1 SABSA

The second interview was with a subject who has experience implementing SABSA at multiple clients, which provided us with much insight. One thing that was especially brought to our attention was the SABSA Business Attribute Profiling to categories requirements and make them clear for demonstration to stakeholders. The usefulness of this method was confirmed in interview 6, of which the candidate also has extensive experience with SABSA, and has at some point met its founder John Sherwood. After these interviews, we have done more literature research which resulted in the extension of section 4.2.5 with a part about Business Attribute Profiling. Based on this we have integrated this process in the combined process in section 6.4.

5.3.2.2 NIST Cyber Security Framework

After the first two interviews, we have searched for a risk-based approach to manage information security in literature, which resulted in focusing more on the NIST Cyber Security Framework. The candidate in interview 4 was at that moment engaged with a client where his advice to move from COBIT to NIST was approved, and the transition had began. He confirmed the use of the NIST framework as a risk-based approach, where he sees the use mostly as guidelines on what topics you should think of when implementing an information security program.

Most of the results on the NIST CSF from the interviews were on what technologies, principles and processes take place in each function. As these results are an extensive list we will not go into detail on all of them, the concepts from each interview mapped to subcategories in the framework can be found in appendix C. In this section we will go into detail on some other notable findings on the NIST framework.

Interview 6 also provided a critical note on the use of the NIST framework for implementing a security program. She stated that as the NIST CSF is based upon multiple (audit) standards, this is also that which the organization will be checked upon in the end. She provided an analogy to building a house: the architect is occupied with what the house will look like, the structure of the walls and to make sure it does not collapse. He does however not concern himself with what the valuator will eventually check upon when the house is finished. If you take that analogy back to our example, the security architect should be concerned with the specific case of an organization in order to keep it as safe as possible. An auditor will check upon the controls of the NIST framework (or in most cases, upon the standards it builds upon). She did specify that you need both in order to succeed, and she agreed with interview 4 that the NIST framework can be used as guidelines when implementing an information security program.

Out of interview 3 and 5 followed that an organization does not necessarily has to check all the boxes in each of the functions. If an organization is for example weak within the protect function it might compensate by investing more in the detect function or vice versa. An example of this was provided by an organization that was subject to a penetration test, and was not very strong with its protection as they had many different machines and servers without adequate patch management. They however compensated this by investing in an external detection service, this way the penetration testers were detected and blocked at the very beginning. The other way around could also be true, if the protection is so strong that nothing could come in, detection will not be as useful. However, interview 3 and 5 note that a balance between the two is advisable. Another relationship between functions that interview 3 pointed out is between detect and response. When an event is detected by a monitoring process or service, by definition the response to that event is handled within the response function. The monitoring itself would not provide any value if the response is not executed well or not in time, and vice versa would the response function be useless when no events are detected within the detect function. Therefore these two functions also provide a balance, and this points out that in order to be protected as an organization, a balance between all of the functions is recommended.

As indicated in the research design and figure 1 more specifically, the interviews could lead to additional literature research. This explains the arrows back and forth between the literature research- and interview phases in figure 1. A good example of this was threat intelligence, which arose in interviews 3 and 4. Both of these interviews noted the importance of identifying what the potential threat to an organization is, what the current state of that threat is, and to monitor attacks against other similar organizations in other regions. All of this comes together in a business process called threat intelligence, which we have included in the background section after these interviews. Another example is the Security Operations Center (SOC), a business department, team or external entity that transcends the NIST CSF functions and handles for a large part the protection, detection and response to external threats for the organization. This came up mostly in interview 4, after which we have also added a background section on it. The interview noted that the best way to implement such a SOC is to start small, use open source technologies that are sometimes available free and build up from that. Often when organizations implement such a process they invest high amounts of money, after which the result might not necessarily be better.

When implementing a monitoring function, according to interview 4 organizations are also often quick to outsource many parts. This interview noted however, that ideally there should be a balance between outsources monitoring and monitoring on premise. The outsourced party is likely better in detecting anomalies within the network and in detecting attacks, but an organizations own network engineers always know the network and the specific situation better. This is especially true when traffic needs to be blocked, the external SOC provider might consider something an attack while in fact it is a vital system activity. To get the most out of these situations, here a balance between the two is again needed.

5.3.3 Relationship between SA and EA

One of the intended outcomes of this viewpoint was to integrate parts of security architecture within enterprise architecture, to get the best out of both worlds and to create a common 'language' between the two disciplines. As we focused on interview candidates with an information security background, an understanding of TOGAF or other EA frameworks was not expected. To get their opinions on this, we focused on the reasoning of TOGAF why security concerns are separated: "security concerns are pervasive throughout the architecture domains and in all phases of the architecture development. Security is called out separately because it is infrastructure that is rarely visible to the business function" (The Open Group, 2018). Here The Open Group (2018) state that security is separate from 'regular' architecture because it is rarely visible to the business function. We have asked the interviewees on their stance, if they agree that security concerns are rarely visible to the business function or that it can be, in a way that it can provide value.

The results on this question varied, although no respondent fully agreed with TOGAF on that statement. All interviewees agreed that security concerns can provide some form of value, and thus can be visible to the business function. Several views where introduced which we will explicate here. One answer was consistent with the risk-based approach introduced in section 5.3.1. If the business is aware of the risks and costs, they can better decide what value they can get out of potential new solutions and measures. This is in line with the response of interview 4, which stated that security does not necessarily create value, but it does allow organizations to get the most out of existing business value. This interview also introduced a nice analogy with a sports car. If you buy a sports car, you will most likely not buy it because it has good brakes. Without the brakes however, you will likely be scared to drive faster than 20 km/h with it. Security is like those brakes, you do not necessarily get value out of it, but it does allow you to move faster, get more out of current and new innovations without constantly worrying.

Another view was that security rarely creates value, but should be there in order to protect the existing value. In some organizations, such as PwC, there are departments that do create value using security, but most will not. This interviewee did not think security will in the future be a qualifying feature, but at best will be a disqualifying feature.

One of the interviews in category C was with a global cloud director for a cloud service provider. They were early to set up an audit framework, focus on security and got certified. This allowed them to reach clients that they otherwise would have never reached, showing that it can be a qualifying feature.

In interview 6, on the topic of designing an architecture on an public cloud, the interviewee mentioned that integration of both the enterprise architecture and security architecture is needed from the start. If security is not integrated from the start, it is very hard to get the system secure later on. This is something we have hypothesized and derived from literature in section 2.

6 The Viewpoint

The purpose of this viewpoint is to assist organizations in implementing the NIST framework from an enterprise architecture view. In this section we will lay out the basic design decisions for our viewpoint, which we will model in the ArchiMate language (The Open Group, 2017).

TOGAF, ArchiMate and ISO 42010 all provide guidance on developing views and viewpoints, on which we will base the construction of our information security enterprise architecture viewpoint. As mentioned in section 4.1.5, viewpoints are references for views, and each view should be governed by one viewpoint within an architecture.

There are two ways of constructing views when no pre-existing viewpoint to base the view on is available. The first is ISO 42010 recommended practice, in which an architect develops a new viewpoint that will cover the outstanding need and generate the view from that viewpoints. The second method can be equally effective, in which an architect constructs ad *ad hoc* view for the specific system which is later generalized into a viewpoint which can be defined explicitly and saved into a library to be re-used (The Open Group, 2018). The viewpoint central in this thesis is developed using the first method, as views based on this viewpoint are implemented in the final validation phase in section 7.

TOGAF provides the following three concepts to guide the development of viewpoints(The Open Group, 2018):

- Selecting a key stakeholder
- Understanding their concern and generalizing/documenting those concerns
- Understanding how to model and deal with those concerns

This guidance is quite high level, and TOGAF, ArchiMate and ISO 42010 all encompass these elements in their definition of viewpoints. In section 4.1.8, we have determined to use the ArchiMate language to model our viewpoint. As a modeling language, ArchiMate provides the most detailed documentation for developing viewpoints of these three frameworks. ArchiMate provides a method for classification, which we will first do to show the scope and dimensionality in the next section. In this classification, we will also show the output of the first two concepts out of the three shown above. The third will be handled within the viewpoint itself in section 6.3.

6.1 Viewpoint classification

In ArchiMate, viewpoints are classified to specify which stakeholders and concerns are relevant, and what the scope and the purpose is. The two most important stakeholders identified in section 5 as the organization's security officer and the enterprise architect.

The purpose of a viewpoint can be determined in ArchiMate as one or more of the dimensions designing, deciding and detail. The implementation of the NIST framework is one that will have a large impact on the risk management of the organization, and could lead to organizational reforms. This indicates that the deciding purpose would be within the scope of this viewpoint, which is described by The Open Group (2017) as to "assist managers in the process of decision-making by offering insight into cross-domain architecture relationships, typically through projections and intersections of underlying models, but also by means of analytical techniques". This viewpoint will assist management by offering cross-domain relationships of how the NIST framework works. However, the purpose of this viewpoint could also be for a security officer to convincing management to implement this framework. To that end, the designing dimension is added as well. The informing dimension is not within scope, which would be aimed more at the employees or customers. An informing viewpoint on the NIST implementation could be for example on the impact of changes that will occur towards the employees, which could be added in a later stage after design is finished.

The identification of relevant stakeholders was a goal of the interviews. Many stakeholders were identified by the interviewees, not all of which were relevant. Often the end user was identified, which would be relevant for the implementation but not within this scope (but would fit in the detailed dimension). Following the purposes identified earlier, the architect stakeholder is identified as relevant due to the designing purpose. This can help the implementation itself, as many other architectures will have to be adjusted. Following the deciding dimension, the organization's security officer is most relevant. He can identify the risks best, and has the end responsibility over the security of the organization.

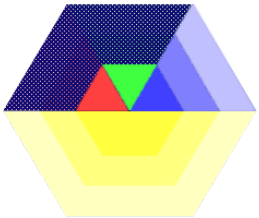
NIST Cyber Security Framework Adoption Viewpoint		
Stakeholders	Enterprise Architects, Security Officer	
Concerns	Implementing the NIST CSF and improving information security management	
Purpose	Designing, Deciding	
Abstraction Level	Coherence, Overview	
Layer	Business, Application, Technology and Motivation layers	
Aspects	Behavior, Active	

Table 3: ArchiMate viewpoint specification.

6.2 Construction of the Viewpoint

Finally we can combine the information gathered in the literature research and the interviews into the final output: a viewpoint organizations can use as guidance in adopting the NIST Cyber Security Framework. In this section we will first go into detail on the process we have used to construct the viewpoint.

First we have transcribed and analyzed all of the interviews. All of the answers on the different NIST functions were coded and divided into a matrix, showing the answers per category over each interview. These codes were then sorted, and the resulting list of codes was mapped onto the NIST Framework Core excel sheet[3]. This matrix and the sorted lists can be found in appendix C, the mapping of these concepts onto the NIST core in appendix D.

With the NIST CSF core as a starting point, we have gone over each of the categories and first determine whether or not it is in scope for this thesis. As the scope of the NIST framework is very wide, enterprise architecture cannot provide value to all aspects. An example of a category we have considered out of scope is RS.IM, improvements of the response function. It is of course vital to any process to include lessons learned to ensure continuous improvements, but enterprise architecture and more so our viewpoint cannot provide real added value to this. For each (sub-) category that we have considered out of scope we have included our reasoning into the text of section 6.3.

Next we check the mapping (appendix D) to see what the input from the interviews was for each specific subcategory. If no input from interviews was found we see if the text itself is clear enough to

[3] Excel sheet available at https://www.nist.gov/sites/default/files/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx

determine its intended goal. Here we also check the literature in the background or look for additional literature. If the goal of the subcategory is still unclear, we check the standards the control was based on to clarify it further, in most cases we can fall back to an ISO27001 control (see section 4.2.7).

If a category and its subcategories are considered within scope and the input is gathered and analyzed, we look at it step by step to see how a modeling technique could be used to visualize the output or make the process more clear. We have tried to keep the end goal of the category and how this modeling technique can be of value to this in mind. We will show an example of the process we have gone through for each subcategory with ID.AM-1: “Physical devices and systems within the organization are inventoried” (NIST, 2018). Interviews 1 and 4 add to this control that for identify an overview of all assets and the data-flows between them is needed. If an organization implements this subcategory, they would have to create this inventory of all assets, technologies and devices. Enterprise architecture can help by creating a method of modeling this inventory, so our viewpoint includes elements to show what assets and systems are located where in the organization, and how they can communicate with each other. That way the viewpoint can be used to create the inventory required by the NIST framework. Finally, we think of how we can translate these ideas into ArchiMate elements, relationships or techniques. In the case of this example it has resulted in multiple technology-layer elements to model different types of devices. These devices are extended with technology-layer software elements and different types of annotations for the other subcategories in the Asset Management category to form a way to inventory the physical devices, the types of software on them and the classification of those elements. The results can be seen in the first part of the next section.

6.3 The Viewpoint

As we have chosen to construct the view by handling each subcategory of the NIST framework, the size of the viewpoint has grown considerably. To make it more clear, we have split the viewpoint into one for each of the functions identify, protect, detect and respond. The end result is not a viewpoint in the sense that a single view can be modeled from it, it is a way of modeling and visualizing controls from the NIST framework or the output created at different phases of implementation.

As explained in the previous section, we will decide for each subcategory if it is within scope of this research. For the recover function, the smallest of the NIST CSF core, all of the categories were considered out of scope. Its categories cover recovery planning, improvements and communications. Within recovery planning the execution of the recovery plan is vital. These plans however are created in the protect function, where we handle its modeling and creation in the viewpoint. The execution is not something that enterprise architecture can be of value to. The same goes for improvements and communications, we do not consider these less important than the other categories but we do not think that a way of modeling can provide added value there.

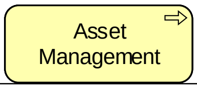
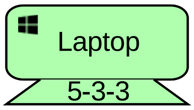
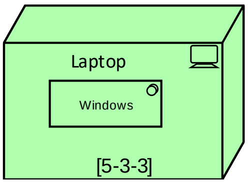
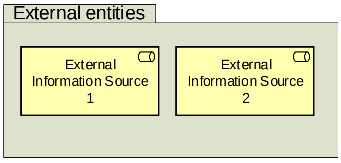
In the text below we have provided as much details as necessary to show which interviews or literature the input came from. For all subcategories that we have considered out of scope, the reasoning behind it is elaborated upon in the text of the relevant category. At the end of each part of the viewpoint, an example view will be provided to show the elements in use. These examples are not based on existing architectures but purely created to exhibit this viewpoint.

6.3.1 Identify

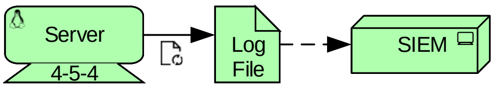
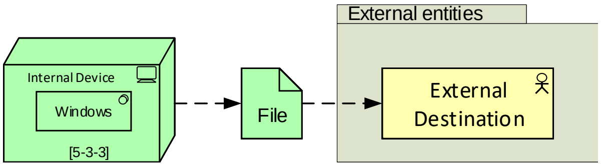
This viewpoint is to show the organization’s management of cyber security risk to systems, people, assets, data and capabilities (NIST, 2018). It can be used as a visualization of the output of all the activities within the NIST Identify function.

Stakeholders	Enterprise-, ICT- and security architects, security officer, asset management
Concerns	Identification of assets, risks, data and capabilities
Purpose	Informing, deciding
Scope	Business, technology, motivation, application

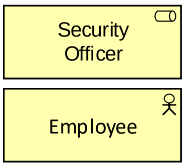
Asset Management (ID.AM) The first category of the NIST CSF is Asset Management, which requires an overview of assets to be developed. Such an overview can be modeled in ArchiMate, using the following elements: **Elements**

	Asset Management is an organizational process, visualized as an ArchiMate process.
 	Linked to NIST subcategory ID.AM-1, physical devices within the organization are organized and inventoried. Using the drawing below the devices, or groups of devices can be visualized. In the upper left corner software platforms can be shown, which is linked to ID-AM-2. In this example it indicates a Windows laptop. ID.AM-5 states that resources are prioritized based on classification, critically and business value. Based on the interviews, in this viewpoint this we have implemented this classification with a CIA rating of 1-5 in the bottom of the device. As the use of logo's can be hard to extend when many different types of software are to be identified, the software can also be visualized with an ArchiMate system software element shown in the bottom example. The classification can be shown at the bottom of the device between square brackets. Using this method, many different (vulnerable) types of software can be shown.
	Artifacts that may arise in this viewpoint can often come in the form of log files, which can be analyzed to detect suspicious behavior. This can also be shown in more details in the detect-viewpoint.
 External entities External Information Source 1 External Information Source 2	As part of the asset management process, ID.AM-4 specifies that all external information sources should be catalogued. This catalogue can be modelled as an ArchiMate group, in which the external sources are specified as roles.

Relationships

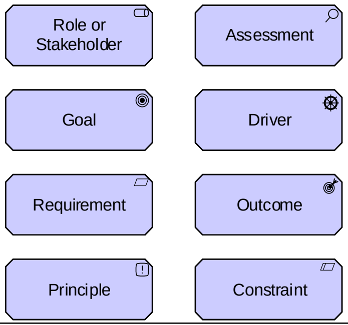
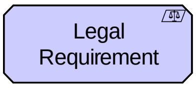
	With the implementation of the NIST CSF, data flows are important to identify and analyze. To that end, a new ArchiMate relationship has been introduced: the *generates* relationship. In the visualization below, a data flow of a server that generates logs, which are pulled by (*flows*-relationship) to a SIEM.
 Internal Device Windows [5-3-3] File External entities External Destination	For these data-flows we have now handled where the data is created and what systems or assets it passes through, but we still miss one important aspect: where the data leaves the organization. Two things are important for this: where the data is sent and how it is being transmitted. Although technically the destination would belong in the elements section, for clarity we both handle them here. The way of modeling that certain elements are outside of the organization can differ in every specific case, this is just an example.

Actors

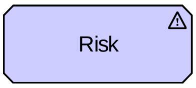
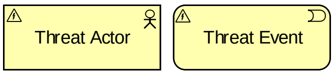
 	NIST CSF's ID.AM-6 specifies to identify cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) (NIST, 2018). These can be modelled as ArchiMate actors and roles. In the example below an employee is assigned a laptop and phone as relationships, while being only associated to the asset management process.

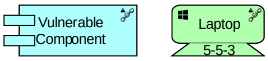
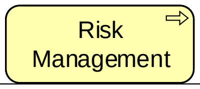
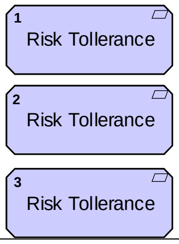
Business Environment (ID.BE) and Governance (ID.GV) The business environment model is used to show the organization's place in the supply chain, and its mission, objectives, stakeholders and activities (NIST, 2018). These elements should already be present in an enterprise architecture, as this is the first step in developing an architecture. Given the prerequisite that to adopt this viewpoint, an enterprise architecture has to already be present, the business environment can easily be adopted from existing models.

Governance can be modelled using the ArchiMate motivation elements:

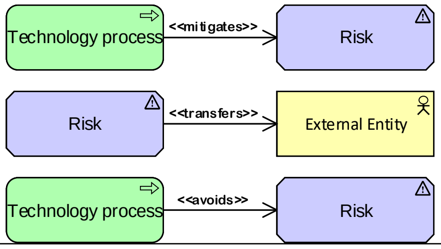
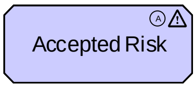
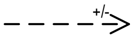
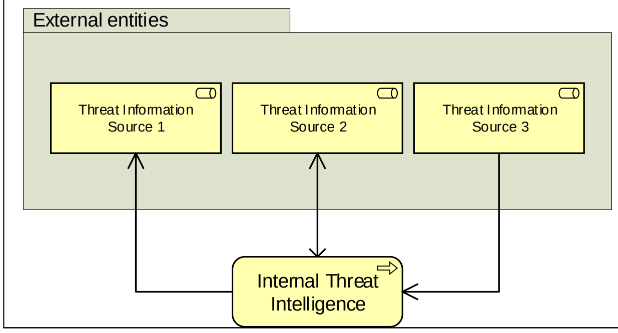
 Role or Stakeholder Assessment Goal Driver Requirement Outcome Principle Constraint	ID.GV-2 and 3 focus on roles & responsibilities, and legal and regulatory requirements. These elements are all readily available in the ArchiMate motivation section.
 	Legal and regulatory requirements can be specified using a requirement element. To differentiate between requirements of the system and requirements by law or regulations, we have adjusted the requirements element for legal and regulations with a balance-logo as can be seen to the left.

Risk Assessment (ID.RA) and Risk Management Strategy (ID.RM) The Risk Assessment category exists to ensure organizations understand the relevant risks, vulnerabilities and threats (NIST, 2018). After the assessment, this viewpoint can be used to visualize the output of that risk assessment. To that end, we have added the following elements:

 	We have added the exclamation point symbol to indicate risks. Risks can occur in any layer of the architecture. We have decided to model these in the motivational layer, as ArchiMate motivations "influence, guide, and constrain the design" (ArchiMate.
 	Threats are modelled with the lightning symbol. A threat is what we are protecting the assets from, which mostly exist outside or within the business layer. We have identified threat actors in the form of malicious entities, and threat events that can cause harm to the organization (such as a surge in DDoS attacks in the sector or region).

	Vulnerabilities are identified within the business itself, showing points where the organization is vulnerable to attacks. We have chosen the ‘weak link’ symbol (a broken chain) to visualize these vulnerabilities in components, which are mostly found in the application- and technology layers. Any component can be identified as vulnerable, here we have chosen a Windows laptop and application component as example.
	ID.RM focuses on the risk management process, which can be visualized as a business process.
 1 Risk Tollerance 2 Risk Tollerance 3 Risk Tollerance	ID.RM-2 and 3 focus on the organization’s risk tolerance. Risk tolerance is a predetermined maximum level of risk, in the scope of an architecture we see this as a requirement. We have adjusted the requirement element to specify an aggressive-, moderate or conservative risk tolerance with respectively a 3, 2, or 1 in the top-left corner. Alternatively this could be specified in the title, with for example `[MODERATE]` in the text of the element.

Relationships

 Technology process <<mitigates>> Risk Risk <<transfers>> External Entity Technology process <<avoids>> Risk	As specified in section 4.3, in risk management risks can be avoided, mitigated, transferred or accepted. We have translated these strategies to relationships between ArchiMate components. In the example to the left a business risk is used, however this relationship can be applied to all types of risks.
	An accepted risk cannot be seen as a relationship, this is visualized as an extension of the component with an ‘A’ with a circle around it.
	Components in the architecture can increase or decrease a risk. These relationships can be identified by an ArchiMate influence-relationship.
 External entities Threat Information Source 1 Threat Information Source 2 Threat Information Source 3 Internal Threat Intelligence	An important aspect of the NIST Cyber Security Framework is the degree to which organizations share information with external entities. This determines to a great deal the organization’s implementation tier. With the *serving* relationship below one can indicate if the organization only shares information to external entities, only receives from external entities or both.

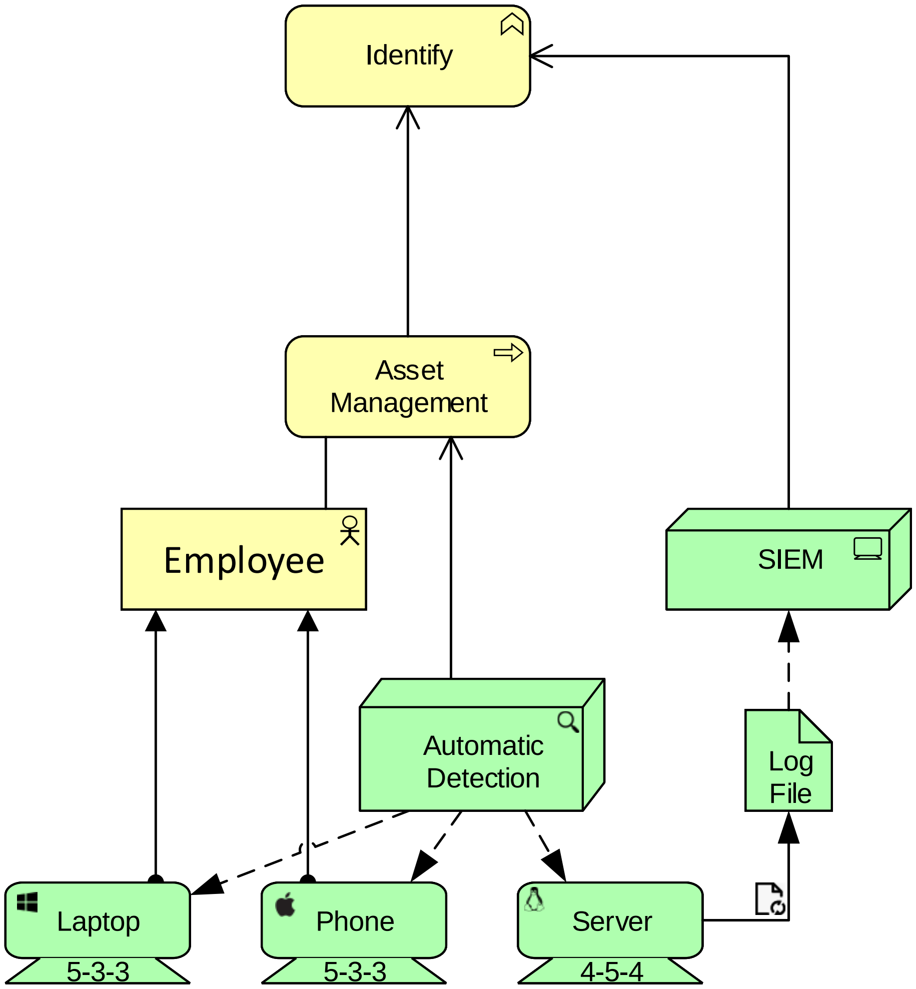


Figure 10: Example view for the Identify viewpoint.

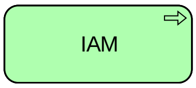
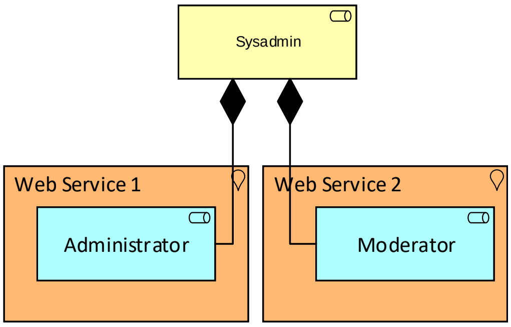
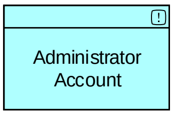
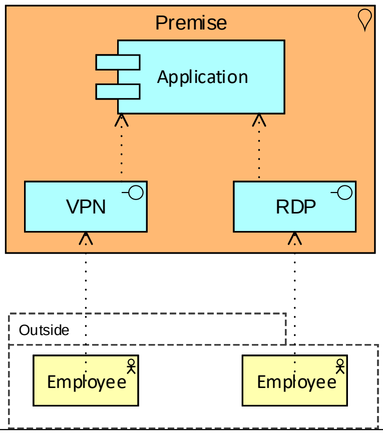
6.3.2 Protect

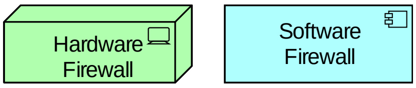
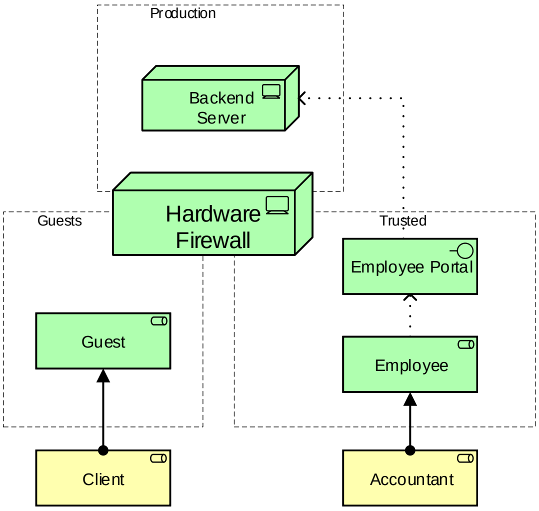
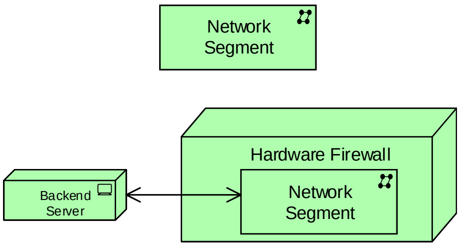
This viewpoint is to show an origination's implementation of appropriate safeguards to ensure delivery of critical services (NIST, 2018).

Stakeholders	Enterprise-, ICT- and security architects, and security officer
Concerns	Information security, ensuring delivery of critical infrastructure
Purpose	Informing, deciding
Scope	Business, technology, motivation, application

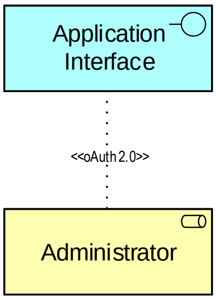
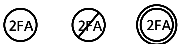
Access Control (PR.AC) and Protective Technology (PR.PT) Shoemaker, Kohnke, and Sigler (2016) state that "The PR.AC-1, PR.AC-2, PR.AC-3 and PR.AC-4 protect function subcategories of the CSF address that need by providing outcomes that require management of credentials for authorized devices and users, managing access to physical assets, and managing server access privileges according to the principles of least privilege and separation of duties, respectively" (p. 225). The need they address is granting and managing user access privileges to servers and other ICT components. Our goal is to accommodate by providing a means to model that outcome. In the protective technology category, PR.PT-3 directs that access to systems is and assets is controlled and PR.PT-4 specifies that the communications and control networks are protected. The other subcategories of PR.PT are considered out of scope, as they both only handle policies rather than elements that can easily be translated to and provide value in enterprise architecture. PR.PT-3 and -4 are handled together with the PR.AC subcategories, because the same modeling components, relationships and actors can be applied to the output.

Elements

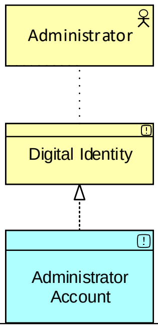
	PR.AC-1 specifies that identities and credentials for authorized devices and users are managed. An Identity and Access Management (IAM) process can be visualized as a technology- or business-layer process.
 Sysadmin Web Service 1 Administrator Web Service 2 Moderator	Interview 6 specified the use of role bases IAM. An IAM role is a specific set of access permissions that can be added to an account (AWS, n.d.). ArchiMate has existing role-elements in the business layer which we can use. However, this type of role would be more suitable in the application layer as AWS (n.d.) suggests "you can use roles to delegate access to users, applications, or services", which reside in the application layer. To that end we have added an application role element, seen to the left. One or more application roles can realize one or more business roles, as the two can but not necessarily have to be the same.
	An important part of IAM is to keep tract of privileged user accounts, accounts that have more than usual rights on the system or on the business. In a combination of PR.AC-1 and -4 the use of these accounts should be managed. These accounts can become a target for malicious entities. We propose to mark these types of accounts of stakeholders with access to these accounts with an exclamation point, as with the ArchiMate principle. To the left an example of an account ArchiMate object extended with the lock, we elaborate on the relationships between accounts and stakeholders in the stakeholders section below.
 Premise Application VPN RDP Outside Employee Employee	PR.AC-3 specifically handles remote access to the system. It is important to keep track of all methods of accessing the network from the outside, and which systems or stakeholders need that method. In the example to the left these services are specified by ArchiMate application interfaces. This example has the premise is a location and the outside as a group, but this can be adjusted to fit the case.
	PR.AC-2 is a requirement of physical security to the assets. This would fit more into the physical architecture of the enterprise, where this viewpoint is aimed towards the technical and part ICT architecture. To that end, in this research physical access is considered out of scope

	The last subcategory of Access Control is aimed at protecting the network integrity. We combine this with subcategory 4 of Protective Technology, which specifies that communications and control networks should be protected. Technologies and software components used to protect the network integrity, such as firewalls, can be visualised with devices or components as shown in the example to the left.
 Production Backend Server Hardware Firewall Guests Trusted Employee Portal Guest Employee Client Accountant	The CSF specifies that network segregation should be implemented, but many more components reside within this control. This is where firewalls and all other network protection elements can be categorized under. These components can be modelled as technology devices or application components, depending on the implementation. Network segregation can be modelled by creating groups with dotted lines. This can be used to see which systems (or groups of systems) reside within which VLAN. The firewall that creates the segregation is the bridge between the VLAN's. This viewpoint can then be used to check if for example users and administrators are not in the same VLAN. Just as the newly introduced application roles, we have also introduced network roles within the technology layer. These roles are based on the VLAN a person connecting to the network would be placed in. This is different from business roles, as for example an accountant and receptionist could well be placed within the same VLAN, and thus have the same network role but different business roles.
 Network Segment Hardware Firewall Backend Server Network Segment	The example above shows how to model different network segments by introducing new elements for clarity. Network segments can also be modeled by using only existing ArchiMate language elements, with the technology network element shown to the left. The downside of this is that a segment where many devices are connected to can become unclear, as this network element will become the center of a large 'web' of relationships.

Relationships

 	The protocols and methods a user uses to authenticate his account can be a large weakness as well, PR.AC-3 of the NIST CSF specifies remote access to be managed. SSH.com (n.d.) adds to this: "Remote access must be properly managed and monitored. Encrypted protocols, such as SSH, Remote Desktop, or HTTPS, are typically used. Access should be monitored and tunneling back into the internal network from the outside should be prevented". To manage all the remote access points and ways of authenticating to the system, organizations could keep track using these elements. Using this viewpoint, the authentication of a user is an extension of the access-relationship of ArchiMate. To model each specific protocol and way of authenticating users would not only introduce many new relationships, it would also be restricting towards newly introduced protocols. Therefore the protocol used to authenticate can be specified as ArchiMate stereotype, between << >> brackets. In views implementing this relationship, it is important to identify and model each service a role has permission to access. PR.AC-4 is based on the least privileged principle, only if all access permissions are modelled this can be checked and shown.
 	In the interviews the need for two-factor authentication was also highlighted. When implemented, this can be visualized as an extension to the authentication relation above by one of the three symbols to the left. The '2FA' in this example is an example, this can be extended easily by other types of authentication by just adjusting the text '2FA'. An example of such an adjustment can be to have 'BIO' as symbol, to indicate which authentications have biometrics as optional, enforced or not allowed/implemented.

Actors

 	Relevant stakeholders in viewpoint can be any users of the system. Each different type of user can and should be modelled to show its access permissions on the system. Inspired by Schoonderbeek (2014), in the example to the left the account is implemented as a realization of the digital identity of the administrator.

Awareness and Training (PR.AT) As the NIST CSF is a high level process framework that affects many different sides of the business, not all aspects translate well into architecture. Awareness and training is such a category, although very important to the resilience to attacks, the creation of awareness among employees is outside of scope for this viewpoint. An architecture for creating awareness could be made as a business process for which many existing viewpoints can be used.

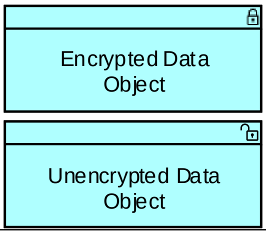
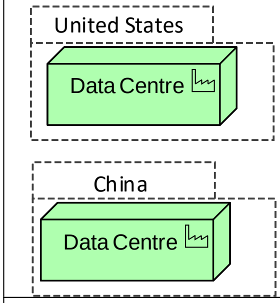
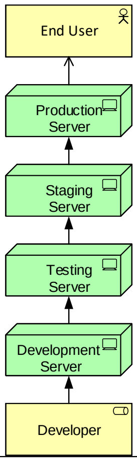
Data Security (PR.DS) Within the data security category, architecture can be useful to some subcategories such as the protection of data-at-rest and in-transit. PR.DS-3 applies to processes within the asset management function, such as the removal, transfer and disposition of assets. The added value of architecture other than already specified in the Identify viewpoint is limited, which is why we will not go into detail on it here.

Another subcategory ensures availability of services by having adequate capacity. This is also hard for this viewpoint to add value to, as it is very specific to the situation. Architecture could definitely be of value to ensure adequate capacity, the output of such a check would however be an entire specific IT architecture, which is out of scope for this viewpoint.

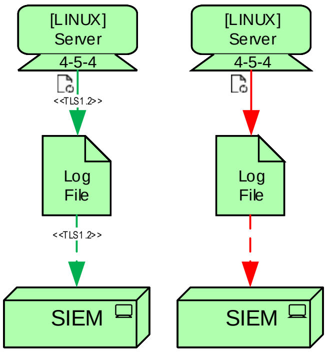
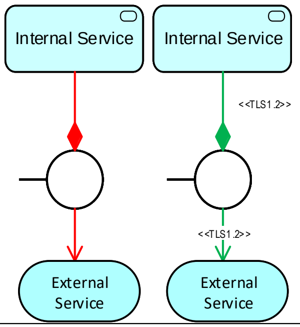
The protection against data leaks is something that can be modeled by means of the elements in the Detect viewpoint of this thesis.

Finally the checking of the integrity of software, firmware and information is omitted in this viewpoint. An implementation of this subcategory would also consist mostly of principles and is not something enterprise architecture can have much added value to.

Elements

	PR.DS-1 specifies data-at-rest to be protected. Out of interviews 1,3 and 4 followed that data encryption is vital to this protection. We have extended the ArchiMate data object with a lock, indicating whether the data it represents is encrypted or not. An unencrypted data object can be marked with an unlocked lock. This can help identify gaps in the implementation of encrypting all data when possible.
	In interview 1 and 6 it was noted that the location of the data can have an effect on its security as well. If the data is for example stored in a U.S. or Chinese data center, national legislation might allow the government to get access to it. These countries can be denoted by an ArchiMate grouping composition.
 End User Production Server Staging Server Testing Server Development Server Developer	PR.DS-7 handles the separation of development, testing and production environments. In software development, a multi-stage environment is often recommended to use to make sure that the environment that end users use is separated as much as possible from the environment that is used to develop the application (Snyder & Southwell, 2006). Such separations can be modeled in many ways using existing ArchiMate elements. In the model to the left a simplified example is shown of a developer triggering changes to the development server, which are mitigated in turn to the testing, staging, and production server. In an actual situation more actors such as testers and reviewers would apply.

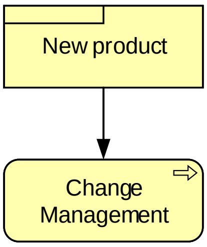
Relationships

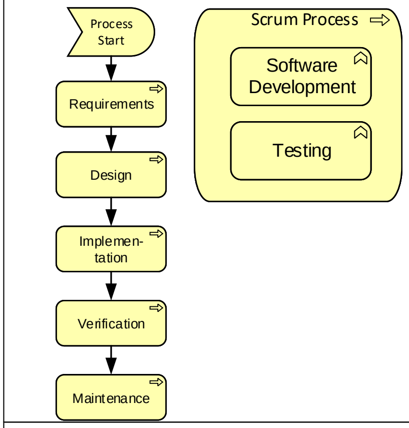
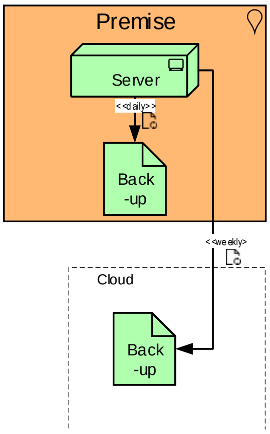
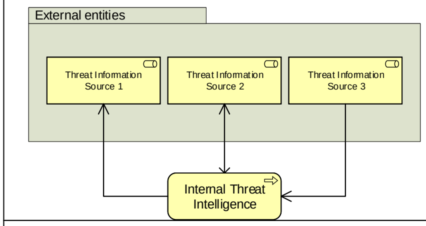
 [LINUX] Server 4-5-4 <<TLS1.2>> Log File <<TLS1.2>> SIEM [LINUX] Server 4-5-4 Log File SIEM	Data in transit can be modeled as an extension of the way a data-flow can be modeled using the Identify viewpoint. Interview 6 noted the importance of not only where and how the data is stored, but how it is transferred and through what systems the data goes. Using the elements introduced in the relationships-section of Access Control (PR.AC) and Protective Technology (PR.PT), the data flows of the Identify viewpoint could be marked with stereotyping the type of encryption (e.g. TLS 1.2) between << >> brackets. However, in interviews 6 a color-coding was also suggested, by marking the encrypted flows green and flows that should be encrypted red. A combination of the two can be used, by for example marking a flow green and specifying that TLS 1.2 is used between << >> brackets.
 Internal Service Internal Service <<TLS1.2>> <<TLS1.2>> External Service External Service	Data cannot only be transferred in the technology layer, but in the application layer as well. In that layer services can communicate, often this is achieved with interfaces that one service provides and another service (or user) consumes. These are part of the data-flows through the organization, and should be encrypted just as well. As with the relationships above, encrypted traffic can be visualized in green with the protocol between << >> brackets, with unencrypted traffic in red.

Information Protection Processes and Procedures (PR.IP) As the name suggests, the Information Protection Processes and Procedures category of the NIST CSF handles processes and procedures. Processes can be modeled with ArchiMate, although other modeling languages might be more suitable such as BPMN.

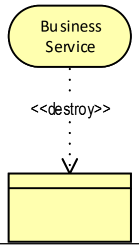
The creation and management of a response plan is management that is hard to visualize within architecture. It could be modeled as a process or function, but this would not provide much value in adopting the NIST framework. To that end we have left this out of scope of this viewpoint. The same applies to the continuous improvement of protection processes, the creation, management and testing of response- and recovery plans, and the inclusion of cyber security in human resources.

Elements

	The first subcategory is to create and maintain a baseline of information technology and industrial control systems. We have checked the guiding ISO27001 standards provided by NIST, these handle mostly change management. Change management is also controlled by PR.IP-3, which is why we group these. When using this viewpoint, the assumption is made that an enterprise architecture is in place within the organization. A part of TOGAF's ADM (H.) is change management, therefore this should already be in place within the organization. In the architecture this function can be visualized as a business process, as seen to the left. All affected parts of the organization can be connected to this process by triggering or association relationships.

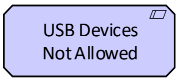
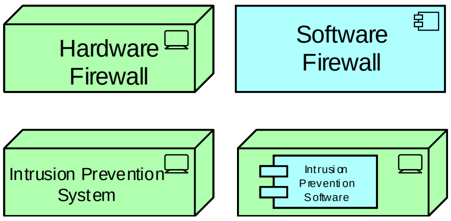
 Process Start Requirements Design Implementation Verification Maintenance Scrum Process Software Development Testing	The next subcategory ensures that a System Development Life Cycle (SDLC) is used to manage systems is implemented. A system development life cycle is a structured approach to creating and maintaining a system used in information technology (Christensson, 2014). Examples of such systems are Waterfall, Scrum and eXtreme Programming. We have identified two ways of how architecture can aide in this NIST control: by modeling such a process and by showing which parts of the architecture use such a model. The first is shown in the figure most left, where the waterfall model is modelled. The second is shown to the right of it, where a process resides within a scrum process.
 Premise Server <<daily>> Back -up <<weekly>> Cloud Back -up	In the interviews the creation, testing and restoring of backups mostly came up within the Recover-phase. However, NIST covers the creation and testing of backups in the Protect function, as this is the protection of the data. In Recover, the creation and testing of backups would be to late – this is where the recovery of backups happens. We have identified two important concerns with backups, the interval or time between backups, and the location of the backups. The interval determines how much of the data will be lost in an event leading to recovery. The location can be on-site or off-site, when for example the location of the on-site backups is hit by a fire, the off-site backups could still be used for recovery. This process can be visualized within the data-flow introduced in the Identify viewpoint, with the interval as stereotype between << >> brackets.
 External entities Threat Information Source 1 Threat Information Source 2 Threat Information Source 3 Internal Threat Intelligence	The sharing of effectiveness of protective technologies can be modeled in the same way as we model the sharing of threat information with outside sources, by grouping external entities and showing which sources are used to share information to and/or from.
	The last subcategory of Information Protection Processes and Procedures is that a vulnerability plan is developed and maintained. In the Identify viewpoint, we have developed a method of classifying vulnerabilities, threats and risks found. The vulnerability management plan handles how those vulnerabilities should be mitigated and dealt with. The elements used to model the vulnerability management plan do not differ from those used to identify vulnerabilities and risks.

Relationships

	The destruction of data is also managed under Protect within the NIST framework. We have modeled that as an access relationship, with `<<destroy>>` as stereotype. The example to the left shows a data object being destroyed, this could also be for example an artifact on the application layer. This part of the viewpoint can be used to show that all data that should be destroyed are considered. Within the stereotyping a time frame could also be shown after which the data will (automatically) be destroyed.

Protective Technology (PR.PT) The last category of Protect handles the management of technical security solutions. The first subcategory is considered out of scope, as it handles policies to which architecture can provide little value. It ensures that audits and log records are determined, documented and implemented according to policy.

PR.PT-3 states that the access to systems and assets is controlled, the modeling of which we have already handled earlier in this viewpoint, in Access Control. The following elements can be used:

	The second subcategory handles the protection and restriction of removable devices according to policy. These policies can be modeled by using motivational elements, such as constraints, principles or requirements.
 Hardware Firewall Software Firewall Intrusion Prevention System Intrusion Prevention Software	The final subcategory of the protect function ensures that communications and control networks are protected. From interview 2, 4 and 5 followed the use of firewalls to ensure this protection, interviews 3 and 4 also noted the importance of Intrusion Prevention Systems (which will also be handled in detail in the Detect viewpoint). These components can be modeled as technology devices or software modules.

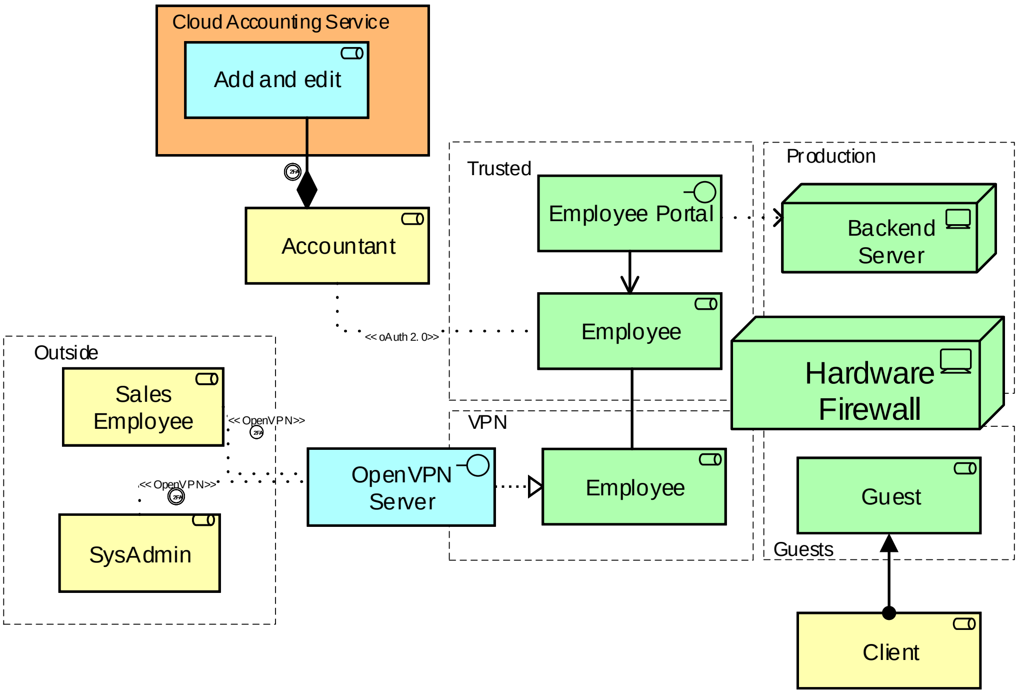


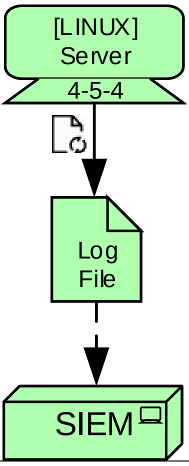
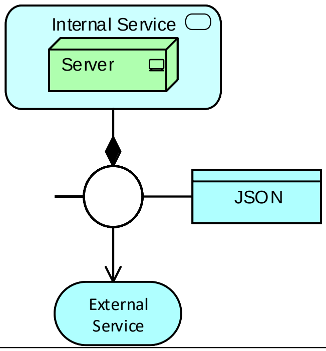
Figure 11: Example view for the Protect viewpoint.

6.3.3 Detect

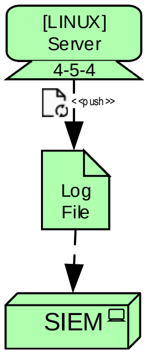
This viewpoint is to show the organization's processes, technologies and people involved in the detection of events in its network and on its assets.

Stakeholders	CISO, SOC-team, security architect
Concerns	Showing current or needed different detection solutions and way of handling events
Purpose	Informing, deciding
Scope	Business, technology, motivation, application

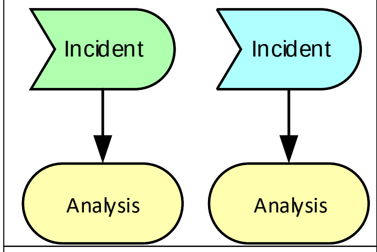
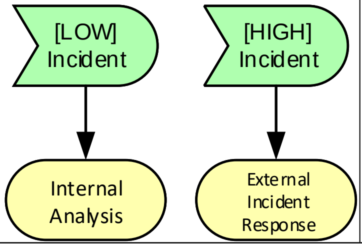
Data-flow In the viewpoints for Identify and Protect, we have categorized elements, relationships and actors on the categories within the framework. Within Detect however we have decided to make a separate example of this for the data-flow (which is also used in previous viewpoints), as from a modeling perspective there is overlap in the categories. The reason for this overlap is that from an enterprise architecture or modeling perspective, the output that the viewpoint can help generate is very similar. The following model belongs in Anomalies and Events (DE.AE) and Security Continuous Monitoring (DE.CM) equally.
Elements

	As seen in both the Identify and the Protect viewpoint, the modeling of a flow of data throughout the network is an important parts of the entire viewpoint, and therefore equally important for the Detect part. In Anomalies and Events, the creation of a baseline of network operations and expected data-flows is the first subcategory. For such a baseline a method of modeling is essential, which can be created by chaining elements that create, handle or pass data as seen to the left (introduced in the Identify viewpoint). Anomalies and Events also calls for the collection and aggregation of data from multiple sources and sensors, which is confirmed by interviews 3, 4 and 6. In these interviews, most of the input was identified as log files from systems and software. The model to the left shows an example of a log file being generated and pushed to a Security and Information Event Management (SIEM) system. This method applies to DE.AE-1 and -3, and DE.CM and -6.
	With architecture moving more and more to micro services and cloud applications, data-flows arise not only within the technical layer but also in the application layer. Communication between application-level services can be modeled using an interface, which is a point of access where the application service is made available to other services or end users (Lankhorst, 2009, p. 97). Therefore these interfaces can als be part of the data-flow introduced in this viewpoint. ArchiMate however does not specify what types of data is, this can be visualized as shown to the left with an association relationship.

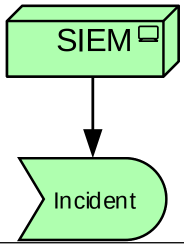
Relationships

 [LINUX] Server 4-5-4 <<push>> Log File SIEM [LINUX] Server 4-5-4 Log File <<pull>> SIEM	When modeling a flow of data, interview 3 noted that it is important to know whether the log files (in this example) are pushed or pulled from the corresponding server. In a push construction, the server sends the files (periodically) to the monitoring service, in a pull construction the monitoring service requests the files from the server. According to interview 3, when pulling the data you can't request too much or too often. That is why there is often a switch towards push, but this can also have its downsides. The arrow in the data flow in the elements-section notes what node *generates* the log file, in that case the server. For the push-or-pull comparison, the question is which node *initiated* the flow of data. The former is more important for clarity, which is why the arrow indicates which system generates the file. Push or pull can be modeled by stereotyping `push` or `pull` between `<<>>` brackets. This type of stereotyping can also be applied to the application-level interfaces shown in the elements section above. Note that this type of stereotyping could be applied to different types of relationships to fit the case, such as the *access* relationship.

Anomalies and Events (DE.AE) As the name suggests, this category deals with the monitoring for anomalies and cyber security events. It makes sure that a baseline of network operations is made and that behavior that alters from that baseline triggers an event, which is handled. This viewpoint can help to show how events are classified and handled. **Elements**

	Without actions following the output of monitoring, the monitoring alone would be useless. This is why DE.AE-2 specifies that detected events should be analyzed to understand attack targets and methods. Events can be modeled as technology- or application events, the service that does the analysis can be a service with further specification in the business layer.
 [LOW] Incident Internal Analysis [HIGH] Incident External Incident Response	With the events modeled above, DE.AE-4 requires the determination of impact of an event. The possible classification (specific to each implementation of this viewpoint) can be shown with the classification between `[]` brackets in the text of the incident. An event element used this way does not represent a single event but an event type, multiple sources can therefore generate the same event, which can then be handled the same way for multiple sources.

Relationships

	The events introduced in the elements section have to be triggered by some element. The ArchiMate triggers relationship can be used to show from which origin certain events might occur. This same relationship is used to show incidents handled by certain (business) services, as the event triggers that service.

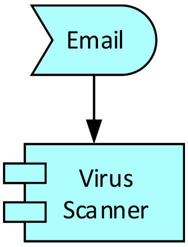
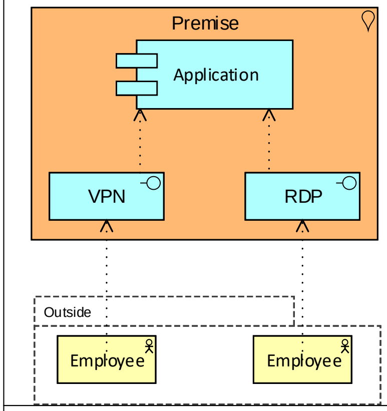
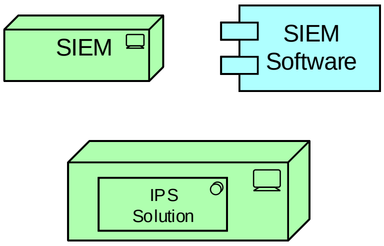
Security Continuous Monitoring (DE.CM) The actual monitoring for these events would fall under the next category, the continuous monitoring of assets and information systems.

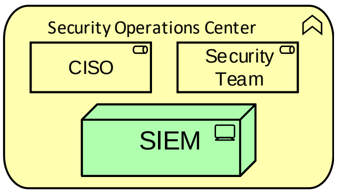
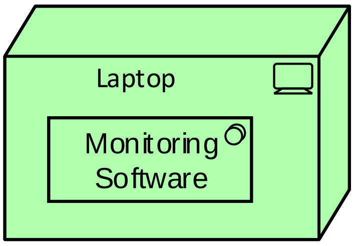
Just as the physical protection in the Protect viewpoint, the subcategory DE.CM-2 handled the monitoring of the physical environment to detect cyber security events. As stated in the Protect viewpoint, the physical protection is certainly not unimportant, but we have considered it out of scope within this viewpoint as it lies more within the physical architecture to show how the physical environment is protected and monitored.

To find out the intend of subcategory DE.CM-6, we have checked the additional controls, and found guidance in the related ISO 27002:2013 controls. These controls specify that all outsourced development should be checked, reviewed and tested before implementing and releasing the software. Due to the fact that these are principles, it is difficult for enterprise architecture to be of assistance to this subcategory.

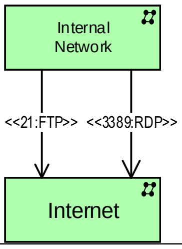
The last subcategory of Security Continuous Monitoring ensures that vulnerability tests are performed. From an enterprise architecture perspective, just ensuring that these tests are performed can be a principle to which an ArchiMate model cannot provide much additional value. The output of these tests can be modeled by means of the Identify viewpoint, which is why we do not handle this subcategory again in this viewpoint.

Elements

	Interview 3 and 6 noted the importance of scanning all data that enters the organization. We have provided a way of modeling two ways data can enter an organization: by means of opened ports or connections, and by means of emails that have been sent to employees. More can of course be identified, we have chosen these two as an example as they have been mentioned in the interviews. An email that enters the organization can be visualized as an event in the application layer. In the first example to the left, this event triggers the scanning of a virus scanner as software component.
 Premise Application VPN RDP Outside Employee Employee	Connections to the outside in the form of opened ports, or services exposed to the internet are crucial model and keep track of as vulnerabilities. Therefore, this method has already been introduced in the Identify and Protect viewpoint. Here the services connected to the outside are visualized as application interfaces, with connections to the outside as a group. In ArchiMate networks can be modeled as relationships or as network technology elements. We will introduce a way of modeling using the technology elements further in the relationships section.
	DE.CM-1 defines that the network is monitored to detect potential cyber security events, to which DE.CM-4, -5, -6 and -7 are specifications for certain parties or (groups of) devices. The interviews specified Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS, basically an IDS with blocking capabilities) and Security Information and Event Monitoring (SIEM) solutions as possible technologies that can apply here. These can be modeled as technology devices, or software on devices as shown to the left. Besides these elements, the dataflow section should be used to show the monitoring capabilities of the network.

 	Interviews 4 and 6 handled the concept of a Security Operation Centre (SOC), which is elaborated upon in section 4.2.4. According to interview 4, a SOC can the detection of events and in some occasions also the response to and protection from those events. A whole viewpoint could be written just on this subject, which is why we will handle it shortly. A SOC is a business function, which can include multiple roles, responsibilities devices and technologies. The internal structure of such as SOC is considered out of scope due to the many possibilities and its size. To the left a small example is shown with example roles and a device within a business function.
 	Interview 3 and DE.CM-3 state that the activity of users should also be monitored, and interview 3 adds to this that (due to the increasing use of HTTPS) monitoring on the users' devices is needed. To show what software is used to monitor this activity on for example the laptops of employees, ArchiMate software components can be used within technology devices. An example of monitoring software on a user's device is shown to the left. This way of modeling can also be used to show software used to detect malicious code on devices for DE.CM-4 and -5.

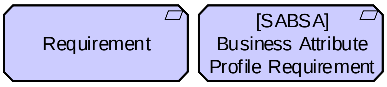
Relationships

 	The example to the left is the alternative version of connections to the outside shown in the elements section of this viewpoint using networks as a technology element. In the example the internal network 'serves' the outside internet (as a server), in this case both are technology networks. the type of connection or port can be stereotyping port:service between `<<>>` brackets. Networks can also be visualized as relationships, this is shown in the Identify viewpoint

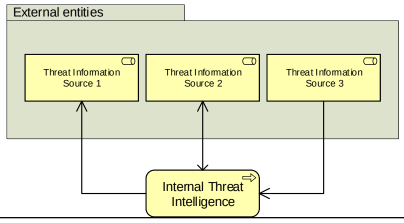
Detection Processes (DE.DP) This category handles the processes and procedures that support the continuously monitoring of the network and organization.

Two subcategories are considered out of scope: DE.DP-3 and -5. DE.DP-3 states that the detection process are tested, and although this is of course vital to the implementation, enterprise architecture and modeling specifically cannot provide much value to it. The same goes for the last subcategory DE.DP-5, which handles the continuous improvement of the processes.

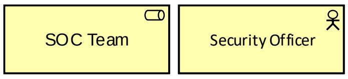
Elements

 Requirement [SABSA] Business Attribute Profile Requirement	The next subcategory handles the compliance with applicable requirements. Relevant requirements in a view are modeled using the motivational requirement element shown to the left. Additionally, interviews 2 and 6 noted the use of SABSA Business Attribute Profiling in the requirements management phase (see section 4.2.5). It can be useful to note which SABSA Business Attribute Profiles are relevant to certain requirements or elements, this can be done by noting `[SABSA]` before the element title.

Relationships

 External entities Threat Information Source 1 Threat Information Source 2 Threat Information Source 3 Internal Threat Intelligence	Lastly, the NIST framework specifies to communicate and share event detection information to the relevant parties. Using the same methods as in the earlier mentioned viewpoints, it can be noted what information is shared with (and from) what entities and stakeholders.

Actors

	Just as with the other viewpoints, NIST specifies that roles and responsibilities are arranged for the detect process in DE.DP-1. Business roles and actors can be used to indicate relevant roles, responsibilities and stakeholder to the detect process.

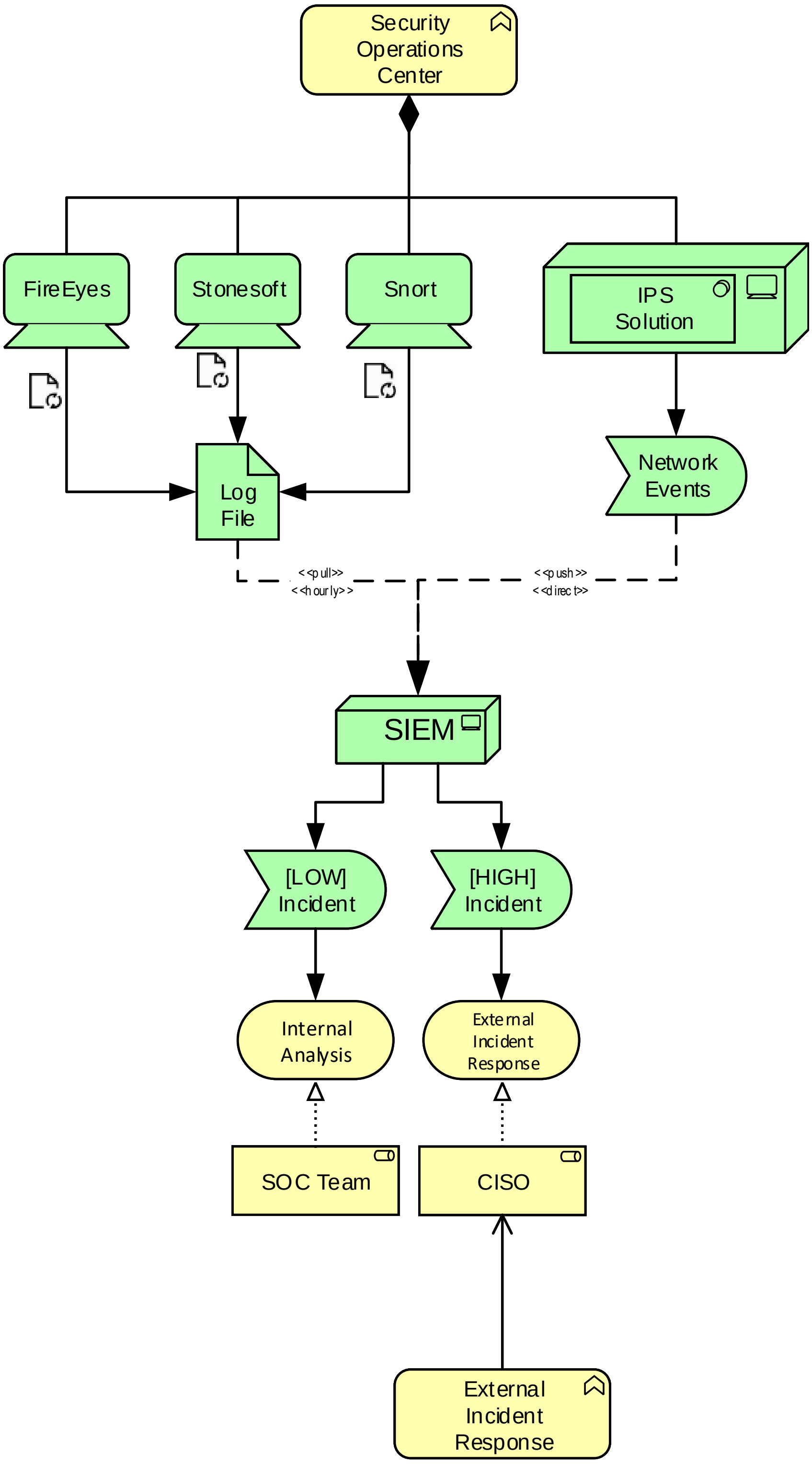


Figure 12: Example view for the Detect viewpoint.

6.3.4 Respond

This viewpoint is to show the organization's processes, technologies and people involved in response to the events and output of the Detect and Protect functions. Additionally it can be used to model a desired architecture how the organization intends to deal with the response to information security events.

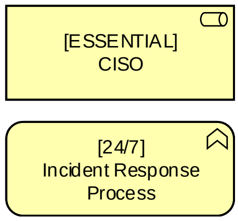
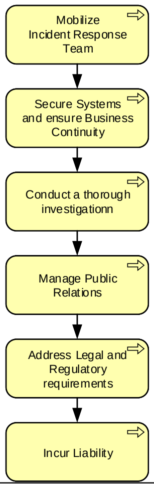
Interviews 4, 5 and 6 name the importance of an incident management plan or an incident response process, this viewpoint helps in modeling that process.

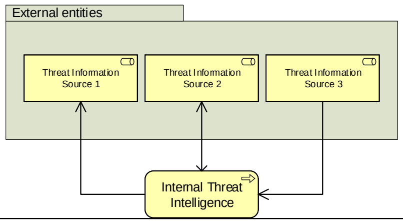
Stakeholders	CISO, SOC-team, security- and enterprise architect
Concerns	Showing the current or desired processes, technologies and stakeholders related to the response to information security incidents
Purpose	Informing, deciding
Scope	Business, technology, motivation, application

Response Planning (RS.RP) The response panning category ensures that the recovery plan (created in Protect) is executed during the event. This supports conclusions from interview 4 that response is the reaction on events from detect and protect. Enterprise architecture can provide little value to whether or not the plan is executed, therefore we consider this category out of scope. Interview 3 and 5 also note that some parts of the response should be automated. However, it is noted in interview 5 and 6 that there should always be a senior (human) decision before high impact decisions (such as taking down a system) are taken. These principles should be present in the response plan.

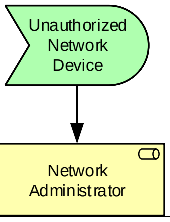
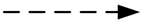
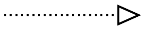
Communications (RS.CO) The communications category of the NIST CSF handles, as the name suggests, how communication should be managed within information security. The elements and relationships described here can be used for this model.

Elements

 [ESSENTIAL] CISO [24/7] Incident Response Process	The first subcategory of the respond function is to ensure that the personnel of the organization knows their roles and order of operations in case a response is needed. Interview 4 and 6 mark that in case of an event, certain people are essential for example in the sense that they may be needed to wake up in the middle of the night to get them involved. Interview 5 noted that in these cases senior decision-making is vital. To mark certain business roles or stakeholders as essential in case a response is needed, the text can be prepended by `[ESSENTIAL]`. Interview 6 also noted the importance of a 24/7 response team. If certain elements in the architecture should be available 24/7, it can also help in the implementation to mark these. This can be done similarly, by marking them `[24/7]`. These elements also cover the fourth subcategory of Communications, that coordination between stakeholders occurs according to the communications plan, by modeling which stakeholders are essential and how the communication flows to support the communications plan.
 Mobilize Incident Response Team Secure Systems and ensure Business Continuity Conduct a thorough investigationn Manage Public Relations Address Legal and Regulatory requirements Incur Liability	The order of operations in case of an event is something where ArchiMate can be of use. We have used the steps provided by Rossi (2015) in to example to the left to show how these kinds of steps can be modeled. The steps can be modeled as business processes, the relationships between as 'triggering'.

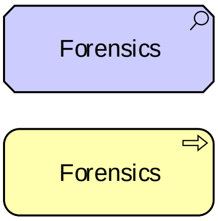
 External entities Threat Information Source 1 Threat Information Source 2 Threat Information Source 3 Internal Threat Intelligence	Lastly, the NIST framework specifies to communicate and share event detection information to the relevant parties. Using the same methods as in the earlier mentioned viewpoints, it can be noted what information is shared with (and from) what entities and stakeholders.

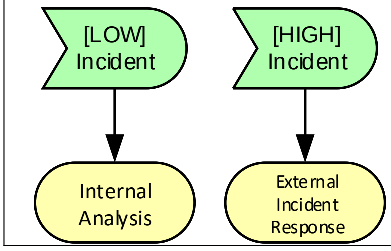
Relationships

	In the Detect viewpoint a method of modeling events that arise, and the classification and analysis of those events. In the scope of respond, the reporting of those events to the relevant stakeholder is covered. This can be modeled as a relationship between a (technology) event and a (business) role. In ArchiMate this can be visualized as a 'triggering' relationship, as shown to the left.
	Part of the response plan is how information should be shared internally. Although the response plan is not created but executed in the Respond function, it can still be useful to model some information flows. For the sharing of information between roles or stakeholders an ArchiMate 'flow' relationship can be utilized.
	The steps in the order of operations in the second row of the elements section above can be specified further using architecture elements. In these cases, a 'realization' relation is applicable to show what functions or processes realize which steps.

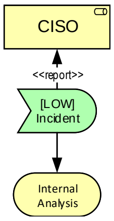
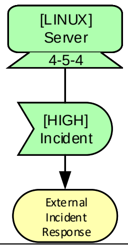
Analysis (RS.AN) The NIST CSF provides this category in the protect function to ensure that events are not only detected (in the detect function) and blocked, but that the cause is found as well. In the analysis category among others the impact of an event is determined and forensics are performed. This section shows what elements and relationships are relevant to this category.

Elements

	The performing of forensics to find the root cause of the event can be visualized in two ways: one in the motivational layer and one in the business layer. In the motivational layer, forensics can be seen as an assessment, as seen to the left at the top. This can be used to show certain actions to be taken based on the outcome of the forensics of the event. In the business layer, an organization might have a forensics services department that performs these kinds of assessments or an external forensics services provider can be engaged. In these cases the performing of forensics is not a simple assessment, but can represent a whole business process. An ArchiMate business process can better be used in those cases, as shown in the bottom example to the left.

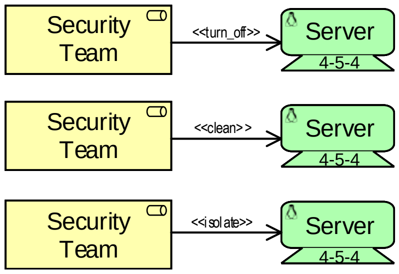
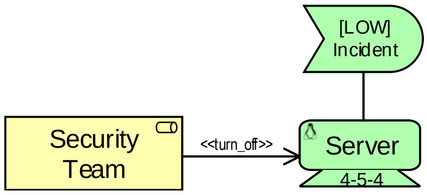
 [LOW] Incident [HIGH] Incident Internal Analysis External Incident Response	The second and fourth subcategory are about understanding the impact of and categorizing the incident consistent with the response plan. Such a classification can be visualized using the elements introduced in the Detect viewpoint, by marking ArchiMate event technology elements with a category between `[]` brackets.

Relationships

	The first subcategory of Analysis states that notifications from detection systems are investigated. This is in line with interviews 4 and 6, which state that this phase is a response to Detect and Protect and the vulnerability scans from those phases are measured and analyzed. In the previous viewpoints, we have modeled incidents and notifications as ArchiMate (technology) events, and the handling of those events with triggering relationships. If a stakeholder or role should not follow up on the event, but should be informed by it, the relationship can be stereotyped with report between `<<>>` brackets.
 [LINUX] Server 4-5-4 [HIGH] Incident External Incident Response	Besides the classification described above, another classification that can be taken into account is that of the Identify viewpoint, related to the CIA classification of a service. Interview 3 noted that if for example a server has an availability classification of 5, it should not simple be taken offline. This does not apply to the event itself, because an event does not have an 'availability'. But the related device can be classified this way and related to the event with an association relationship.

Mitigation (RS.MI) In the mitigation category, actions are taken to make sure that the event does not expand and that its effects are contained as far as possible. Two subcategories are relevant to this viewpoint: the containment and the mitigation of incidents. We handle these two together, as the actions to mitigate or contain incidents identified in the interviews mostly overlap. The third refers to the documentation as accepted risks of newly identified vulnerabilities. This is certainly important in this phase, but the methods of identifying and classifying vulnerabilities are already described in the Identify viewpoint. Therefore we consider this category out of scope.

Relationships

 Security Team <<turn_off>> Server 4-5-4 Security Team <<clean>> Server 4-5-4 Security Team <<isolate>> Server 4-5-4	Comparable with the mitigation and transfer of risks in the Identify viewpoint, we view the actions taken to contain or mitigate an incident as a relationship between the event and the element requiring the mitigation or containment. In interviews 3 and 4, some actions that can be taken to isolate or mitigate an incident were identified: to isolate a system in the network, to block traffic, to clean or reinstall a system, and to turn off a system. These are of course only examples of actions that can be taken, many more might be identified in the response plan. The example to the left shows how such actions can be visualized with a 'serving' ArchiMate relationship with the action stereotyped between <<>> brackets.
 [LOW] Incident Security Team <<turn_off>> Server 4-5-4	Besides the action to be taken, it is also important to note what incident affects what element, to show how that action relates to the incident. As the name suggests, this can be indicated with the ArchiMate 'association' relation. In the example to the left we see that in the case of a low-classified incident on that server, the security team should turn off that system.

Improvements (RS.IM) The last category of the respond functions is to take lessons learned during the response into account and form continuous improvements of the process. Although these improvements are vital to a good protection, enterprise architecture cannot provide much value to this part as it affects the process itself. To this end we have decided to leave this part out of scope in this viewpoint.

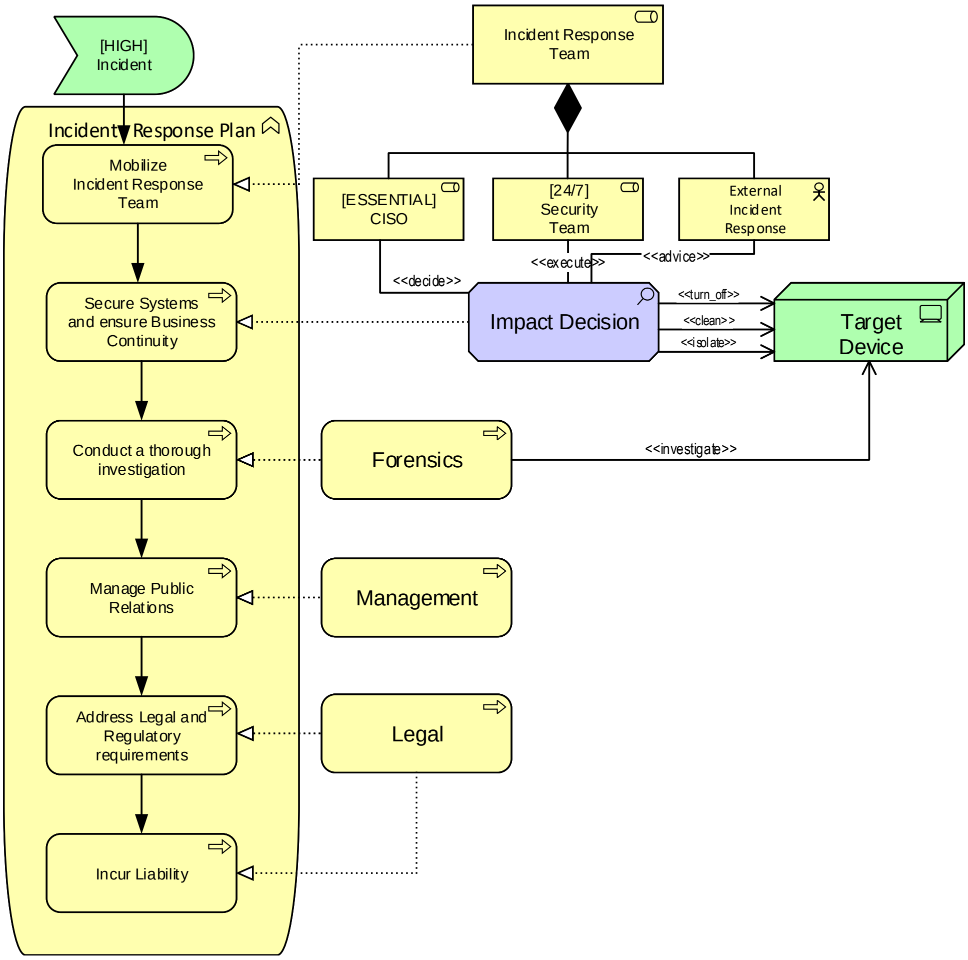


Figure 13: Example view for the Respond viewpoint.

6.4 Combined Process

At the moment of writing, no existing (scientific) research has been found on integrating the NIST Cyber Security Framework within TOGAF. In this section we will try to map the different functions of the NIST framework core onto TOGAF.

In the case of integrating TOGAF and SABSA, both frameworks are extensive and cover an organization in its whole. The NIST Cyber Security Framework is much smaller and more practical, as it is a combined set of standards, guidelines and best-practices for managing cyber security risk rather than an architecture framework covering an entire organization. To that end, we will start with TOGAF as a basis onto which we will map the NIST functions.

6.4.1 ADM and NIST implementation steps combined

Most architecture frameworks contain, besides the framework itself, a process how to design an architecture within the framework. TOGAF's ADM and the SABSA lifecycle are examples of this. This is also a good point of collision between frameworks. When you try for example to implement an architecture according to two frameworks, you need one single process. This is why The Open Group TOGAF-SABSA Integration Working Group (2011) mainly focuses on the architecture creation process to get the best out of both frameworks. The ADM is a proven method for architecture development, and NIST has introduced seven steps to create or improve a cyber security program, described in section 4.2.6. We introduce a mapping between these two into a single process in this section, the results can be seen in figure 14. The resulting process can be used to implement the NIST Cyber Security Framework within a TOGAF architecture development cycle. As enterprise architecture in general has a much larger scope

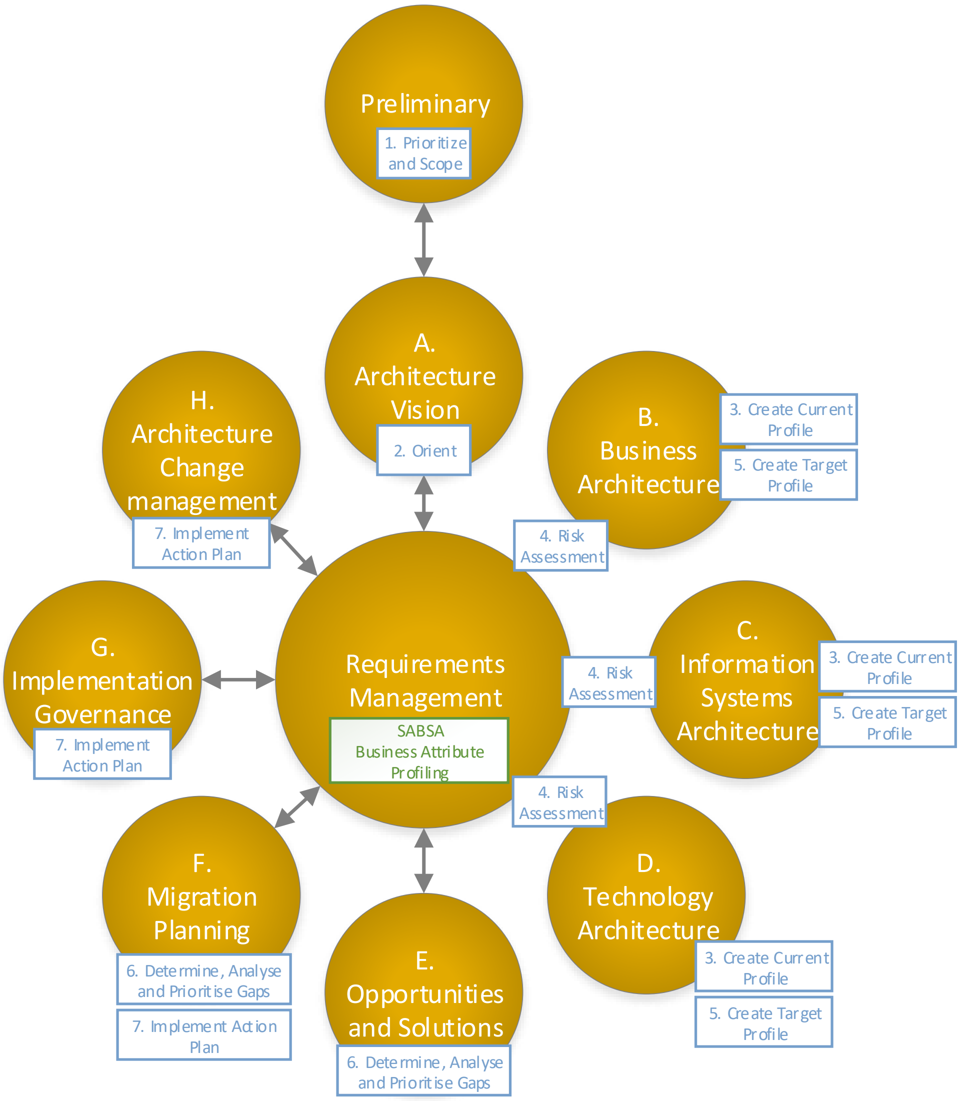

Preliminary
1. Prioritize and Scope
A. Architecture Vision
2. Orient
B. Business Architecture
3. Create Current Profile
5. Create Target Profile
4. Risk Assessment
H. Architecture Change management
7. Implement Action Plan
G. Implementation Governance
7. Implement Action Plan
Requirements Management
SABSA Business Attribute Profiling
4. Risk Assessment
C. Information Systems Architecture
3. Create Current Profile
5. Create Target Profile
4. Risk Assessment
F. Migration Planning
6. Determine, Analyse and Prioritise Gaps
7. Implement Action Plan
E. Opportunities and Solutions
6. Determine, Analyse and Prioritise Gaps
D. Technology Architecture
3. Create Current Profile
5. Create Target Profile

Figure 14: Combined process for implementing the NIST Cyber Security Framework within an architecture development cycle, aided by the SABSA business attribute profiling.

than the NIST CSF, we will map each step of the NIST framework onto phases of the ADM, and not vice versa.

The first step of the NIST CSF is to prioritize and scope. In it scope, business goals, and high-level priorities are set. These activities would take place in the ADM's preliminary phase, where the scope of the architecture and its elements is determined. The setting of the target NIST implementation tier also reflects the aspirational vision, and therefore nicely fits into the architecture vision phase.

The orient step of NIST CSF is where systems and assets, regulatory requirements and an over-all risk approach is identified. The setting of the risk approach is a highly strategic decision, which should be handled by top management of the organization. In TOGAF, the strategic drivers for the architecture are set in phase A.

Steps three and five of NIST CSF create relatively a current- and target profile. In phases B, C and D of the ADM, an architecture for relatively business, information systems (data and application) and technology are developed. All three steps follow the same basic steps, one of which is to create a baseline architecture description, and one is to create a target architecture description. These baseline- and target architecture descriptions can be compared with the current- and target profiles of the NIST steps. As stated earlier in this section, a profile in the NIST framework is made up of multiple categories and subcategories, each of which spans one or more architectural dimensions. For that reason, the creation of a current- or target profile is partly done in ADM phase B, C and D. Step four, conducting a risk assessment, is not specifically present in the ADM. Focusing on the (security) risks is essential to implementing an architecture for information security, therefore this step can also best be integrated in phases B, C and D. Step four would ideally be between the phases themselves and the requirements management phase in the centre, as the level of cyber security risk is essentially the basis for requirements of a security architecture.

The next step of the NIST CSF is to determine, analyze and prioritize gaps. This step fits perfectly with Phase E of the ADM, in which the gaps between the baseline- and target architecture descriptions are analyzed. Besides analyzing and prioritizing the previously identified gaps, in this step an organization should also create the action plan. In Phase E of the ADM, architects start the creation of an Implementation and Migration plan, which is completed in Phase F. Therefore, we have decided to let step 6 span both Phase E and F of the ADM in figure 14.

The last step introduced by NIST (2018) is to implement the action plan created in step 6. Implementation is handled more extensively by TOGAF, this is why this step spans phases F, G and H of the ADM. This shows that implementing the NIST Cyber Security Framework could benefit greatly from adapting this combined method, as it takes governance and change management much more into account.

Interviews 2 and 6 noted the importance of using SABSA's methodology in security architecture development, with its Business Attribute Profiles in particular. As explained in section 4.2.5, this method provides guidance with requirements management specially tailored towards requirements for the protection of information security of the organization. To that end we have also incorporated the SABSA business attribute profiling in the requirements management step central to the ADM, to get the best out of the processes of TOGAF, SABSA and NIST.

7 Application

In the final phase of this research, we apply the viewpoint to existing architecture. At the end of sections 6.3.1, 6.3.2, 6.3.3 and 6.3.4, we have shown an example view for each function of the viewpoint. These examples were however not based on existing architecture but specifically made to show the models in use. In this section we apply the viewpoint to three existing ArchiMate views of the ArchiSurance case study by Jonkers et al. (2016). For each view we will first show the original view, followed by the adjusted view with reasoning and changes in the text. Due to the size of our viewpoint, we will not be able to show all elements used. Instead, we will use as many we can, while still keeping the view consistent, clear and realistic. We have chosen functions of the NIST framework viewpoint that best fit with the ArchiSurance view, resulting in a Protect, Detect and Identify view.

7.1 Protect and the ArchiSurance Infrastructure View

For the first example we compared all of the architecture views in the ArchiSurance case study to find the one with the most overlap with the protect viewpoint introduced in section 6.3. We have found that for this example, the target Technology Architecture: Infrastructure View (Jonkers et al., 2016, p. 34) suited best. We have used the target view instead of the baseline to show that the extensions we have made to the architecture are also in a 'target' state and not in the current ArchiSurance case, but the differences are small. The original architecture view is shown in figure 15.

As noted in the beginning of this section, we have tried to apply as many aspect of our viewpoint as possible while still keeping the same case study without making it unclear. From the protect viewpoint, we have added network segments, encryption of traffic, backup process, patch management, a network role, a VPN server as connection to the outside, and in part a data flow. The resulting view can be seen in figure 16.

In the viewpoint, there are two ways to model network segments. One is with the existing ArchiMate elements, as a Communication Network within the technology layer. The other is with dotted lines around device elements. We have decided to use the first in this case, as the connections to a central network were already present (the Home & Away LAN). We have extended this LAN, and added a segment for the Front Office, Back Office and one for employees. When employees login to the network,

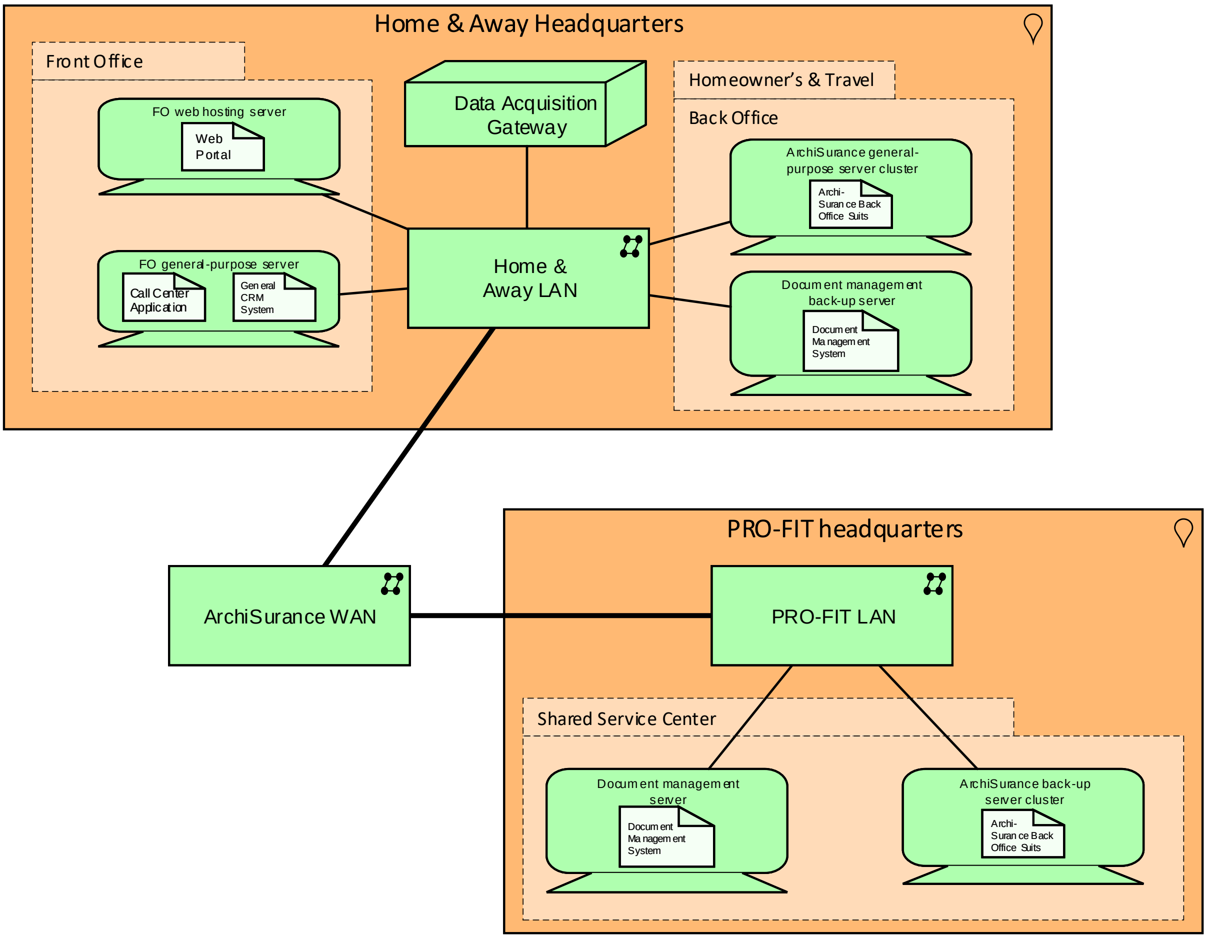

Home & Away Headquarters
Front Office
FO web hosting server
Web Portal
FO general-purpose server
Call Center Application
General CRM System
Data Acquisition Gateway
Home & Away LAN
Homeowner's & Travel
Back Office
ArchiSurance general-purpose server cluster
Archi-Surance Back Office Suits
Document management back-up server
Document Management System
PRO-FIT headquarters
ArchiSurance WAN
PRO-FIT LAN
Shared Service Center
Document management server
Document Management System
ArchiSurance back-up server cluster
Archi-Surance Back Office Suits

Figure 15: Original target ArchiSurance Technology Architecture: Infrastructure View (Jonkers, Band, Quartel, & Lankhorst, 2016, p. 34).

they are placed in the employees-segment based on their role in the network. This role is associated to the employee-segment in the view.

There were some parts of the original ArchiSurance view that fit particularly well with our viewpoint. An example of this is that in the original view, two servers are backed up off-site: the Homeowner's & Travel general purpose server cluster is backed up in the PRO-FIT shared service center, and the PRO-FIT document management server is backed up in the Homeowner's & Travel Back Office. Our viewpoint adds some additional logic to backups to support KPI's used by disaster recovery protocols in the NIST framework. In this view we have visualized this by adding an arrow from the original location as specified in the Protect viewpoint. The backup frequency is specified between <<>> brackets.

Another example of a good fit between the view and our viewpoint is for the marking of encrypted and unencrypted traffic, because some traffic flows are present in the original view. In figure 15, association relationships can be seen between for example the FO web hosting server and the Home & and Away LAN, and between the PRO-FIT LAN and the Document management server. These kinds of traffic can be encrypted or not, the viewpoint introduced in this thesis specifies that the lines can be made green or red, and the protocol used for the encryption can be stereotyped upon the lines. In the example in figure 16 we have shown some traffic flows to be encrypted (e.g., between the ArchiSurance WAN and the PRO-FIT LAN), and some are marked unencrypted (e.g., between the PRO-FIT LAN and the ArchiSurance back-up server cluster). As an additional example we have shown the connection between the Data Acquisition Gateway and the Home & Away LAN to be encrypted, but using an outdated protocol. This connection is marked red as well. This is also the part of the data-flow that we have implemented into this view. Another part of this data-flow is to indicate in which relationship the data was *created*, rather than passed on. In this example this is only the case with the backups, where 'creates' icon is places besides the word 'Backup' on the relationships. In this view however, the amount of data that is passed through is limited.

Another new element we have introduced in this view is the technical Patch Management process in both headquarters. This process is used to indicate how long it takes the organisation to install the latest patches for the software on the devices.

Lastly, we have specified the type of connection between the two locations of ArchiSurance. A VPN Server is added as a software interface, as specified in our viewpoint. This server encrypts the traffic with `TLS 1.2`, which is why the line is marked green. The icon used in the viewpoint to specify that 2-factor authentication is enforced is also added below the protocol. Using these elements we can see that employees in the PRO-FIT Headquarters connect to the Home & Away LAN with a VPN, for which they have to use 2-factor authentication logging in.

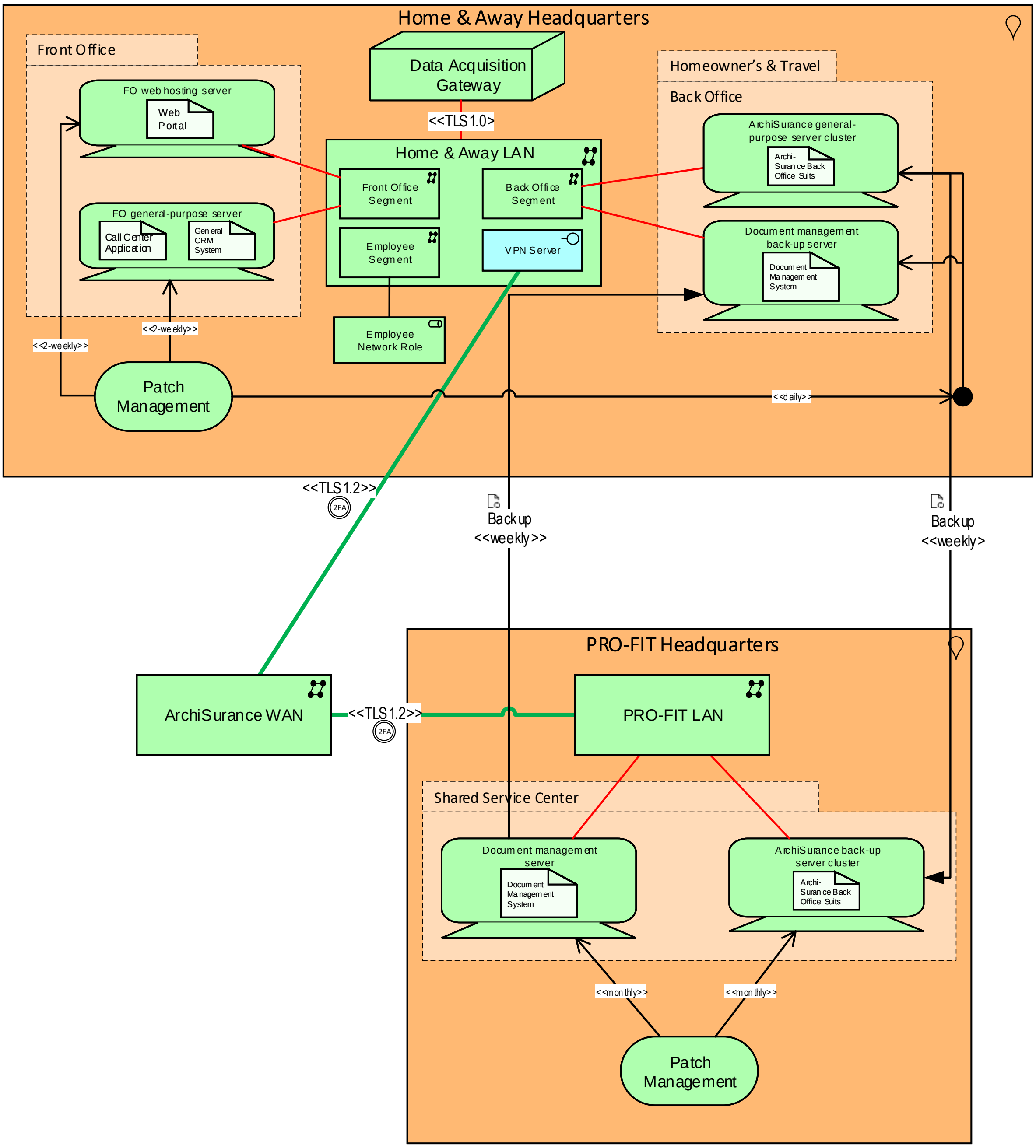
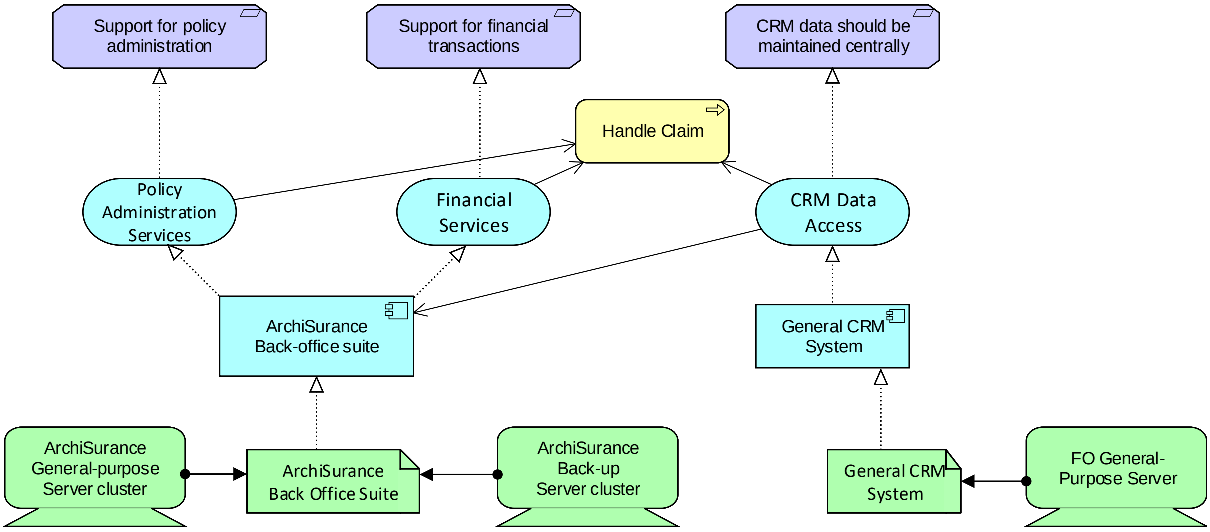


Figure 16: Protect viewpoint applied to the ArchiSurance technical infrastructure view.

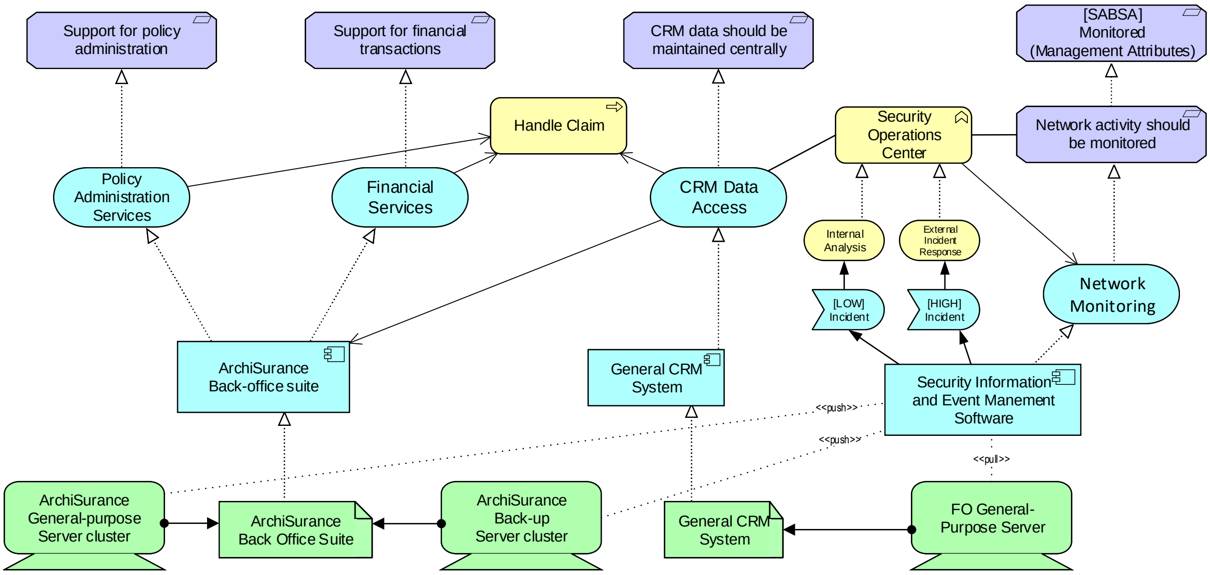
7.2 Detect and the ArchiSurance Requirements Realization View



Support for policy administration
Support for financial transactions
CRM data should be maintained centrally
Handle Claim
Policy Administration Services
Financial Services
CRM Data Access
ArchiSurance Back-office suite
General CRM System
ArchiSurance General-purpose Server cluster
ArchiSurance Back Office Suite
ArchiSurance Back-up Server cluster
General CRM System
FO General-Purpose Server

Figure 17: Original ArchiSurance Requirements Realization View.

For the second example of our viewpoint applied to existing architecture, we have decided to use the ArchiSurance Requirements Realization View. This type of view is intended to show how certain processes fulfill requirements set in the Architecture Vision view. The original view can be found in figure 17.



Support for policy administration
Support for financial transactions
CRM data should be maintained centrally
[SABSA] Monitored (Management Attributes)
Handle Claim
Security Operations Center
Network activity should be monitored
Policy Administration Services
Financial Services
CRM Data Access
Internal Analysis
External Incident Response
[LOW] Incident
[HIGH] Incident
Network Monitoring
ArchiSurance Back-office suite
General CRM System
Security Information and Event Manement Software
<<push>>
<<push>>
<<pull>>
ArchiSurance General-purpose Server cluster
ArchiSurance Back Office Suite
ArchiSurance Back-up Server cluster
General CRM System
FO General-Purpose Server

Figure 18: Detect viewpoint applied to the ArchiSurance Requirements Realization view.

The Detect viewpoint specifies two types of requirements: the standard ArchiMate requirements, and SABSA Business Attribute Profile-based requirements. We have introduced a requirement that network activity should be monitored, which in this example is based on the SABSA Business Attribute 'Monitored' from the Management Attributes set. This requirement is realized by an newly introduced application level process, the Network Monitoring process.

This Network Monitoring process is itself realized by a software based Security Information and Event Management system, or SIEM. As explained in the viewpoint, such a system can be a physical technology device, or a software component running on a device. In this view we have chosen to model the SIEM as a software component rather than a technology device, as the physical devices belong more in the technical infrastructure view. That is also the reason that this software component has access to the devices in the network, rather than a flows-type of relationship. This relationship does specify if the data is pulled from- or pushed to the SIEM.

Another new component is introduced in this view: the Security Operating Center (SOC). The monitoring software in the Security Information and Event Management component generates two types of events: an incident classified as high or low. Incidents of a low classification trigger an internal analysis, realized by the Security Operating Center. In this example incidents with a high classification are also realized by the Security Operating Center, but in a different view these can be handled differently.

The Security Operating Center also serves the Network Monitoring service, as the monitoring will most likely be performed by- or supported by the SOC. This is also the reason that the SOC function has an association relationship with the requirement that the network should be monitored. Lastly it also has an association relationship with the CRM Data Access, as there might also be processes worth monitoring or protecting using SOC capabilities.

7.3 Identify and an alternative ArchiSurance Technical Infrastructure View

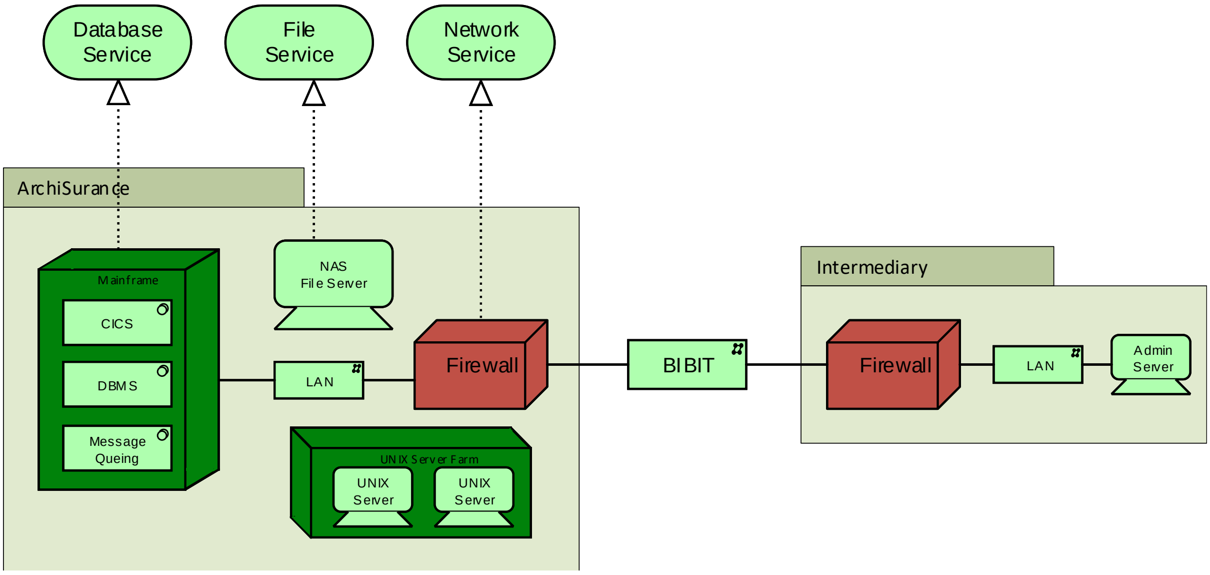


Figure 19: Original alternative ArchiSurance Technology Architecture View.

For last example of the modeling methods introduced in this thesis applied to an existing architecture, we have looked for ArchiSurance views beyond the paper by Jonkers et al. (2016). In a repository by the creators of the Archi modeling tool for ArchiMate (Archi, 2015) we have found another set of models for the ArchuSurance case study. This architecture has a different and simpler technology infrastructure architecture view, which we have used to show our identify viewpoint in effect. The original model can be found in figure 19.

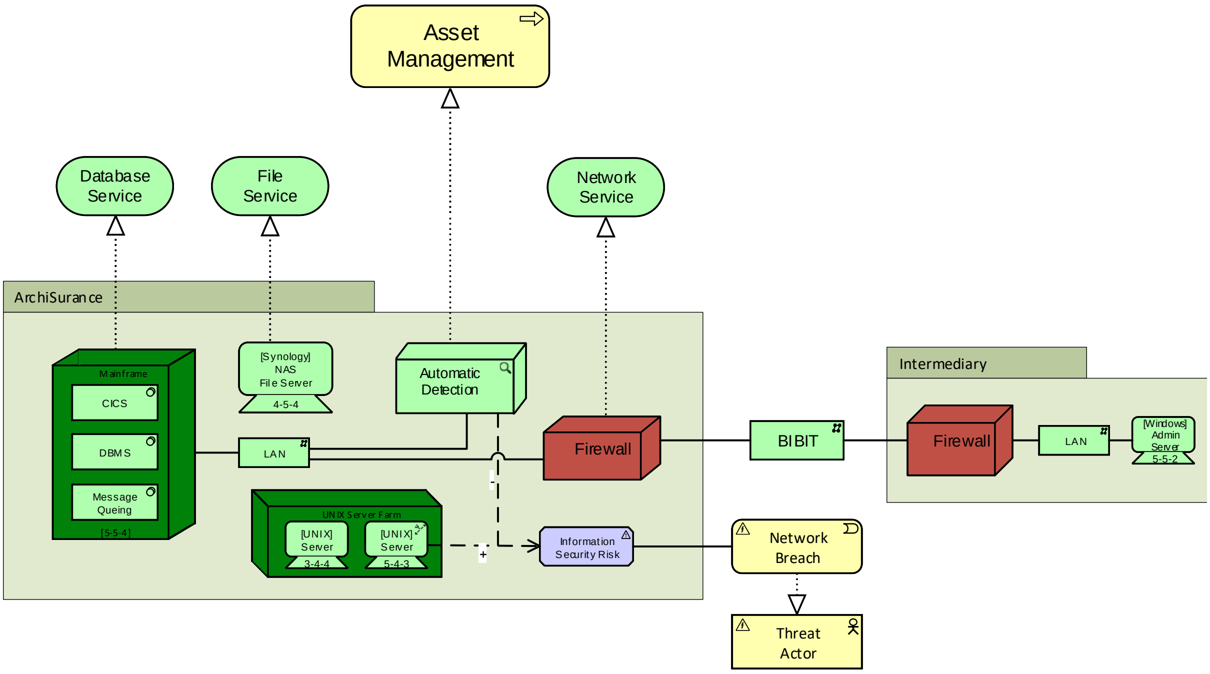


Figure 20: Identify viewpoint applied to the alternative ArchiSurance technical infrastructure view.

The first thing we have added to the existing view is the output of the identification of operating systems used in the network. The servers in the UNIX server farm were already marked with the operating system, here we only adjusted the text between `[UNIX]` to fit the viewpoint. For the other devices in the models we have applied some example operating systems, by making the NAS File Server use Synology, and the Admin server in the intermediary use Windows. Another important aspect of the Identify viewpoint introduced in this thesis is the use of a CIA classification. The NIST framework requires that all network devices are classified, based on interview 3 we have used a confidentiality, integrity and availability-classification between 1 and 5. In this view we have applied some example classifications, where the Mainframe is highly classified and the data should always be correct, with an availability that is slightly lower. The two UNIX servers also have different classifications, where one has a very high confidentiality and the other has a higher availability requirement. This can help decide what new investments should focus on, if a server for example has a high availability it may be worth the investment to duplicate that server off-site.

The first category of the NIST CSF identify category is asset management, for which we have added a business function to the view. The inner workings of that business function would be specified in a different view. In this view, there is automatic detection technology at work to scan the LAN of ArchiSurance and detect devices unknown by the asset management function.

Another important part of the identify category is to identify risks, vulnerabilities and threats. As an example we have assumed that in this view, one of the UNIX servers was found to be vulnerable. This vulnerability increases the information security risk, which is associated to the threat of a network breach. Finally this network breach threat is realized by a threat actor, which is also to be identified. These are all a single example of threats, risks and vulnerabilities, in an actual situation there would be many to be identified in a continuous process.

8 Conclusion

In this thesis we have searched for a bridge between the domains of enterprise architecture, security architecture and information security. We have developed an enterprise architecture viewpoint modeled in the ArchiMate language, which can be used by organizations implementing the NIST Cyber Security Framework. Accompanied by a process to adopt the framework within a cycle of the TOGAF ADM we have shown that enterprise architecture can be of value to certain aspects of information security management. A complete bridge between enterprise architecture, security architecture and information security is not achieved by this thesis, but we have captured useful parts from some of the most used frameworks in each domain: TOGAF and ArchiMate for enterprise architecture, SABSA for security architecture and the NIST CSF for information security management. By doing so, the NIST CSF becomes a little more practical and applicable.

As it is based on audit standards, the NIST framework tells organizations what measures should be taken to improve the state of information security management. The output of this research can show organizations not only *what* measures are to be taken, but also show an example of *how* these measures can be implemented within the scope of enterprise architecture. We have introduced methods of modeling and visualizing the output generated in the NIST CSF, with examples that can make parts of the framework more applicable. These modeling techniques should not be followed as hard rules, but as guidelines to show how certain aspects and steps can be modeled in ArchiMate.

Initially an additional goal was to find a reference architecture, or translation to increase the comprehension of security concerns with top management. After the first two interviews however we noticed that this goal might not only be unfeasible, but also unnecessary. The top management of an organization should be involved in security concerns just as with certain technical concerns: up to a point that is of interest to them and the organization. The technical details might not matter to them, they should concern themselves with the level risk they take, and the level of risk a new measure might introduce or mitigate. That realization was also when the NIST CSF became more interesting to the end goal of this thesis.

As the interviews noted, the NIST framework is a risk based approach to information security management. It is a high level framework that handles the organization as a whole for the functions identify, protect, detect, respond and recover. One interviewee has placed a critical note on the intend to use the NIST framework to design a security program. She stated that the framework is based upon compliance standards which the organization will be checked upon in an audit in the end. Architects should not be concerned with what the auditor checks upon, they should be concerned with keeping the particular case as safe as possible. She did however note that the NIST framework can be useful as a guide to keep in mind which topics to think of while implementing a security program. With that state of mind we have created our model, of which the intention is not to help organizations get certified in certain standards, but to help them be as safe as possible.

The viewpoint we have introduced in this thesis is not be the bridge or translation that is needed between enterprise architecture, security architecture and information security. It can however be of value to organizations that work with enterprise architecture and are looking to adopt the NIST Cyber Security Framework. NIST provides seven steps to implementing its framework, we have taken these steps and mapped them onto the ADM of TOGAF. At the ADM's core is Requirements Management, something to which our interviews have shown that the Business Attribute Profiling method of SABSA can be of value when it comes to security concerns. This combined process of the ADM, NIST implementation steps and SABSA Business Attribute Profiling can help organizations with implementing the NIST Cyber Security Framework within an architecture development cycle. An architecture view based on our viewpoint can clarify the changes in the organization due to this implementation, and identify the strong points and weaknesses of information security. In the identify phase of each repeating cycle the architect can go over the old view and check if the technologies are still secure.

We have applied this viewpoint to the existing architecture of the ArchiSurance case study in three views. This application shows how the viewpoint can be adopted into practice, but the case is not ideal. In a 'real' case there would of course be much more involved with the implementation than our example has shown. Our initial intention was to apply this viewpoint to an actual organization in the process of adopting the NIST framework. But as the viewpoint has grown considerably, applying this viewpoint to an actual case and actually adopting the viewpoint in its entirety would result in a thesis of its own. To that end we have decided to stick with our next-best option: the ArchiSurance case study. This case study shows that our viewpoint can easily be used to implement security measures into existing enterprise architecture, making the steps to implement the NIST CSF a little more practical.

The size of the viewpoint may in the end be too big to fully apply. Although is was never the intention to apply every aspect when implementing a view based on it, at some points it may have become unclear due to the size. This is due to the fact that we have chosen to go through each subcategory of the NIST framework, and see where enterprise architecture can be of value. Another approach was to pick some that enterprise architecture can be of most value to, and model the viewpoint to those. This choice may in the end have resulted in a more clear viewpoint, but the current is more complete. Due to this size, we have also decided to split the viewpoint up for each NIST CSF function. In the interviews however it was noted that between some of these there should be a balance, and they cannot be seen purely separated.

Many elements that we have modeled in the viewpoint are in the technology layer, some of which the technical details are more in-depth that usual for models in ArchiMate. We have chosen to model the whole viewpoint in ArchiMate, at some points we will likely have reached or even crossed the boundaries of what ArchiMate is capable of and intended for. We have introduced many relationships that use stereotyping to indicate the type of relation, many elements that use square brackets in its text, and some newly introduced logos. These are extensions to the language, which also indicates that we have moved beyond the ArchiMate language. For some parts, a domain modeling language may be more applicable. By doing so in ArchiMate however, we have stayed consistent in a way that it can be of value to most divergent cases.

The NIST framework is a large, complex, and high-level framework that consists of many standards, guidelines and best-practices to improve information security management. We have introduced a viewpoint that reduces this complexity on some levels, makes it easier to implement, and combines it with enterprise architecture. To further help adoption we have combined the ADM of TOGAF with the implementation steps of NIST to show how organizations can implement the NIST framework in an architectural way.

8.1 Research Questions

This research has been based on the research questions introduced in section 2.1, which we have tried to answer as extensively as possible. Although the answer of these questions lies mostly in the output, we will summarize them in this section.

SQ 1 : *What processes take place within the different functions identify, protect, detect, response & recover of the NIST Cyber Security Framework?*

We have handled this question by conducting expert interviews, in particular those focused on the NIST CSF (groups B. and C.). We have selected candidates who have experience working with many clients on technical topics in those five functions, or who have carried the responsibility themselves in a security-focused management function of an organization. By asking them the questions in appendix B, we have tried to gather what processes, technologies and other elements take place in those functions.

The results of the interviews have been transcribed, encoded, sorted and shown in appendix C. In section 5.3.2.2 we elaborate further upon these results, but to summarize we will highlight some of the findings here. We have asked the interviewees what examples of technologies, processes and principles take place in each of the NIST function. For identify, an example was the use of threat intelligence to identify what types of threat actors are relevant to the organization. This subject came up in multiple interviews, after which we have dedicated a section of background on it. An example of what the interviews noted in the protect function is to show how the network of an organization is segregated. The NIST framework requires that the network is segregated, our interviews provided some additional information on what the use and limits of the segregation are. For detect the most notable finding was the use of a SOC, a business function (that may span multiple NIST functions) where all security events are collected and analyzed.

Many more technologies, processes and principles were identified in the interviews, the complete list of results can be found in appendix C. The result of this research question is used as input for the next, where the viewpoint itself is formed.

SQ 2 *What does a TOGAF enterprise architecture viewpoint look like as a reference to implement the NIST Cyber Security Framework?*

The second research question focuses on the construction of the viewpoint itself. The answer to this question is provided by the viewpoint in section 6.3. We have used the output of the previous sub-question and literature research to construct the viewpoint. In section 7 we have shown an example of this viewpoint applied to the existing enterprise architecture of the ArchiSurance case study.

Organizations can use this viewpoint in the implementation of the NIST CSF by modeling steps to be taken, their output, and the as-is and to-be architectures. In the identify function for example there is a control that requires all physical devices and systems to be inventoried. Our viewpoint provides a way that inventory can be modeled within enterprise architecture in ArchiMate. Other controls state that risks should be identified, to which our viewpoint also provides a way of modeling.

We have divided the viewpoint into one section for each of the NIST functions. For each function we show what elements, relationships and actors are relevant at the lowest level of the NIST CSF (the subcategories). Due to the amount of categories and subcategories, this viewpoint has grown quite large. Therefore it is not the intention that organizations adopt all elements when creating a view based on it, but follow the steps in the process (see RQ 3 below) and use the elements, relationships and actors when necessary.

SQ 3 *What does the combined process for implementing the NIST Cyber Security Framework and the TOGAF Architecture Development Method look like?*

The viewpoint provided by the answer to SQ 2 is intended to help organizations implement the NIST CSF. This sub-question complements SQ 2 by researching what a combined process of those two frameworks looks like. We have answered this question by constructing the combined process shown in figure 14. In this process we have mapped the steps for implementing the NIST framework onto phases in the ADM, and combined the requirements management phase in the center with the Business Attribute Profiling method of SABSA, as the interviews pointed out the use of this method for handling security requirements. The resulting process provides a way of implementing the NIST CSF within a TOGAF architecture development cycle, creating an architecture of the organization with the NIST Cyber Security Framework adopted.

The answers of these sub-questions together form the answer to the research question of this thesis:

RQ 1 *What does an enterprise architecture viewpoint and process for implementing the NIST Cyber Security Framework within enterprise architecture look like?*

SQ 1 provides input for SQ 2, which together with SQ 3 provide the answer in two parts of RQ 1: a viewpoint and a process. We have answered the question what an enterprise architecture viewpoint and process for implementing the NIST CSF looks like with an example of a viewpoint and process. These two can together be used as guidance for any organization implementing the NIST Cyber Security Framework within an enterprise architecture development cycle. The process can be followed to implement the framework, the viewpoint can be used at multiple steps to show how the architecture changes or should change in this process.

9 Further Research

In the combined fields of information security and enterprise architecture much research still lies ahead in the future. As shown in section 1, the topic of information- and cyber security will likely only become more important in the future, and enterprise architecture can be of value to organize this process for large organizations. The relationship between security architecture and enterprise architecture can still be more close and intertwined, an single architecture framework that encompasses both in a comprehensible manner could close this gap.

As discussed in section 8, our viewpoint has grown large to encompass as much of the NIST Cyber Security Framework in its entirety within a modeling method. To get more in-depth and detailed, smaller viewpoints tailored to single categories could provide value at a different level to those implementing the NIST framework. We have chosen to handle as many (sub-) categories as we thought enterprise architecture could be of value to, another approach would be to select some and handle them in detail.

In section 8 we have also stated that some parts of the model may have surpassed the use of ArchiMate as a modeling language. Combined with the in-depth handling of small parts of the viewpoint as described earlier, it can be of value to translate some these parts into domain modeling languages such as UML or BPML. The value of these models in a domain modeling language is that it is of more value to practitioners of those domains, who are used to modeling that way.

The approach we have taken to assist in implementing the NIST Cyber Security Framework can also be adopted to many other frameworks to which enterprise architecture can provide value. Within the field of information security some examples would be the ISO 27000 family to help implement an ISMS, the framework by ENISA, The COBIT cyber security framework, and many other frameworks could use additional guidance and modeling tools for implementation.

Another interesting research following this thesis can be to apply this viewpoint to an organization in the process of implementing the NIST Cyber Security Framework. This would require close cooperation with those involved with the decision-making for the adoption of the framework and architects, which is where the viewpoint is of most value. This would also apply to the process we have introduced in section 6.4. An interesting topic of research would be to apply this process to an organization using the TOGAF and the ADM to maintain an enterprise architecture. This does require an organization that uses the ADM and plans to implement the NIST Cyber Security Framework.

References

Allen, G. & Derr, R. (2015). *Threat assessment and risk analysis: An applied approach.* Elsevier Science. Retrieved from https://books.google.nl/books?id=YzFOBQAAQBAJ

Archi. (2015). Archimodels. https://github.com/archimatetool/ArchiModels/tree/master/Archisurance. GitHub.

AWS. (n.d.). AWS identity and access management user guide. Retrieved from https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf

Bailey, T., Miglio, A. D., & Richter, W. (2014). The rising strategic risks of cyberattacks. *McKinsey Quarterly*, *2*, 17–22.

Bejtlich, R. (2010). Understanding the advanced persistent threat. Retrieved from https://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat

Bidou, R. (2005). Security operation center concepts & implementation. Retrieved from http://www.iv2-technologies.com/SOCConceptAndImplementation.pdf

Chan, Y. E. & Reich, B. H. (2007). It alignment: What have we learned? *Journal of Information technology*, *22*(4), 297–315.

Cherdantseva, Y. & Hilton, J. (2013). A reference model of information assurance & security. In *2013 international conference on availability, reliability and security* (pp. 546–555). IEEE.

Christensson, P. (2014). SDLC definition. Retrieved from https://techterms.com/definition/sdlc

Clark, T., Barn, B., & Oussena, S. (2012). A method for enterprise architecture alignment. (Vol. 120). doi:10.1007/978-3-642-31134-5_3

Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: Challenges and opportunities. (pp. 1–6). doi:10.1007/978-3-319-73951-9_1

Department of Defense. (2010). DoD reference architecture white paper. Retrieved from https://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf

Ekstedt, M. & Sommestad, T. (2009). Enterprise architecture models for cyber security analysis. *Industrial Information and Control Systems, KTH - Royal Institute of Technology, Sweden.*

Gosselt, R. (2012). A maturity model based roadmap for implementing TOGAF. In *17th twente student conference on IT.*

Greenwald, J. (2017). Cyber security framework marches forward. *Business Insurance*, *3*. Retrieved from https://www.businessinsurance.com/article/20170703/NEWS06/912314233/Cyber-security-framework-President-Donald-Trump-executive-order

Grounded Theory Online. (2016). What is grounded theory? Retrieved from http://www.groundedtheoryonline.com/what-is-grounded-theory

Hernandez, N. (2018). Noc/soc integration: Opportunities for increased efficiency in incident response within cyber-security. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/noc-soc-integration-opportunities-increased-efficiency-incident-response-cyber-security-38290

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(1), 113–125.

ISO 22301. (2012). *Societal security - Business continuity management systems - Requirements.* International Organization for Standardization. Geneva, CH. Retrieved from https://www.iso.org/standard/50038.html

ISO/IEC 27001. (2005). *Information technology — security techniques — information security management systems — requirements (iso/iec 27001:2005.* International Organization for Standardization. Geneva, CH. Retrieved from https://www.iso.org/standard/50297.html

ISO/IEC 27002. (2013). *Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2005).* International Organization for Standardization. Geneva, CH. Retrieved from https://www.iso.org/standard/54533.html

ISO/IEC 27000. (2012). *ISO-IEC-27000-2012, Information security management systems — Overview and vocabulary (2012) (ISO/IEC 27000:2012).* International Organization for Standardization. Geneva, CH. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

ISO/IEC/IEEE 42010. (2013). *Systems and software engineering – Architecture description.* International Organization for Standardization. Geneva, CH. Retrieved from https://www.iso.org/standard/50508.html

Joint Task Force. (2018). Risk management framework for information systems and organizations. *NIST Special Publication*, *800*, 37.

Jonkers, H., Band, I., Quartel, D., & Lankhorst, M. (2016). Archisurance case study version 2. *The Open Group.* Retrieved from https://publications.opengroup.org/downloadable/download/link/id/MC42MDAyMjAwMCAxNTUwNTkwODIxMzIzMzc1MzM0NDgwMjcx/

Kotusev, S. (2016). The critical scrutiny of togaf. British Computer Society.

Lankhorst, M. (2004). Archimate language primer. introduction to the archimate modelling language for enterprise architecture.

Lankhorst, M. (2009). *Enterprise architecture at work: Modelling, communication and analysis* (4th ed.). Heidelberg: Springer-Verlag.

Martin, P. Y. & Turner, B. A. (1986). Grounded theory and organizational research. *The journal of applied behavioral science*, *22*(2), 141–157.

Mees, W. (2017). Security by design in an enterprise architecture framework. *Royal Military Academy, Department CISS. Renaissancelaan*, *30.*

Nadel, B. A. (2004). *Building security: Handbook for architectural planning and design.* McGraw-Hill Education. Retrieved from https://www.amazon.com/Building-Security-Handbook-Architectural-Planning-ebook/dp/B001QFY54U?SubscriptionId=AKIAIOBINVZYXZQZ2U3A&tag=chimbori05-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=B001QFY54U

NIST. (2018). Framework for improving critical infrastructure cybersecurity v1.1. *National Institute of Standards and Technology.* Accessed: 2018-7-9. doi:10.6028/NIST.CSWP.04162018

Oda, S. M., Fu, H., & Zhu, Y. (2009). Enterprise information security architecture a review of frameworks, methodology, and case studies. In *Computer science and information technology, 2009. iccsit 2009. 2nd ieee international conference on* (pp. 333–337). IEEE.

OSA. (n.d.). Open security architecture. Retrieved from https://www.opensecurityarchitecture.org/cms/definitions/it-architecture

Rossi, B. (2015). 6 critical steps for responding to a cyber attack. Retrieved from https://www.information-age.com/6-critical-steps-responding-cyber-attack-123459644/

Saito, W. H. (2016). It's time to think of cybersecurity as a business enabler. *Forbes.* Retrieved from https://www.forbes.com/sites/williamsaito/2016/07/01/its-time-to-think-of-cybersecurity-as-a-business-enabler

Saltzer, J. H. & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278–1308.

Schoonderbeek, J. (2014). Long read: Modelling identity in enterprise architecture / archimate – archi. Retrieved from https://www.archimatetool.com/blog/2018/12/07/long-read-modelling-identity-in-enterprise-architecture-archimate/

Sessions, R. (2007). A comparison of the top four enterprise-architecture methodologies. *Houston: ObjectWatch Inc.*

Shackleford, D. (2015). Who's using cyberthreat intelligence and how? – a sans survey. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-%2035767

Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise security architecture-SABSA. *SABSA, White Paper.*

Shoemaker, D., Kohnke, A., & Sigler, K. (2016). *A guide to the national initiative for cybersecurity education (NICE) cybersecurity workforce framework (2.0).* CRC Press.

Snyder, C. & Southwell, M. (2006). *Pro PHP security.* Apress.

Sousa, P., Caetano, A., Vasconcelos, A., Pereira, C., & Tribolet, J. (2007). Enterprise architecture modeling with the unified modeling language. In *Enterprise modeling and computing with uml* (pp. 67–94). IGI Global.

Spencer Pickett, K. (2006). *Enterprise risk management: A manager's journey.* Wiley. Retrieved from https://books.google.co.uk/books?id=MlQ4SZyxL3AC

SSH.com. (n.d.). NIST cybersecurity framework. Retrieved from https://www.ssh.com/compliance/cybersecurity-framework/

The Open Group. (n.d.). Security architecture — the open group. Retrieved from http://www.opengroup.org/content/security-architecture

The Open Group. (2017). *Archimate 3.0.1 specification.* The Open Group. Retrieved from http://www.opengroup.org/archimate/downloads

The Open Group. (2018). The TOGAF® standard, version 9.2. Retrieved from http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html

The Open Group TOGAF-SABSA Integration Working Group. (2011). TOGAF® and SABSA® integration. *The Open Group and The SABSA Institute.*

Thorn, A., Christen, T., Gruber, B., Portman, R., & Ruf, L. (2008). What is a security architecture? *Information Security Society Switzerland.*

Umeh, N., Dagli, C., & Miller, A. (2007). TOGAF vs. DoDAF: Architecting frameworks for net-centric systems. In *Iie annual conference. proceedings* (p. 322). Institute of Industrial and Systems Engineers (IISE).

Von Solms, R. & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Wahe, S. & Petersen, G. (2011). *Open enterprise security architecture (O-ESA): A framework and template for policy-driven security.* Zaltbommel: Van Haren Publishing.

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

Wrenn, G. (2017). *CSO Online.* Retrieved from https://www.csoonline.com/article/3239968/security/how-can-my-cyber-program-benefit-from-a-standards-based-approach.html

ENISA. (n.d.). NIS directive. Retrieved from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive

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

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

A Interviewee Qualifications

Qualifications interviewees

This document specifies the minimal requirements that an interviewee for the thesis should have. It is divided into two groups: internal and external interviewees. This differentiation is made in the thesis to gather knowledge from people who have worked as an expert advising third parties on enterprise- or security architecture or cyber security, and from people who have themselves had the responsibility for the protection of information security within an organisation. The internal interviewees are employed as consultant within the business unit Cyber Forensics & Privacy of PwC.

Internal

Minimum function level	Senior associate*
Minimum years of experience	3

* Management level would be preferred, however the higher in the hierarchy employees tend to be further away from the actual experience. To capture that experience, some senior associate level employees might be interviewed.

External

Minimum function level	Management
Minimum years of experience	5
Additional requirements	Has carried the responsibility for information security within an organisation
OR	Has, successfully or unsuccessfully implemented or revised an enterprise architecture focussed on information security

B Interview Questions

General

1. Is it okay if I record this interview? I will of course treat it confidentially, and delete it after use. I am currently writing my thesis on Enterprise Architecture, specific the integration of information security within enterprise architecture. I am creating an enterprise architecture viewpoint, aimed at assisting organisations in implementing the NIST cyber security framework.
2. What is your current function and area of expertise?
3. How many years of experience do you have in this field?
4. How would you describe your, or your organisation's, experience with Enterprise Architecture?
    a. Security Architecture
    b. Frameworks, TOGAF, SABSA?
    c. Relationship between the fields
5. Do you use or have experience with any security frameworks, such as NIST CSF?

   TOGAF states on security concerns: "security concerns are pervasive throughout the architecture domains and in all phases of the architecture development. Security is called out separately because it is infrastructure that is rarely visible to the business function"
6. Do you agree with this statement, or can security concerns provide value to the business function?

7. Is there anything I have forgotten to ask, or you would like to say on the subject?
8. Would you potentially be available for a follow-up via email?
9. Thank you for your time!

Only focused on the NIST cyber security framework

10. The viewpoint I'm creating is based on the NIST CSF, in a way it may make it easier to implement this framework. Within NIST there are 5 classifications: Identify, Protect, Detect, Respond & Recover. Can you name examples of processes, components or systems you have implemented in each classification? In addition, what would you like to add with unlimited resources and no limitations?
    a. Identify
    b. Protect
    c. Detect
    d. Respond
    e. Recover
11. What problems would you encounter implementing this, why is it a 'perfect world' scenario?
12. How do you think the involvement of top management would be?
13. How would you increase that involvement?
    a. Risk classification/translation?

Only focused on EA/SA and information security management

10. If you could start from scratch to implement your organization from scratch, no limitations. What would you do for information security?
    a. Business, data, application and technology layer
    b. How do you think top management would be involved in this?
11. What difficulties would you encounter, why is this a 'perfect world' scenario?
12. How do you think you can increase involvement of stakeholders, such as top management and get them to see the need?
13. Do you think these difficulties could be solved with architecture?

14. Can you explain what you experience with the NIST cyber security framework has been?
    a. Do you think current cyber security frameworks such as NIST could help?
15. How do you think that involvement and awareness from top management helps?
    a. How do you think this could be increased?

If it has not yet come up, mention viewpoint/plan, simplification of security architecture within enterprise architecture.

16. Do you think this could be a solution to (certain) problems mentioned today?
    a. To which, which not?
17. How would do you think this could be used in practice?
    a. Which processes, principles, stakeholders etc.

C Interview Results Coded

		1	2	3	4	5	6
Identify	ID	Cloud assets & services	Business strategy & direction	Penetration tests to identify vulnerabilities	Relevant threats and risks	Automatic cloud asset discovery	Data flows
	ID	Crown jewels	Requirements (+ classification)	Threat actors	Maturity	Automatic network device discovery	Data flows that should be encrypted
	ID	Legal obligations	SABSA Business Attribute Profiling	Threat actor goals	Applications	Risk assessment	Business Impact Analysis
	ID	Data location (US)	Risks, costs and benefits of new tech.	Critical business processes	Assets	Lower risk	Automatic Discovery
	ID	Shadow IT	Risk calculation, statistics	CIA classification - balance needs	Threats	Accept risk	CMDB
	ID	Business strategy	Risk appetite	Threats	Risks	Mitigate risk	Outsourcing
	ID	Mission	Procurement for buying new tools	Dataflows	Dataflows between assets	Risk cost benefits	Governance plan (structuring)
	ID	Vision		Monitoring also vuln: collect data	Vulnerabilities	Continuous risk assessment process	Stakeholders internal and external
	ID	Change management		Analyse current state	Information influencing risks and threats		Vendor management
	ID	Non functional requirements		Risks	Governance		Roles and responsibilities
	ID	Business Impact Analysis		Accept risk	Criticality classification of systems		ID.BE = combination of governance and risk
	ID	Governance		Identify vulnerabilities & paths	Crown jewels		Business values, mission, vision
	ID	Threat actors			Threat intelligence		SABSA entities and attributes
	ID	Threat intelligence			Involve legal stakeholders		Vulnerability scans
	ID	Risk management					SABSA Business Attribute Profiling
Protect	PR	Disk encryption	Awareness	Redundancy	Mitigate threats and risks	Firewall	Physical access
	PR	Managed devices	Firewall	Different degrees of acces	Security controls	Cloud protection subscription	IT security access control
	PR	Cloud encryption	CHOMP server	Network segmentation & layers	Policies		IAM
	PR	Data centre duplication	IAM (as a service)	admin & users different segment	Procedures		Old system usernames and passwords
	PR		PIM, PAM, PUM (PxM)	Dataflow same class as source	Antivirus		Tokens
	PR		Authentication - collaboration (oAuth etc)	Patch management cycle - how long	Firewall		2-factor authentication
	PR			Central proxy	Intrusion Prevention (IPS)		Role based IAM system
	PR			Endpoint protection	Encryption		PR.AT Awareness campaigns
	PR			No local admin, users low level	SIEM		PR.AT Awareness Phishing emails
	PR			FireArk, sandbox scan incoming	Incident Management		PR.AT Awareness tests
	PR			No account re-use			PR.AT Awareness training
	PR			Disk encryption			PR.DS Where is the data stored
	PR			Password policies			PR.DS Classification of data
	PR			USB stick vulnerabilities & policies			PR.DS Network security: what systems the data goes through
	PR			IPS + service			Color-coding (un)encrypted dataflows
	PR						Principles
Detect	DE	x	x	Monitoring automised	SOC	Detective measures	Fraud management department
	DE			Sensors, network, people	Intrusion Detection (IDS or IPS)	In-depth inspection & correlation	Focus on incoming and outgoing data
	DE			False positives (peak), callibration	Traffic flows in network	Maintenance and tuning	Global SOC
	DE			Collect data - monitoringsolution	Classification	Threat-or-no-threat classification	Managed Security Provider
	DE			Monitoring push vs pull --> relationship	Log collection	Resource intense	SIEM
	DE			User activities	Map traffic with threat analysis	False positives	Logging
	DE			IPS	SIEM		Monitoring
	DE			External detection service (SOC)			Threat Hunting
	DE			Endpoint protection			Threat Intelligence
	DE			Privacy issues			
Respond	RS	x	x	Response escalation automised	SOC	Security Incident Procedures	Incident Management process
	RS			Kill traffic	Procedures	Security council as stakeholder	24/7 security teams
	RS			Related to CIA (down traffic <> A=5)	Clean system	Incident Management Process	Outsourcing
	RS				Isolate system	Automatic reactions	Measure and analyse vuln. scans
	RS				Turn off system	Stakeholder senior decisions needed	Output to backlog of IT
	RS				Wake up		
	RS				External incident response		
	RS				Response to detect & prevent		
	RS				Correct permissions to block etc		
	RS				Incident Response (external)		
	RS				Quick contact with CISO stakeholder		
	RS				Continuous improvement		
Recover	RC	x	Reputation	x	Business Continuity	Recover backups	Business Continuity
	RC				Recover after incident	Rules and routing	Separate role
	RC				Something was down, on purpose or attack	Public cloud failover	Outside of IT and security
	RC				Structured recovery	Declaration of disaster	Drills
	RC				Recover backups	Multi-cloud recovery	Incident Management process
	RC				Lessons learned	Recover cloud location	Tabletop
	RC				Root cause analysis		Audit process
	RC						
	RC						

ID			PR			DE			RS			RC		
Code	**Source**	**Used**	**Code**	**Source**	**Used**	**Code**	**Source**	**Used**	**Code**	**Source**	**Used**	**Code**	**Source**	**Used**
Accept risk	3	x	2-factor authentication	6	x	Classification	4	x	24/7 security teams	6	x	Audit process	6	
Accept risk	5	x	admin & users different segment	3	x	Collect data - monitoringsolution	3	x	Automatic reactions	5	x	Business Continuity	4	
Analyse current state	3		Antivirus	4		Detective measures	5	x	Clean system	4	x	Business Continuity	6	
Applications	4	x	Authentication - collaboration (oAuth etc)	2	x	Endpoint protection	3	x	Continuous improvement	4	x	Declaration of disaster	5	
Assets	4	x	Awareness	2	x	External detection service (SOC)	3	x	Correct permissions to block etc	4		Drills	6	
Automatic cloud asset discovery	5	x	Central proxy	3		False positives	5	x	External incident response	4	x	Incident Management process	6	
Automatic Discovery	6	x	CHOMP server	2		False positives (peak), callibration	3	x	Incident Management Process	5	x	Lessons learned	4	
Automatic network device discovery	5	x	Cloud encryption	1	x	Focus on incoming and outgoing data	6	x	Incident Management process	6	x	Multi-cloud recovery	5	
Business Impact Analysis	1	x	Cloud protection subscription	5		Fraud management department	6		Incident Response (external)	4	x	Outside of IT and security	6	
Business Impact Analysis	6	x	Color-coding (un)encrypted dataflows	6		Global SOC	6	x	Isolate system	4	x	Public cloud failover	5	
Business strategy	1	x	Data centre duplication	1		In-depth inspection & correlation	5	x	Kill traffic	3	x	Recover after incident	4	
Business strategy & direction	2	x	Dataflow same class as source	3	x	Intrusion Detection (IDS or IPS)	4	x	Measure and analyse vuln. scans	6	x	Recover backups	4	
Business values, mission, vision	6	x	Different degrees of acces	3	x	IPS	3	x	Output to backlog of IT	6		Recover backups	5	
Change management	1	x	Disk encryption	1	x	Log collection	4	x	Outsourcing	6	x	Recover cloud location	5	
CIA classification - balance needs	3	x	Disk encryption	3	x	Logging	6	x	Procedures	4	x	Reputation	2	
Cloud assets & services	1	x	Encryption	4	x	Maintenance and tuning	5	x	Quick contact with CISO stakeholder	4	x	Root cause analysis	4	
CMDB	6		Endpoint protection	3		Managed Security Provider	6		Related to CIA (down traffic <> A=5)	3	x	Rules and routing	5	
Continuous risk assessment process	5	x	FireArk, sandbox scan incoming	3		Map traffic with threat analysis	4	x	Response escalation automised	3	x	Separate role	6	
Critical business processes	3	x	Firewall	2	x	Monitoring	6	x	Response to detect & prevent	4	x	Something was down, on purpose or attack	4	
Criticality classification of systems	4	x	Firewall	4	x	Monitoring automised	3	x	Security council as stakeholder	5	x	Structured recovery	4	
Crown jewels	1	x	Firewall	5	x	Monitoring push vs pull --> relationship	3	x	Security Incident Procedures	5	x	Tabletop	6	
Crown jewels	4	x	IAM	6	x	Privacy issues	3		SOC	4		x	1	
Data flows	6	x	IAM (as a service)	2	x	Resource intense	5		Stakeholder senior decisions needed	5	x	x	3	
Data flows that should be encrypted	6	x	Incident Management	4		Sensors, network, people	3	x	Turn off system	4	x			
Data location (US)	1	x	Intrusion Prevention (IPS)	4	x	SIEM	4	x	Wake up	4	x			
Dataflows	3	x	IPS + service	3	x	SIEM	6	x	x	1				
Dataflows between assets	4	x	IT security access control	6	x	SOC	4	x	x	2				
Governance	1	x	Managed devices	1	x	Threat Hunting	6	x						
Governance	4	x	Mitigate threats and risks	4		Threat Intelligence	6	x						
Governance plan (structuring)	6	x	Network segmentation & layers	3	x	Threat-or-no-threat classification	5	x						
ID.BE = combination of governance and ris	6	h	No account re-use	3	x	Traffic flows in network	4	x						
Identify vulnerabilities & paths	3	x	No local admin, users low level	3	x	User activities	3	x						
Information influencing risks and threats	4	x	Old system usernames and passwords	6	x	x	1							
Involve legal stakeholders	4	x	Password policies	3		x	2							
Legal obligations	1	x	Patch management cycle - how long	3	x									
Lower risk	5	x	Physical access	6	x									
Maturity	4		PIM, PAM, PUM (PxM)	2	x									
Mission	1	x	Policies	4										
Mitigate risk	5	x	PR.AT Awareness campaigns	6	x									
Monitoring also vuln: collect data	3		PR.AT Awareness Phishing emails	6	x									
Non functional requirements	1		PR.AT Awareness tests	6	x									
Outsourcing	6		PR.AT Awareness training	6	x									
Penetration tests to identify vulnerabilities	3		PR.DS Classification of data	6										
Procurement for buying new tools	2		PR.DS Network security: what systems th	6	x									
Relevant threats and risks	4		PR.DS Where is the data stored	6	x									
Requirements (+ classification)	2		Principles	6										
Risk appetite	2	x	Procedures	4										
Risk assessment	5	x	Redundancy	3										
Risk calculation, statistics	2	x	Role based IAM system	6	x									
Risk cost benefits	5		Security controls	4										
Risk management	1	x	SIEM	4	x									
Risks	3	x	Tokens	6	x									
Risks	4	x	USB stick vulnerabilities & policies	3										
Risks, costs and benefits of new tech.	2	x												
Roles and responsibilities	6	x												
SABSA Business Attribute Profiling	2	x												
SABSA Business Attribute Profiling	6	x												
SABSA entities and attributes	6													
Shadow IT	1													
Stakeholders internal and external	6	x												
Threat actor goals	3	x												
Threat actors	1	x												
Threat actors	3	x												
Threat intelligence	1	x												
Threat intelligence	4	x												
Threats	3	x												
Threats	4	x												
Vendor management	6													
Vision	1	x												
Vulnerabilities	4	x												
Vulnerability scans	6	x												

D Interview Codes and NIST CSF Mapping

Function	Category	Subcategory	#	Interviews	Ideas of application in the viewpoint
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.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	1,4 5,6	Overview of assets and data flow between them Automatic discovery of (cloud) assets	Model physical devices as components Technology layer Laptop, server, mobile device etc. Automatic discovery tools, SIEM etc
		ID.AM-2: Software platforms and applications within the organization are inventoried	1,4	Overview of applications and services	Model applications as components Windows/linux, modeling and categorizing software on machines Automatic discovery tools (SIEM etc)
		ID.AM-3: Organizational communication and data flows are mapped	3,4,6 6	Data flows within the organisations are mappped Data flows should be catigorized, e.g. encrypted	Model types of communication as relationships Way of modeling data flows between servers and clients. Generates logfile Flows relationship
		ID.AM-4: External information systems are catalogued	1,5 1	Overview of cloud services and applications Location of the data (e.g., U.S.)	External information systems visualised --> Specify 'outside of the organization' by e.g. groups --> Different sources of information shared to and from
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	3 4	Classification of CIA of 1 to 5 - balance needed Classify the criticality of systems	Link to ID.AM-1 and -2. Criticality rating (or colour coding) needed. (1-5) CIA triad, on a scale between 1-5
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	6 6	Roles and responsibilities are clearly defined Stakeholders internal and external are identified	Model cybersecurity actors and roles Different actor model for workforce, suppliers, customers.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated			--> Out of scope, already in business architecture
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated			--> Out of scope, already in business architecture
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	1,2,6	Business mission, vision, strategy and objectives are identified	--> Out of scope, already in business architecture
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	3 1,3,4	Identify critical business processes Identify what the crown jewels of the organisation are (goals of threat actors)	--> Out of scope, already in business architecture
		ID.BE-5: Resilience requirements to support delivery of critical services are established			--> Out of scope, already in business architecture
		Other remarks	6	Business environment is a combination of governance and risk	
	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 cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	1,4,6	Governance for information security should be defined	Model information security policy somehow
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	6	Roles and responsibilities are clearly defined	Roles & responsibilities Actors and roles "A business role is the responsibility for performing specific behavior, to which an actor can be assigned, or the part an actor plays in a particular action or event."
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	1 4 2,6	Legal requirements Stakeholders from legal involved SABSA business attribute profiling for requirements	Requirements, obligations --> special type of requirement for legal requirement --> special type of requirement for SABSA business attributes
		ID.GV-4: Governance and risk management processes address cybersecurity risks	1,4,6	Governance for information security should be defined	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	4,6 3 3 5	Vulnerabilities are identified (by automatic scans) Vulnerabilities and possible paths Penetration tests Risk assessment	Vulnerability element extension Can be added to all assets - Technical device - Software component
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	1,4,6	Threat Intelligence	Sharing source entity Relationship oneway or twoway
		ID.RA-3: Threats, both internal and external, are identified and documented	1,3 3,4	Identify possible threat actors Identify threats	Threat element extension Internal and external
		ID.RA-4: Potential business impacts and likelihoods are identified	1,6	Business Impact Analysis	Business impact analysis is the way risks are determined and found. Its output can be modeled by the risk, vulnerabilities and threat elements of the other subcategories.
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	1,6	Business Impact Analysis	Relationship between threat, vulnerabilities, likelihood and risk ⚠
		ID.RA-6: Risk responses are identified and prioritized	3,5	Accept, mitigate, transfer risks	Element for risk response? Mitigate, transfer, accept --> relationships between elements and risks
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	1,2,3, 5	Risk management Continuous improvement	Risk management as a business process
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	2	Organisation's Risk Appetite is determined	Different levels of risk tollerance as elements in the motivational layer
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	2	Risks are calculated based on statistics	
	Others	**Maturity**	#	Identify maturity of functions, capabilities or components	
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	2,6 2 3	IAM service, IT Access Control Authentication method (oAuth) Privileged User Management	Model different roles and identities (admin, user etc) Model type of authentication - Tokens, OTP, SSH Keys, etc. Mark privileged user accounts, lock? --> exclamation mark (from Archimate principle)
		PR.AC-2: Physical access to assets is managed and protected	6	Physical access is managed, e.g. gates	Extension of physical architecture. Outside of scope?
		PR.AC-3: Remote access is managed	3 3 a	Different degrees of access Identify different paths (of possible attackers) Remote access must be properly managed and monitored. Encrypted protocols, such as SSH, Remote Desktop, or HTTPS are typically used. Access should be monitored and tunneling back into the internal network from the outside should be prevented.	Model different points of acces in and out of the network? --> all ways of communicating with the outside world should be monitored --> catalogue all external communications
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and	6 3 6	Role based IAM No local admin, no account re-use Access by tokens, 2FA, passwords	Specify the type of access allowed, 2FA, OTP --> Application roles for different services

PROTECT (PR)		separation of duties	b	Role based IAM	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	3 3 2,4,5 3,4 a	Network is segratated in layers Admin and users are not in the same layer Use of firewalls Use of IPS	Model different segments in the network and what machines are where Model firewalls, IPS, etc. --> Network roles for segregation
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	6 6 6	Awareness training Awareness campaigns Phishing campaigns	Model all types of awareness activities - Training - Campaigns
		PR.AT-2: Privileged users understand roles & responsibilities	6 6 6 6	Awareness training Awareness campaigns Awareness tests Tabletop	
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities			
		PR.AT-4: Senior executives understand roles & responsibilities	6 6	Awareness training Awareness campaigns	
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	6 6 6 6	Awareness training Awareness campaigns Awareness tests Tabletop	
	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.	**PR.DS-1:** Data-at-rest is protected	1,3,4 6	Data is encrypted Location of the data	Way of modeling data that is encrypted or unencrypted: lock icon 🔒 🔓
		PR.DS-2: Data-in-transit is protected	6 3 a	What systems the data goes through Dataflow has same classification as source File transfers should use secure protocols.	Way of modeling data flows that are encrypted or should be encryted --> communication channels with protocol, e.g. TLS 1.3
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	1	Use of managed devices	--> Asset management, out of scope
		PR.DS-4: Adequate capacity to ensure availability is maintained			--> to specific to each case, out of scope
		PR.DS-5: Protections against data leaks are implemented	a	Data Loss Prevention (DLP) systems should be deployed. Such systems should also monitor encrypted file transfers and terminal sessions.	DLP systems modeled as component --> handled more in detail in detect
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity			Model the output of verification/verification process Source of software and certificates?
		PR.DS-7: The development and testing environment(s) are separate from the production environment			Model different environments? Servers?
	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.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained			ISO27001: change management, control and restriction of installation of software, changes to systsems in SDLC --> mostly change management process
		PR.IP-2: A System Development Life Cycle to manage systems is implemented			System development life cycle is a management approach to develop systems Examples are scrum, waterfall etc. How to show - parts of the EA that use some type of SDLC? - or parts that make the process
		PR.IP-3: Configuration change control processes are in place	1	Change management process involved	Change management process in place, model process
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	4,5	Recovery of backup in Recover, here these backups are made	From server to backup location - dataflow Periodic - show how often somehow. Location - onsite or offsite
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met			Out of scope
		PR.IP-6: Data is destroyed according to policy			Data destruction visualised somehow
		PR.IP-7: Protection processes are continuously improved			Continuous improvement, not modelable? Out of scope
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties			External entities to be shared with - same as in identify
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed			Out of scope
		PR.IP-10: Response and recovery plans are tested			Out of scope
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)			Out of scope
		PR.IP-12: A vulnerability management plan is developed and implemented			Followup on Identify vulnerability scanning & detection Management plan can be modeled, output from ID.RA-1
		PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools			

	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	` `			
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	3	Patch management cycle - time to patch	Model how long it takes to roll out patches
	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.	**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	3	USB devices enabled/disabled, enforced by tech.	
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality			Eleboration of PR.AC
		PR.PT-4: Communications and control networks are protected	2,4,5 3,4	Use of firewalls Use of IPS	Eleboration of PR.AC
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed			Data flow of Identify
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	5	In-depth inspection and correlation	Event --> response Process, outcome is an event, flows to analysis
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	3,4,6	Log collection	Multiple sources, logs etc.
		DE.AE-4: Impact of events is determined	3,5 4,5	False positives Classification of threats	Same as in identify
		DE.AE-5: Incident alert thresholds are established			
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	3,4 4,6 3 3,6 4 3,6	Intrusion Detection & Protection (IDS/IPS) SIEM, SOC Monitoring, push vs pull Incoming and outgoing data Traffic flows in the network Monitoring service	IPS, SIEM, SOC modeling Log collection - push or pull SOC outsourced or inside Incoming and outgoing data flows --> ports opened/services exposed? Emails scanning. Incoming mail = event, starts scanning procedure?
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events			Out of scope
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	3 3	Detection on endpoints Users' activity monitored	Technology used to scan -- Software/hardware --Antivirus on endpoints
		DE.CM-4: Malicious code is detected	3	Detection on endpoints	Virus scanners on endpoint Not very modelable
		DE.CM-5: Unauthorized mobile code is detected	3	Detection on endpoints	Virus scanners on endpoint Not very modelable/different from previous subcategory in this scope
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	ISO	The organization shall supervise and monitor the activity of outourced system development.	ISO: checking of outsourced development. Testing, reviewing etc. --> Out of scope
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	3,4	Intrusion Detection & Protection (IDS/IPS)	IDS/IPS as technology node or software component
		DE.CM-8: Vulnerability scans are performed	3 6	Penetration tests Vulnerbility scans	Main to model is outcome, already in identify
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	3	Detective measures	Roles and responsibilities, business roles --> actors
		DE.DP-2: Detection activities comply with all applicable requirements	2,6	SABSA business attribute profiling for requirements	Requirements + SABSA Business Attribute Modeling
		DE.DP-3: Detection processes are tested			Testing of the system as a process? --> Out of scope
		DE.DP-4: Event detection information is communicated to appropriate parties	4,6	Threat Intelligence	Sharing source entity, same as identify and protect
		DE.DP-5: Detection processes are continuously improved	5	Maintenance and tuning	Out of scope
		Overig			
	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	4 4,5,6 4,5 3,5	Response to detect & protect Incident management plan or Incident response process Procedures Automisation	Out of scope - but expanation of automation and procedures.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	6,4	24/7 on call, who to wake	Mark essential personell, i.e. who to 'wake' Order of operations
		RS.CO-2: Events are reported consistent with established criteria			Model reporting of events Events are archimate elements, link to roles --> relationship between event and role
		RS.CO-3: Information is shared consistent with response plans			Sharing of information - relationship?
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	5 4,5	Senior stakeholder decisions needed Quick contact with CISO/Security Counsil	Group with 1
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness			Sharing source entity, same as identify and protect
		RS.AN-1: Notifications from detection systems are investigated	4 6	Response to detect & protect Measure and analyse vulnerability scans	Notifications = event --> technology event

RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.				
		RS.AN-2: The impact of the incident is understood	6	Measure and analyse vulnerability scans	Model of classification --> motivational assessment
		RS.AN-3: Forensics are performed	4,6	External incident response	Forensics services = assessment
		RS.AN-4: Incidents are categorized consistent with response plans	6 3	Measure and analyse vulnerability scans Related to CIA, don't kill traffic if A=5	Classification of impact --> motivational assessment
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	4 3 4 4	Isolate system Kill/block traffic Clean system Turn off system	Actions to be taken based on class/ --> action is strategy course of action?
		RS.MI-2: Incidents are mitigated			
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks			Vulnerabilities, mitigation, accepted risk --> already in identify
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	4	Continuous improvement	Out of scope
		RS.IM-2: Response strategies are updated			
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event			Out of scope
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	4	Lessons learned	Out of scope
		RC.IM-2: Recovery strategies are updated			Out of scope
	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.	**RC.CO-1:** Public relations are managed			Out of scope
		RC.CO-2: Reputation after an event is repaired	2	Damage to reputation	Out of scope
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams			Out of scope
		Out of scope	# #	Separate role	Out of scope