UNIVERSITY OF TURKU

ABSTRACT

	Bachelor's thesis
X	Master's thesis
	Licentiate's thesis
	Doctor's thesis

Subject	Information systems science	Date	27.11.2019
Author(s)	Johannes Kossila	Student number	77428
		Number of pages	67 p. + appendices
Title	A Light Enterprise Information Security Architecture Model for Creating and Improving Security Architecture		
Supervisor(s)	Prof. Reima Suomi Prof. Jukka Heikkilä		

Abstract

For decades companies have utilized enterprise architecture for improving enterprise level IT management in order to achieve competitive advantage. For this purpose, several enterprise architecture frameworks have been created to describe business processes and IT systems, their interrelations, and connections to different parts of the company. To complement the general enterprise architecture frameworks companies can also utilize dedicated information security architecture frameworks to ensure that information security is addressed as part of enterprise architecture. However, these security frameworks are typically complex and require significant effort and resources for successful implementation. This makes companies often hesitant to actively develop their security architecture which results in insufficient security management practices making the organizations more prone to common security threats.

This thesis studies improving enterprise information security architecture by utilizing the best practices of common security architecture frameworks and combining them into a light enterprise information security architecture model. The model is flexible, easy to use and highly compatible with various enterprise architecture frameworks. This thesis contributes to the previous information security architecture research significantly as it provides a cost-effective model for creating and improving information security architecture without a need for changing the overall enterprise architecture framework. The model can also be used as basis for future information security architecture research and development.

First, this thesis introduces the concepts of enterprise and information security architecture and presents some of the related frameworks. Then, it utilizes the best practices of these architecture frameworks to create a light enterprise information security architecture model. Finally, the proposed security architecture model is applied into an existing enterprise architecture environment and the results of implementation and the limitations of the model are discussed.

Key words	Enterprise architecture, information security architecture, TOGAF, SABSA
Further information	

TURUN YLIOPISTO

TIIVISTELMÄ

	Kandidaatintutkielma
X	Pro gradu -tutkielma
	Lisensiaatintutkielma
	Väitöskirja

Oppiaine	Tietojärjestelmätiede	Päivämäärä	27.11.2019
Tekijä(t)	Johannes Kossila	Matrikkelinumero	77428
		Sivumäärä	67 s. + liitteet
Otsikko	Kevyt yritystietoturva-arkkitehtuurimalli tietoturva-arkkitehtuurin luomiseksi ja kehittämiseksi		
Ohjaaja(t)	Prof. Reima Suomi Prof. Jukka Heikkilä		

Tiivistelmä

Yritykset ovat vuosikymmenten ajan hyödyntäneet yritysarkkitehtuuria parantaakseen sisäisten IT-järjestelmien kokonaisvaltaista hallintaa kilpailuedun saavuttamiseksi. Tähän tarkoitukseen on kehitetty useita yritysarkkitehtuurimalleja kuvantamaan liiketoimintaprosesseja ja IT-järjestelmiä, niiden liittymäkohtia ja yhteyksiä yrityksen eri osa-alueisiin. Yleisten yritysarkkitehtuurimallien lisäksi yritykset voivat hyödyntää myös erillisiä tietoturva-arkkitehtuurimalleja varmistaakseen tietoturvan sisällyttämisen osaksi yritysarkkitehtuuria. Tosin nämä tietoturva-arkkitehtuurimallit ovat tyypillisesti monimutkaisia ja niiden käyttöön ottaminen vaatii huomattavasti resursseja. Tämän vuoksi yritykset eivät halua aktiivisesti kehittää tietoturva-arkkitehtuuriaan, mikä tekee yrityksistä alttiimpia tietoturvauhille.

Tämä pro gradu -tutkielma käsittelee tietoturva-arkkitehtuurin parantamista kevyen tietoturva-arkkitehtuurimallin avulla, joka pohjautuu yleisesti käytössä olevien tietoturva-arkkitehtuurimallien käytäntöihin ja toimintamalleihin. Tutkielma luo uuden tietoturva-arkkitehtuurimallin, joka on helppokäyttöinen, mukautuva ja yhteensopiva useimpien yritysarkkitehtuurimallien kanssa. Tämän tutkielma löydökset tuovat merkittävää lisätietoa aikaisempiin tietoturva-arkkitehtuuritutkimuksiin, sillä se luo kustannustehokkaan mallin tietoturva-arkkitehtuurin kehittämiseksi niin, ettei koko yritysarkkitehtuurimallia tarvitsee muuttaa. Mallia voidaan hyödyntää myös tulevien tietoturva-arkkitehtuurimallien kehittämisen pohjana.

Pro gradu -tutkielma luo ensin tieteellisen pohjan aiheelle esittelemällä oleelliset yritysarkkitehtuuri- ja tietoturva-arkkitehtuurimallit ja niiden toimintaperiaatteet. Tämän jälkeen se luo näiden mallien ja toimintaperiaatteiden pohjalta uuden tietoturva-arkkitehtuurimallin ja esittelee sen toimintaperiaatteet. Lopulta tutkielma soveltaa uutta mallia olemassa olevaan yritysarkkitehtuuriympäristöön ja keskustelee soveltamisen tuloksista ja niiden yleistämisestä muihin yritysarkkitehtuurimalleihin.

Asiasanat	Yritysarkkitehtuuri, tietoturva-arkkitehtuuri, TOGAF, SABSA
Muita tietoja	

UNIVERSITY OF TURKU
Turku School of Economics

A LIGHT ENTERPRISE INFORMATION SECURITY ARCHITECTURE MODEL FOR CREATING AND IMPROVING SECURITY ARCHITECTURE

Master´s Thesis
in Global IT Management

Author:
Johannes Kossila

Supervisors:
Prof. Reima Suomi
Prof. Jukka Heikkilä

27.11.2019
Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

Table of contents

List of figures

1 INTRODUCTION

1.1 Background and motivation of the thesis

Modern companies are constantly searching for ways to achieve competitive advantages in the ever-changing market situation where competition is high, and customers are increasingly interested in quality and price (Ross et al. 2006). In order to answer to this demand, companies have utilized information technology (IT) already for decades to improve the internal processes and product quality, and to lower the related operative costs (Galliers & Leidner 2009). Therefore, IT driven internal efficiency has become a prerequisite for gaining competitive advantage in the markets for companies of all sizes (Ross et al. 2006).

However, at the same time insufficient and badly managed IT environments often cause problems and have a negative impact on internal efficiency. Companies often purchase new IT systems for narrow-scoped purposes in pursuit of utilizing new emerging technologies without considering the holistic approach for IT system management (Galliers & Leidner 2009). IT systems are purchased gradually over a long period of time and hence old legacy systems often exist within the same IT environment as the new modern systems (PWC 2018). Older IT systems are also often left without proper maintenance and update which causes them to be incompatible with the newer systems (PWC 2018). Such diverse IT environments often face problems during the onboarding of new systems and decommissioning of old ones. This results in increased costs and delivery time which causes a loss of internal efficiency and competitive advantage (Galliers & Leidner 2009).

Enterprise architecture (EA) is a methodology which aims to solve challenges of enterprise level IT management. EA presents a high-level holistic view of company's business processes and IT systems, their interrelations, and connections to different parts of company (McGovern et al. 2003). The goal of EA is to describe the present state of company's business processes and IT systems, define a future target state for these processes and systems, and aid in creating a roadmap between these two states (McGovern et al. 2003). EA also aims to help in building basic principles for IT solution thus harmonizing and standardizing the variety of IT systems within a company (Ross et al. 2006).

Since enterprise architecture is a holistic approach for managing and developing company IT and business processes, it is also natural to manage information security as part of EA when aiming to gain a holistic overview of company security posture. In order to complement traditional EA frameworks, there are several dedicated enterprise information security architecture (EISA) frameworks available which focus on managing

and developing information security processes as part of enterprise architecture (Tahajod et al. 2009). However, these frameworks are often complex and require significant effort and resources for successful implementation (Sherwood et al 2005; Safari et al. 2016). The difficulty and high costs of implementation make organizations often hesitant to actively develop their information security architecture which results in insufficient security management practices making the organizations more prone to security threats such as data leaks and hacking (Safari et al. 2016).

In order to solve the challenges of current EISA models and to provide organizations an effective method for creating and improving their security posture, this thesis presents a light enterprise information security architecture (LEISA) model which is compatible with various enterprise architecture models following the common industry standards. The model is based on best practices of several enterprise and security architecture frameworks such as TOGAF, SABSA and Open Security Architecture. The proposed security architecture model provides a flexible and easy to use methodology which can be applied to different architectural environments and tailored as needed. Organizations can utilize the model as such for creating a completely new security architecture or they can use the model as reference architecture by implementing only the components they need to fulfill their specific requirements for security architecture.

The thesis is structured in a way that this chapter presents the background and motivation of the thesis and discusses the utilized research methodology. Chapters 2 and 3 lay out the theoretical foundations for the thesis by introducing the concepts of enterprise and security architecture and by presenting some of the common frameworks associated with these architecture types. In chapter 4 the best practices of enterprise and security architecture frameworks are utilized to create a light enterprise information security architecture model. Finally, in chapter 5 the proposed security architecture model is applied into an existing enterprise architecture environment and the results of implementation and the limitations of the model are discussed.

1.2 Research methodology

1.2.1 Research scope and ethics

The needs and scope for this thesis have been defined by the target company introduced in chapter 5. This company has a need for improved enterprise information security architecture and has not been able to find a suitable solution from the current existing common EISA models. Therefore, the overall scope of this thesis is impacted by the requirements set by the target company. The impact on the scope is mostly limited to the

implementation phase of the suggested LEISA model as the company has defined the scope in which the model is applied within their own organization. The limitations of the implementation scope within the target organization are discussed more in chapter 5.

In addition to having an impact on the implementation scope of this study, applying the LEISA model in an actual organizational context also sets requirements for research ethics. Disclosing company confidential information related to information security of a globally working company can have serious impact on the company's stock price or overall security of the operative processes (PWC 2018). Therefore, there are for example some company internal documents that cannot be shared in detail but are used as basis for the LEISA implementation in this study. In accordance some of the research data produced as part of the implementation cannot be shared either. Such documents and data are briefly covered when necessary in chapter 5.

1.2.2 Selected research methods

There are several different research methods available for conducting research. From these methods the most common include quantitative and qualitative research methods. Quantitative research focuses on creating and testing hypotheses by utilizing data sources and quantifying them in order to find connections between the studied variables (Creswell 2003). Quantitative research can be considered as top-to-bottom approach where the hypotheses are first created and then the collected data is analyzed to confirm the hypotheses (Trochim et al. 2016). This method aims to generalize findings of a small group into bigger context (Creswell 2003).

In qualitative research the focus is on making observations from the events and data that is available for the researches (Creswell 2003). In this approach the hypotheses and theories are created based on these made observations. As opposite of quantitative research, qualitative research is a bottom-to-top approach where research starts from finding patterns from the existing data and then proceeding towards understanding if hypotheses and theories can be created from these patterns (Trochim et al. 2016).

In addition to using one of the options above, it is also possible to utilize a mixed research method which combines the data gathering and analysis methods from both quantitative and qualitative research (Creswell 2003). As mixed researched is not limited to certain research methods it can provide a more holistic approach for gathering and analyzing research data (Trochim et al. 2016). However, mixed research method is considered to also have some weaknesses since it often requires more resources than using only a dedicated method and conducting the research may be more complex than with the other two methods (Trochim et al. 2016).

As this thesis aims to create a new and improved enterprise information security architecture model, it is not straightforward to utilize the traditional research methods discussed above. The traditional research methods aim to analyze a set of data typically generated via targeted and customized questionnaires (Trochim et al. 2016). Therefore, they do not as such fit the needs of this thesis since it is not possible to gather targeted data in the limited scope of the study as required by these traditional research methods. However, it is possible to utilize some of the practices associated with these methods. For example, qualitative research methods can be utilized for observing the findings of different enterprise and information security architecture literature. Based on these observations it is possible to form a security architecture model containing security elements from common EISAs.

In accordance, there are also some elements in this thesis which are similar to quantitative research. These elements are mainly present in the fifth chapter of the thesis where the proposed model is applied in the context of target company. Here, the thesis aims to prove that the model can be used to simplify and create a security architecture. Although there is no quantitative data analysis done as part of the implementation, the thesis aims to generalize the findings to be applicable also outside of the target company. This resembles the research methods of quantitative research despite that no actual data analysis is done in the scope of the thesis.

Based on the above discussion, the research methodology chosen for this thesis is mixed methods. Although the thesis does not apply the traditional research methods in their typical manner it still utilizes elements from both methods. Therefore, by selecting the best practices of both methods the most appropriate approach for conducting the study in the predefined scope can be found.

1.2.3 Data collection

As discussed above, this thesis aims to create a flexible and easy to use model based on the best practices of the common enterprise and information security architecture frameworks. Questionnaires and data samples associated with the traditional research methods are not usable in the scope of this study as such. They could be utilized in a study focusing on the usability of the proposed security architecture model in future research covering more companies but for the selected target company it is not possible to collect data with such methods.

For collecting data about best practices and elements of the current enterprise and security architecture frameworks a literature review is the best option available. Therefore, this thesis utilizes a literature review of the most relevant enterprise and architecture frameworks in order to collect data for creating the proposed security

architecture model. The literature review of the selected frameworks focuses on the content of the frameworks described in the relevant literature rather than focusing on the output of the articles. The literature view produces an understanding of common elements of EA and EISA which will then be used as basis for creation of a new model by utilizing elements of qualitative research.

It has to be noted that there is a minor challenge in performing a full literature review of common enterprise and information security architecture frameworks. Many of the frameworks are produced for commercial use and therefore parts of their full content may be unavailable for the purpose of this research. However, in such situations the literature review uses complementing material and resources to describe the content in necessary detail. Hence, the literature review achieves suitable level of detail for the needs of this thesis.

2 ENTERPRISE ARCHITECTURE

2.1 Purpose of enterprise architecture

As mentioned in the previous chapter, enterprise architecture is a methodology which is used to solve challenges of enterprise level IT management. EA presents an overview of the connections between business processes and IT systems in order to understand the present state and plan the future target state for these processes and systems (McGovern et al. 2003). EA also aims to harmonize and standardize the variety of IT systems within a company (Ross et al. 2006).

Enterprise architecture is a vast concept which touches all organizational levels starting from high-level IT and business strategy creation and ending in very focused IT system and component architecting (Tamm et al. 2011). EA translates the broader goals defined in business and IT strategy into principles which are implemented in systems and processes that enable reaching the strategic goals. In fact, enterprise architecture planning resembles strategic planning since both provide a long-term and organizational-wide vision of future for business processes and IT systems. However, EA describes this vision in much more detail making it a support tool for implementing the strategy (Tamm et al. 2011).

Due to its position between IT and business, enterprise architecture has a key role in bridging the gap between these two. It is common that companies make business and IT decisions separately which often results in bad technology choices and arising conflicts between business and IT decision makers (Iacob et al. 2014). Business representatives often think that IT cannot provide solutions that support their needs while IT employees believe that business is not capable of describing their needs with enough detail (Galliers & Leidner 2009).

In order to close the gap between business and IT, business modelling can be utilized as part of EA planning. In business modelling, the planned IT change or project is first analyzed from the perspective of how it will support and affect business processes. This process includes assessing the purpose of the change, its impact on the current business processes and architecture environment, and requirements for completing the change (Iacob et al. 2014). With the help of business modelling companies are able to analyze how changes affect their IT and business environment, assess costs related to changes, and make decisions of implementing changes (Iacob et al. 2014).

2.2 Structure of enterprise architecture

2.2.1 Common processes related to enterprise architecture creation and governance

Since companies implement and adjust their enterprise architecture based on their specific organizational and industry needs, the amount of different architecture models is huge. Even the most common enterprise architecture frameworks vary a lot in their structure, processes, method of implementation and preferred tools. Still, there are certain common processes and structures associated with most EA models.

Defining an enterprise architecture within a company typically starts by analyzing the business and IT strategies (Pavlak 2006). These strategies should define the goals and vision for developing the EA. Based on these goals and vision, the company defines a set of target architectural principles and starts looking into existing EA models and best practices that would be able to fulfill the set principles.

In order to understand the specific organizational needs and find suitable EA models, the company must understand the current state of their enterprise architecture. This current state is often referred as as-is architecture (Pavlak 2006). After understanding the current architecture setup, companies often create several models and analyze them to find the most suitable EA model to fulfil the needs of business and IT. After several iterations, the company chooses an EA model and best practices which define and guide the future target EA vision for the company. The future target EA model is commonly known as to-be architecture (Pavlak 2006).

As a part of analyzing the EA models and best practices, companies also often prepare a roadmap for reaching the to-be architecture (Pavlak 2006). This roadmap acts as a transition plan between the as-is and to-be architectures containing the business process and system changes required to reach the EA goals. Roadmaps are considered to be a critical part of the target EA model by making it more concrete and setting practical guidelines for EA implementation (Pavlak 2006).

In order for enterprise architecture to work efficiently it must evolve as integrated part of the business. If the architecture does not constantly adapt to changes in the business needs and IT environment, it will eventually become outdated and cannot be used to plan and implement the company's strategy. The evolution of EA is iterative as it should develop as part of every IT initiative and project that is carried out according to the current enterprise architecture (Heikkilä et al. 2010). All initiatives and projects should provide feedback to the current architecture model and enable continuous improvement of the EA. Therefore, developing an enterprise architecture is not a comprehensive one-time project but a continuous iterative process.

Performing regular business modelling and business strategy review also enable the continuous development of EA. Business modelling and strategy both set demands for the current EA and challenge it to make new business requirements possible (Heikkilä et al. 2010; Iacob et al. 2014). In accordance, EA also impacts business strategy by helping in setting strategic priorities and by giving insight about new strategic opportunities enabled by technical solutions (Ross et al. 2006).

Efficient and developing enterprise architecture also needs a strong governance model. Lack of governance in EA often results in unrealistic IT projects, lack of coordination between actors, and inadequate setting of business and IT goals (Heikkilä et al. 2010). Governance in enterprise architecture enables compliance of IT projects with the company EA framework, ensures quality assurance, and improves communications between business and IT (Liimatainen et al. 2007). Also, continuous evolution of EA is not possible without governance since change management and coordination between business and IT is essential for EA evolution to succeed (Liimatainen et al. 2007).

Successful governance can be achieved if the purpose and goals in each development initiative are clear, most appropriate implementation methods are chosen, and if active stakeholder management is done (Heikkilä et al. 2010). Typical governance practices include monitoring compliancy, auditing projects, setting roles and responsibilities, and continuously assessing the current use and future needs for IT (Heikkilä et al. 2010).

2.2.2 Common elements of enterprise architecture

As discussed above, enterprise architecture development usually starts with the planning process in which the company investigates and defines the current state of EA and then sets goals for the future target architecture. The direct outputs of this process form one of the key elements commonly shared by most EA models. This element is the EA representation (Tamm et al. 2011). The EA representation composes of stakeholder views and viewpoints of the enterprise architecture components and is supported by several EA artifacts such as roadmaps, architecture diagrams, and other documentation supporting the implementation of the EA (Heikkilä et al. 2010).

The EA stakeholder viewpoints describe the overall architecture representation in different abstraction levels from a specific stakeholder perspective combining the related EA views into more holistic overview (Urbaczewski & Mrdalj 2006). These stakeholder viewpoints are used by different organizational levels to understand each other (Urbaczewski & Mrdalj 2006). For example, business decision makers have a different need for detail about the overall enterprise architecture than IT system owners. By utilizing their respective stakeholder viewpoints these two groups are able to communicate more easily with each other (Pavlak 2006).

In typical EA representation, the stakeholder viewpoints start from a high-level description with wide scope and shift towards more detailed descriptions when moving down the organizational levels (U.S. Government Accountability Office 2001). The stakeholder viewpoints have some variance between different EA models, but they usually follow a similar pattern. Typical viewpoints describe EA from business or strategic, owner, designer, and operative perspectives (Urbaczewski & Mrdalj 2006; U.S. Government Accountability Office 2001).

Since there are different stakeholder views and viewpoints covering a variety of systems and processes, creating a single holistic description of the overall IT and business environments can be difficult. Therefore, enterprise architecture is often described in a partial representation hiding other irrelevant interconnected systems and descriptions (U.S. Government Accountability Office 2001). These partial representations form another common element of EA and are known as architecture domains.

Unlike architecture viewpoints, domain descriptions can address concerns of several different stakeholders with one representation (U.S. Government Accountability Office 2001). EA domains often represent an architectural interest such as business or technology infrastructure. For example, business architecture could cover business functions, processes, roles and actors, and capabilities related to certain business system or environment. In accordance, application architecture could cover structure and behavior of all IT applications related to a certain business function or organization.

The main benefit of using EA domains is that they provide a holistic but focused description of certain architecture area covering several architectural components and viewpoints thus enabling better communication between stakeholders within a certain area (U.S. Government Accountability Office 2001). The typical architecture domains covered by majority EA frameworks include business, data, application, and technology domains (Urbaczewski & Mrdalj 2006; U.S. Government Accountability Office 2001). In addition to these, many frameworks have also chosen to describe other architecture domains depending on their purpose of use. Such domains may include for example software, or security domains (Sherwood et al. 2005).

2.2.3 Benefits and challenges of enterprise architecture

As discussed above, one of the main benefits of enterprise architecture is the improvement of internal efficiency and company performance by solving challenges of enterprise level IT management (McGovern et al. 2003). This is achieved by optimizing several organizational processes and increasing communications between different stakeholders. One of the goals of EA is to provide a common framework for IT and business which can be used to improve communications and decision making between IT and business. In

order to identify interdependencies and understand stakeholder requirements, companies are forced into cross-organizational collaboration which brings different organizational units closer to each other (Tamm et al. 2011). Therefore, EA improves organizational alignment within companies. This helps avoiding conflicts and often hastens decision making and as such also improves the performance of the company.

Enterprise architecture also promotes the availability of information by presenting it in more understandable format via architecture diagrams and other EA artifacts. Since the purpose of EA includes harmonizing the variety of IT systems and enabling better integrations, information flow between systems is also improved as part of EA implementation (Ross et al. 2006). In addition, enterprise architecture helps organizations in resource optimization (Tamm et al. 2011). By analyzing the current state of internal processes and IT, companies can identify overlapping resources, lower their support and maintenance costs, and find enterprise-wide synergies (Tamm et al. 2011).

It has to be noted that when discussing the benefits of EA, all companies are not able to utilize all the advantages of EA implementation. It is common for larger organizations with complex IT environments to experience more EA benefits than the organizations with smaller and simple IT environments (Tamm et al. 2011). This is because organizations with complex IT environments typically have more room for resource optimization, organizational alignment, and finding synergies in internal IT and business operations.

There are also some challenges with enterprise architecture. One key challenge is that many enterprise architecture frameworks are difficult to understand and implement (Safari et al. 2016; BCS 2016). Organizations lack the necessary skills to implement common EA frameworks, or the frameworks and related support materials are too complex for the intended use. EA initiatives are also often quite time consuming and require lot of governance and resources. This requires long-term top management engagement, support, and budget which many companies often lack (BCS 2016).

Implementing EA also requires some maturity and significant planning effort from the organization itself and therefore hastily made decisions or low maturity are probable to cause problems during the implementation process or result in ineffective EA models (Kaisler et al 2005). The extensive architectural representations and toolsets are also somewhat difficult to maintain (Kaisler et al 2005). Since enterprise architecture is not static but keeps on evolving organizations need to be continuously reviewing and updating their EA representations.

Yet another common EA challenge is the measurement and evaluation of the realized benefits of EA (Lehong et al. 2013). Some benefits of EA might not be perceived equally valuable by different stakeholders as other benefits. This might cause disruptions in stakeholder relationships and result in prioritization challenges during the implementation process (Lehong et al. 2013). It is also difficult to quantify for example the benefits gained

from organizational alignment. Without showing clear quantified results of the EA implementation for stakeholders it might be difficult to get the proper approval and support required for successful implementation.

Finally, implementing EA changes can cause disruptions to business and IT processes (Safari et al. 2016). EA implementation includes almost always introducing new technologies and processes to the company which will have an impact on the current operative IT and business processes. If the related process and technology changes are not planned carefully, they can cause dissatisfaction among stakeholders or even loss of income to the company (Safari et al. 2016).

The next subchapters will shortly present and discuss some of the widely used enterprise architecture frameworks. It has to be noted that a commonly shared understanding among enterprise architects is that there does not exist a single best EA framework suitable for all organizations (BCS 2016). All EA frameworks have their own advantages and disadvantages and organizations might have specific EA needs that are not addressed by these frameworks (BCS 2016). The best implementation results are often achieved when companies utilize best practices from several frameworks that are suitable for their own specific needs (BCS 2016).

2.3 Enterprise architecture frameworks

2.3.1 Selecting the relevant enterprise architecture frameworks

As discussed earlier in this thesis, there are several different enterprise architecture frameworks available for creating and managing enterprise architecture. Organizations work differently in different industry sectors and hence have different needs for enterprise architecture (BCS 2016). Therefore, it is necessary to limit the EA frameworks discussed in the scope of this thesis only to the most relevant frameworks.

The enterprise architecture frameworks selected to this study have all been widely adapted and actively developed for over a decade (Urbaczewski & Mrdalj 2006; Architecture-Center 2019; Avolution 2019). Due to their extensive history and wide acceptance these frameworks are often referred to as industry standards when discussing about enterprise architecture (Architecture-Center 2019; Avolution 2019). Also, many modern and newer EA frameworks are based on these frameworks (Architecture-Center 2019).

In addition to the frameworks discussed below, there are also few other frameworks which are often addressed along the selected frameworks. However, these frameworks are either specific to certain industries or have been developed with some specific narrow

purpose. Therefore, these frameworks are not relevant for the scope of this thesis and are left out of discussion.

2.3.2 The Zachman framework

The Zachman enterprise architecture framework (1987) was one of the first frameworks to introduce the concept of enterprise architecture to a wider audience. The Zachman framework presents a fundamental structure for EA in order to provide different perspectives to view a company, its information systems, and their interrelations (Sowa & Zachman 1992). Zachman believes that a set of architecture representations describing different stakeholder perspectives should be always created during information system development (Ylimäki & Halttunen 2005). He also believes that the same system can be described in different ways to fulfill different purposes (Ylimäki & Halttunen 2005).

Zachman framework organizes different perspectives of information systems into a conceptual matrix. The 6 x 6 matrix consists of 36 cells each focusing on a specific dimension or perspective of system development. The matrix columns represent different stakeholder abstraction views involved in system development and in each view a unique representation of the system is created (Ylimäki & Halttunen 2005). The six views are based on English language interrogatives such as what, where, and how (Zachman International Inc. 2008). These views represent abstractions of different systems and the related components such as data, network, people, and time. The matrix rows consist of descriptions of different stakeholder perspectives of system development (Ylimäki & Halttunen 2005). These perspectives include for example executive, business management, and architect perspectives (Zachman International Inc. 2008). The rows can also be represented as EA perspectives such as scope, business concepts, system logic, and technology (Zachman International Inc. 2008).

A single cell of Zachman framework contains all models and descriptions of EA from the specific stakeholder perspective on certain level of abstraction. Each cell must also be aligned with the immediately above and below cells, and all cells in a row must be aligned with each other (Sowa & Zachman 1992). The collection of all cells within a row gives a holistic presentation of the EA from certain stakeholder perspective. In accordance, collection of all cells within a column gives a similar presentation on certain view. A high-level overview of the Zachman architecture framework is described in figure 1.

Despites its name, Zachman framework is not a fully working framework as such. It is a conceptual framework for defining EA perspectives and views. However, it does not present any methodology or instructions for EA implementation, development, or evolution within a company (Zachman International Inc. 2008). The main use of the framework in practice is to use it as a tool for organizing EA documentation and other

EA methodologies for creating representations of system development as per different Zachman views (Ylimäki & Halttunen 2005). Therefore, typical approaches for applying the Zachman framework include applying it only partially as a complementing framework, or utilizing it as a starting point for overall EA development (Ylimäki & Halttunen 2005).

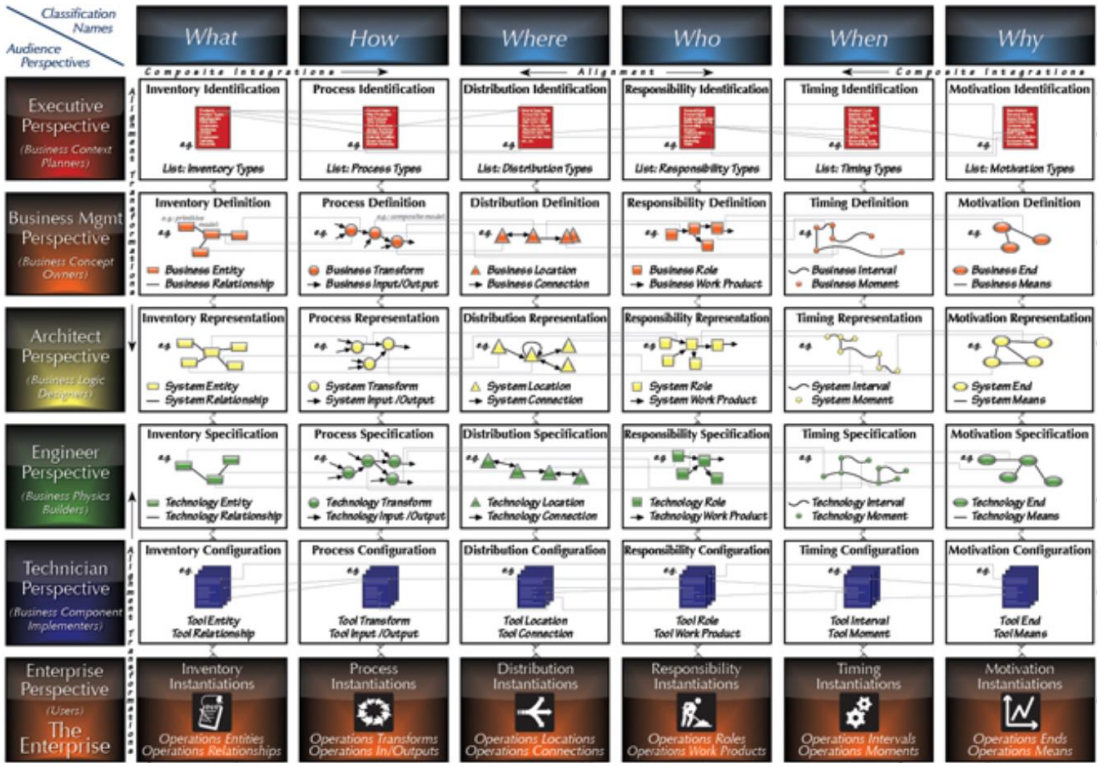

Figure 1 A high-level overview of the Zachman framework (adopted from Zachman International Inc. 2008)

2.3.3 The Open Group Architecture Framework

The Open Group Architecture Framework or TOGAF is a widely adapted enterprise architecture standard which provides comprehensive frameworks, methodologies, and guidelines for EA implementation (The Open Group 2018). TOGAF offers vast documentation library and practical instructions which support specific needs of different types of organizations. The framework also covers EA topics supplementing traditional EA domains such as business value streams and information security (The Open Group 2018). TOGAF is designed to be compatible with other EA standards and methodologies (The Open Group 2018).

TOGAF describes EA in four main architecture domains. These domains are business, data, application, and technology architectures (The Open Group 2017). Architecture representations of the four EA domains are created and developed by using the two main

components of TOGAF. These components are the architecture development model (ADM) and content architecture framework.

ADM provides a process for developing architectures. The process includes establishing an architecture framework, developing the content of architecture, transitioning between architectures, and governing the created architectures (The Open Group 2018). All the ADM activities are carried out within an iterative cycle including continuous architecture refining and implementation enabling companies to response to constantly changing business and IT needs. ADM consists of ten different phases which all produce number of EA artifacts such as project plans, process flows, and architectural requirements (The Open Group 2018).

The content architecture framework provides a structural model for architecture content created as part of ADM (The Open Group 2017). It allows major EA artifacts to be consistently defined, structured, and presented while ensuring the quality of the work products. The content architecture framework enables using it as a stand-alone framework irrelevant of the possible other EA frameworks used in the same EA environment. TOGAF also enables replacing the content architecture framework with other EA frameworks without losing the compatibility with ADM and other TOGAF components (The Open Group 2017).

A key component of the content architecture framework is the content metamodel. The content metamodel provides a description of all different building blocks that may exist within an architecture setup (The Open Group 2017). The metamodel also describes the relationship between the building blocks. The content metamodel consists of the core metamodel and possible extensions. The metamodel core is used to provide a minimum set of architectural content to understand the overall architecture and relation between building blocks (The Open Group 2018). The metamodel extensions can be used to describe more in-depth modelling of a certain area of interest, such as governance processes or data modelling (The Open Group 2017).

The content metamodel utilizes entities to describe different building blocks and their relation within EA. Such entities include for example actors, roles, application components, functions, and organizational units (The Open Group 2017). As with other architectural representations, the content metamodel can also be described in different abstraction levels and stakeholder perspectives. A high-level description of overall content architecture framework can be seen in figure 2.

In addition to the main components discussed above, there are also other components within TOGAF. These components include for example the architecture capability framework and the enterprise continuum. The architecture capability framework provides templates and guidelines for creating appropriate organizational structures, roles, and processes to realize efficient enterprise architecture models (The Open Group 2018). The enterprise continuum aims to explain how generic TOGAF solutions can be leveraged

and specialized to support individual companies (The Open Group 2018). These two components are intended to mainly provide support for the architecture implementation and are not a mandatory part of architecture development.

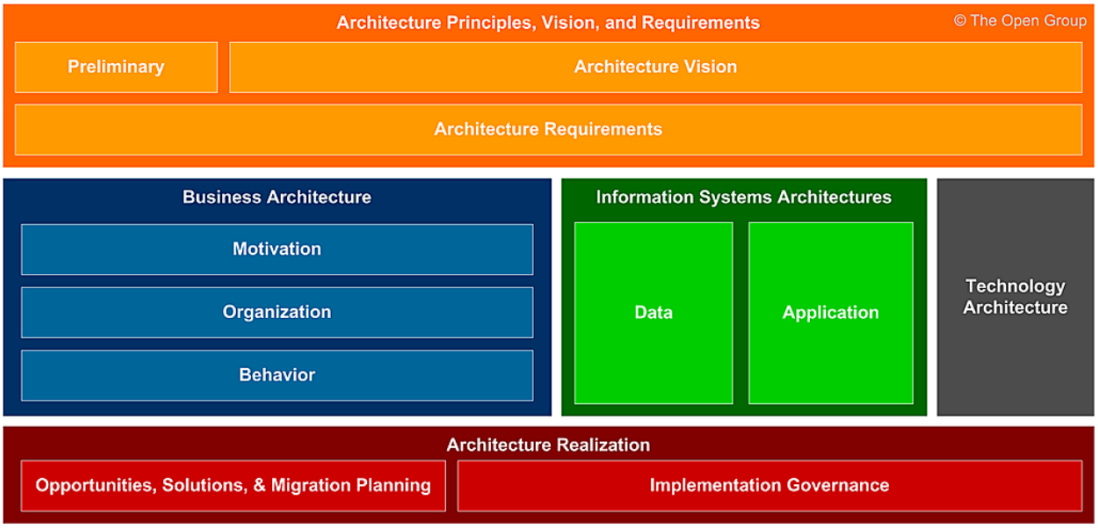

Figure 2 A high-level overview of the content architecture framework (adopted from The Open Group 2017)

2.3.4 Federal Enterprise Architecture Framework

Federal Enterprise Architecture Framework (FEAF) created by the Federal CIO Council in United States is a tool for managing the creation, use, and development of enterprise architecture for governmental authorities (The U.S Federal CIO Council 2013). FEAF provides reference architecture models for coordinating common business and IT processes, information exchange, and IT investments shared between governmental agencies (The U.S Federal CIO Council 2013).

FEAF is part of comprehensive collection of enterprise architecture best practices and processes created to ensure the implementation of EA in US governmental agencies. This collection is called the Common Approach to Federal Enterprise Architecture (CA) (The U.S Federal CIO Council 2012). CA defines the underlying EA practices that US governmental agencies should follow when organizing their IT and business processes. The common approach provides processes, guidelines, and tools related to EA scope, development, and governance. FEAF is designed to comply and follow the principles set in CA. The main focus of FEAF is to provide reference architecture models that agencies can use as part of CA implementation. When implemented successfully, CA and FEAF promise to improve service delivery quality, functional integration, and resource optimization (The U.S Federal CIO Council 2013).

The core of FEAF is the Consolidated Reference Model (CRM) which provides a common language and framework for describing and analyzing governmental IT processes (The U.S Federal CIO Council 2013). The CRM consists of a set of interrelated reference models which describe the six architectural domains in the scope of FEAF. These domains are strategy, business, data, applications, infrastructure, and security architecture (The U.S Federal CIO Council 2013). The reference models of CRM aim to describe the important elements of business and IT operations within governmental agencies in respect to each these domains.

As with TOGAF, FEAF also includes an EA development method defined in CA. This process is called the Collaborative Planning Methodology (CPM). CPM consists of two phases which are organize and plan, and implement and measure (The U.S Federal CIO Council 2012). The CPM development process works iteratively. The EA plans and deliverables are reviewed during the two phases and if improvement needs are found the whole process should be repeated until the architecture reaches sufficient maturity (The U.S Federal CIO Council 2012).

As with many other EA frameworks, also CA suggests that the overall EA development should start from defining the current and future states of EA (The U.S Federal CIO Council 2012). The transition between the current and future states is carried out iteratively by following the phases of CPM. The transition plan can utilize FEAF's own consolidated reference model or agencies can use separate architecture reference models to help in EA development (The U.S Federal CIO Council 2012).

In the next chapter, information security is discussed in the context of enterprise architecture. The chapter first presents the concept of information security in general and then proceeds to discuss how security is addressed in the enterprise architecture frameworks introduced in this chapter. The chapter also discusses some widely used enterprise architecture frameworks dedicated solely for addressing information security.

3 MANAGING INFORMATION SECURITY AS PART OF ENTERPRISE ARCHITECTURE

3.1 The concept of information security

Information security is an increasingly complex concept expanding throughout multiple fields of study. It covers a variety of topics such as technology, human behavior, management, and business processes. Information security can be defined as protection of information and the systems, people, physical environments, and processes which use, store, or transmit that information (Solms & Niekerk 2013).

Traditionally in information security the information is protected by ensuring its confidentiality, integrity, and availability. The protection of this "CIA triad" is considered to be the security industry standard which is used as basis for the definition of threats and corresponding protective measures for information (Solms & Niekerk 2013).

Holistic information security management generally relies on both processes and technical controls rather than purely focusing on technical solutions. Information security management should also be addressed in all organizational processes and behavior in order to ensure effective protection of company assets (Peltier 2016). This enables security controls to be adjusted to the specific needs of different organizational units and further improves the effectiveness of security management (Peltier 2016).

In recent years, cybercrimes have become an increasing threat for modern business. This has forced companies in all industry sectors to improve their overall information security practices and make investments in their information security capabilities (PWC 2018). In addition, recent governmental legislation also puts pressure on companies for maintaining the confidentiality of customer personal data (PWC 2018). This sets new requirements for the internal IT systems and processes from the security perspective. Therefore, companies need a holistic approach for planning and managing information security as integrated part of their daily business operations.

Since enterprise architecture is a holistic approach for managing and developing company IT and business processes, it is also natural to manage information security as part of EA when aiming for gaining a holistic overview of company security posture. Enterprise architecture focusing on management and improvement of information security is generally known as enterprise information security architecture (Tahajod et al. 2009).

3.2 Enterprise information security architecture

The main goal of enterprise information security architecture is to ensure the integration of different security elements, such as security networks, systems, applications, and processes into company overall IT and business processes (Tahajod et al. 2009). EISA is a comprehensive security design which sets requirements for security controls that need to be in place for different systems and environments (Tahajod et al. 2009). These controls include for example authentication, authorization, vulnerability management, and end-point protection (Tahajod et al. 2009; Bel et al. 2009).

As with enterprise architecture, effective security architecture should also be based on the business and IT strategies of the company. Therefore, all security decisions done in the EISA should originate from specific business needs and also be traceable back to these needs (Oda & Zhu 2009). This is extremely important with both enterprise and security architecture since they do not often provide quantifiable business benefits but rather have a direct increase of costs for organizations (Bel et al. 2009). Traceability ensures that EISA has formal justification within the company and organizations aim for the cost-effectiveness of security control implementation (Tahajod et al. 2009; Oda & Zhu 2009).

The scope of EISA is not often predefined as it depends on the target systems and organizations (Bel et al. 2009). Different systems and organizations have different requirements for confidentiality, integrity, and availability, and hence there may be security controls which are not applicable for the predefined scope. Therefore, risk analysis is a critical part of defining the security controls and security architecture (Tahajod et al. 2009). The organizational risks are often determined by company business model, related systems and their corresponsive threats, and industry legislation (Bel et al. 2009). In order for the company to define proper level of security for different risks a security baseline is required. This baseline is often described in the company information security policy which includes requirements for protection of different kinds of information and assets (Tahajod et al. 2009).

Information security policy provides general security rules that can be applied to different systems and processes. This makes security architecture the underlying set of coherent principles aiming to guide the implementation of company information security policy (Tahajod et al. 2009; Bel et al. 2009). In accordance, the company information security policy should be based on the company strategy in order to support and fulfill the needs of business (Tahajod et al. 2009).

Enterprise information security architecture can be described either as a separate architecture representation or as an integrated part of the other enterprise architecture representations (Bel et al. 2009). In accordance, security controls can also be represented as part of the security domain or as part of other EA domains since these controls often relate to other architecture domains such as application or infrastructure domains.

However, from the perspective of usability and simplicity many EA and EISA frameworks choose to describe security as a dedicated domain since this enables gathering all security related controls into one holistic representation (Tahajod et al. 2009; Oda & Zhu 2009). In most representations which use a dedicated security domain this domain is often presented as cross-cutting with the other architecture domains (The Open Group 2016; The U.S Federal CIO Council 2012).

As with general EA, EISA also utilizes different stakeholder viewpoints. These viewpoints also vary in detail to suit the needs of specific stakeholder groups ranging from the higher strategic level to the lower operative level (Oda & Zhu 2009). When considering development of overall EA, security architecture is not typically the primary architecture domain from which companies start their architecture development. It often follows the development of other architecture domains adapting to the ongoing changes and enabling the decisions made in business and IT strategies (Bel et al. 2009).

Security architecture has most of the same benefits for organizations as traditional enterprise architecture. These benefits include for example ensuring a unified way of arranging security throughout the organization and cost-reduction via reduced delivery times and resource optimization (Bel et al. 2009). As with traditional EA, different stakeholders have different security requirements and therefore EISA also provides a common terminology and serves as a basis for stakeholder communication (PWC 2018; Bel et al. 2009).

From information security perspective, EISA improves company overall security posture by integrating security processes into other business and IT processes (Tahajod et al. 2009). EISA also enables security process standardization, evaluation of security practices, business and security alignment, change management improvement, and realization of the company security policy into systems and processes (Sherwood et al. 2009).

As with the implementation of traditional EA, companies with large and complex IT environments benefit the most from the implementation of EISA. This is because such companies tend to have more overlapping security systems and processes in place thus gaining more benefits from resource and process optimization (Bel et al. 2009).

As with the general enterprise architecture, there are also challenges in enterprise information security architecture. The challenges in both architecture types are mostly very similar but rather than having a primary effect on company internal efficiency problems in security architecture can have more diverse impact to the company.

Enterprise information security architecture frameworks tend to be complex and require significant effort and resources for successful implementation (Sherwood et al. 2005). This difficulty and high costs of implementation make organizations often hesitant to actively develop their information security architecture which results in insufficient security management practices making the organizations more prone to security threats

such as data leaks and hacking (Safari et al. 2016). Therefore, rather than losing only efficiency, the company can lose other valuable assets such as intellectual property, reputation, or money (Peltier 2016).

In accordance, uncontrolled implementation of security architecture can cause disruptions in business and IT processes. However, uncontrolled implementation can also cause disruptions in the existing security controls which again may leave company open for new security threats (Safari et al. 2016). This causes problems in security architecture have more severe and direct impact for the company than problems in traditional enterprise architecture.

Although information security is not typically addressed in much detail in regular enterprise architecture frameworks, there are general EA frameworks which also consider security as part of their architecture domains. Some frameworks also have security extensions available which introduce security into the overall framework. The below subchapters discuss how security is addressed in the enterprise architecture frameworks described in chapter 2.

3.3 Information security in enterprise architecture frameworks

3.3.1 Security in the Zachman framework

As discussed earlier, the Zachman framework is a conceptual framework which only presents viewpoints and abstractions from EA. The framework does not contain any methodology, tools, or reference models for actual EA implementation and therefore as such the framework does not contain any references for security architecture. However, there are several EISA frameworks which have been developed from the basis of Zachman framework. Such frameworks include for example Henning's (1996), DeLooze's (2001), and Heaney's (Heaney et al. 2003) frameworks. These frameworks mostly focus on applying different stakeholder perspectives of Zachman framework in the context of security.

Henning and DeLooze have chosen a very similar approach for applying Zachman framework into security. Both frameworks start by creating a security policy in the highest stakeholder perspective of Zachman framework and continue by narrowing down the scope of security requirements and applying them on operative work in lower levels of the framework (Henning 1996; DeLooze 2001).

Henning and DeLooze both also believe that the most significant stakeholder perspectives for defining and applying security requirements are the top three perspectives of the framework. These perspectives are the executive, business

management, and architect perspectives (Henning 1996; DeLooze 2001). In the executive stakeholder perspective, company should focus on defining rules for data classification and processing. This general set of principles should then act as a security policy guiding the lower level security implementation (Henning 1996; DeLooze 2001). In the business management perspective, the data owners should now be able to assess the security requirements of their data based on the principals set in the executive perspective.

DeLooze proposes here that data should be assessed and grouped by internal and external accessibility (DeLooze 2001). Based on this assessment for example firewall and routing rules could be created. Henning proposes a more detailed approach in which the system processing the data will be assessed as whole. The system should be assessed regarding data input and output, mechanisms of data manipulation and processing, and controls which are in place to protect data access (Henning 1996). This assessment enables defining detailed requirements for the system security. Both frameworks agree that after the initial requirements have been set, the implementation will continue in the lower levels of Zachman framework (Henning 1996; DeLooze 2001).

Heaney et al. propose integrating information assurance into Zachman framework. They believe information assurance elements do not exist in isolation and hence these elements must be integrated into all EA elements (Heaney et al. 2003). Heaney et al. suggest that instead of considering assurance only at system development level, it should be considered in all levels of enterprise architecture (Heaney et al. 2003). Therefore, they introduce a new information assurance column as an additional abstraction view to the Zachman framework.

This assurance view works as the other abstraction views of Zachman framework by integrating information assurance into all architecture stakeholder perspectives (Heaney et al. 2003). The authors believe that this approach will enable modularization of information assurance to all levels of system engineering and demonstrate how system security elements support the company's business needs (Heaney et al. 2003). However, Heaney et al. do not provide much details about different information assurance elements that should be considered on each level of Zachman framework. They also fail providing proper insight on integrations to the other Zachman abstraction views. Therefore, their framework seems just to consider few selected security topics explicitly without giving a holistic view of security architecture.

3.3.2 Security in The Open Group Architecture Framework

TOGAF does not provide a holistic approach for creating comprehensive security architecture as such. However, TOGAF ADM can be utilized for addressing security as part of EA development. ADM contains some security artifacts which are aimed to ensure

that security controls are implemented into other architecture domains and processes (The Open Group 2016). Security artifacts in ADM are designed to consider two aspects of enterprise security. These aspects are risk management end security management (The Open Group 2016). The two aspects are embedded into other EA domains and artifacts as part of standard ADM process.

According to TOGAF, enterprise architects utilize EA frameworks to define the standards for IT processes and solutions. ADM security artifacts can be used in this process to provide security input and output in each EA development phase for possible situations where the standard processes and solutions might fail to address the related security concerns (The Open Group 2011). From this perspective, TOGAF considers security as an integrated part of other EA processes rather than as a separated EA domain or reference model.

The ADM security artifacts present different areas of concern for security architecture. These areas include authentication, authorization, audit, assurance, availability, asset protection, administration, and risk management (Ertaul et al. 2011). According to TOGAF, common EISA security artifacts should include at least business rules for data and asset handling, asset ownership information, risk analysis documentation, and a security policy (Ertaul et al. 2011).

As with many other security architectures, TOGAF also considers the company security policy as a defining documentation for the security controls (The Open Group 2011). In addition, proper risk assessment should always be performed to justify each security decision made throughout EA development (Ertaul et al. 2011).

Embedding security controls into EA development starts within the preliminary phase of ADM. In this phase the definition of underlying security policies, guidelines, and regulation should be performed (Ertaul et al. 2011). These rules and policies will act as basis for the rest of EISA development process. In the following phase, security architect must get an approval for the made security architecture decisions and document these decisions properly (Ertaul et al. 2011). In this phase, possible conflicts between business processes and security must also be solved (The Open Group 2011).

Next, the three following ADM phases focus on defining and establishing security controls for the architecture domains of TOGAF. These controls include defining system owners and responsible persons, creating architecture and security element inventories, defining disaster recovery procedures, and defining security technology baselines and solutions (Ertaul et al. 2011). The next phase focuses on identifying already existing solutions and tools that could be utilized in the development of security architecture. The focus of this phase is to reduce costs and improve internal efficiency while trying to search for the best possible solutions for security architecture (The Open Group 2011).

The final three phases of ADM aim to establish security controls for the transition to the desired architecture. These phases include defining controls for ensuring monitoring

and continuity of new environments, establishing code reviews and security acceptance criteria for new solutions, managing system configurations in secure manner, and providing input and best practices for future architectural development (Ertaul et al. 2011).

3.3.3 Security in Federal Enterprise Architecture Framework

According to FEAF, security and privacy have been the two primary forces in the development of the framework (The U.S Federal CIO Council 2013). The main security goals set in CA for FEAF are to secure governmental information from unauthorized access and to protect people's privacy according to relevant legislation (The U.S Federal CIO Council 2012). As discussed in chapter 2, security is one of the six architecture domains of FEAF. As with many other EISA frameworks, the security domain of FEAF also intersects with the other architectural domains. This is because according to CA security and privacy controls are most effective when build into all services, processes, systems, and applications (The U.S Federal CIO Council 2012).

FEAF provides a security reference model (SRM) which supports architectural security analysis and reporting in all architectural domains. SRM provides a roadmap for integrating security into EA, introduces mechanisms for identifying security requirements, and promotes inclusion of security and privacy into business processes (The U.S Federal CIO Council 2013). In addition, SRM utilizes National Institute of Standards and Technology's risk and information processing frameworks and standards for establishing security practices compatible with overall enterprise architecture (The U.S Federal CIO Council 2012). The standards and guidelines are integrated into SRM via architectural questions that can be used for defining security controls for each reference model (The U.S Federal CIO Council 2013).

With the help of SRM, FEAF promises to make security and privacy requirements a key component of business decision making (The U.S Federal CIO Council 2012). In practice this is done by identifying touchpoints with other FEAF reference models and setting key artifacts to be produced as part of each model. Each touchpoint is assigned with a high-level mission to define corresponding security controls and as a result they produce security artifacts for supporting security implementation, measuring control effectiveness, and acting as future reference (The U.S Federal CIO Council 2013). Such security artifacts include security control catalogues, security and privacy plans, continuous monitoring procedures, and business continuity plans (The U.S Federal CIO Council 2012).

As with other security architecture frameworks, also FEAF highlights the importance of organizational security policy in defining guidelines and controls for security (The U.S

Federal CIO Council 2012). In addition, FEAF security reference model also emphasizes the importance of risk management in security planning. Risks in SRM are evaluated by first considering the purpose of the system and then defining corresponding regulatory controls and risk profile for the system (The U.S Federal CIO Council 2013). Based on the risk profile, the implementing organization can start the corresponding risk impact mitigation. As a result, proper security controls corresponding to the system risks are created, recorded, and if necessary, adjusted to company security policy or other guidelines (The U.S Federal CIO Council 2013).

3.4 Enterprise information security architecture frameworks

3.4.1 Selecting the relevant enterprise information security architecture frameworks

In addition to the regular enterprise architecture frameworks which address information security to varying degree, there exist also several dedicated enterprise information security architecture frameworks. These frameworks focus mainly on addressing the security domain and related security controls in the context of enterprise architecture and do not pay much attention to other architecture domains or aspects (Tahajod et al. 2009). Therefore, these frameworks are often used to complement general enterprise architecture frameworks.

As opposite of the huge amount of general enterprise architecture frameworks, there are not many dedicated enterprise information security architecture frameworks available for creating and managing information security as part of enterprise architecture (Shariati et al. 2011; Koning 2017). Many EISA models are based on the common EA models and aim to extend the coverage of original frameworks towards security. As with general enterprise architecture, there are also security frameworks that only address the needs of certain industries (Shariati et al. 2011). Some frameworks have also been created to focus only on a certain perspective related to information security, such as risk management (Chuvakin 2018). Such frameworks are ignored in the scope of this thesis since they do not provide holistic overview of information security.

The selected enterprise information security architecture frameworks discussed below are widely accepted and have been actively developed for over a decade (Shariati et al. 2011; Koning 2017). They are also often referred to when discussing about modern standardized EISA models (Shariati et al. 2011; Koning 2017; Chuvakin 2018). Due to the low amount of the widely accepted EISA models, also few lesser known security architecture models created in recent years are discussed below in order to extend the

security literature basis for creating the new information security architecture model in chapter 4.

3.4.2 Sherwood Applied Business Security Architecture framework

The Sherwood Applied Business Security Architecture or SABSA framework is a methodology for developing risk-driven enterprise information security architecture for secure delivery of critical business initiatives (The SABSA Institute 2018). SABSA contains several models and processes which are not dependent on any service management tool or methodology. The SABSA framework is fully scalable and therefore it can be implemented incrementally on any scope from a single system to enterprise wide security architecture (The SABSA Institute 2018).

The framework consists of several components which aim to help companies design, implement, end develop their own security architecture. From these components, there are four key components that form the core of the framework. These key components are the SABSA model, SABSA matrix, development lifecycle, and business attributes profile (Sherwood et al. 2009).

The first key component of the framework is the SABSA model which provides a top-down approach for the EISA development process. The model follows the principles set in Zachman framework and consists of six layers of architectural stakeholder perspectives which all have adapted a security approach. These layers are business, architect, designer, builder, tradesman, and service manager views (Sherwood et al. 2009). However, SABSA model also replaces the traditional stakeholder perspectives with architectural domains corresponding to regular EA frameworks. These domains contain the requirements and definitions made for each of the perspective.

The architectural domains of SABSA model are contextual, conceptual, logical, physical, component, and security service management architecture domains (Sherwood et al. 2009). As with other EA frameworks, each domain in SABSA describes the specific security concerns and requirements and defines deliverables produced in the domain. The SABSA model emphasizes that the security service management architecture should intersect with all the other architectural domains since security management problems arise in each of the domains (Sherwood et al. 2009).

As with the Zachman framework, the SABSA model also inspects the architectural domains through different abstraction views. These views are represented via questions what, why, how, who, where, and when (Sherwood et al. 2009). In accordance with the Zachman matrix, the architecture domains and abstraction views can be arranged into the second key component of the framework, the SABSA matrix. This 6 x 6 matrix creates a holistic representation for enterprise information security architecture. By raising and

addressing security topics of every cell companies are able to develop a comprehensive security architecture (Sherwood et al. 2009).

The SABSA matrix also provides two-way traceability between business requirements and justification behind security decisions (The SABSA Institute 2018). Tracking all business requirements is enabled by presenting all requirements and related solution components in the matrix. In accordance, since all security requirements are listed in the matrix, the justification for all decisions is clearly trackable in the matrix. The SABSA matrix can be seen in figure 3.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figure 3 The SABSA matrix (adopted from Sherwood et al. 2009)

The third key component of the framework is the architecture development process of SABSA. It consists of four phases which are strategy and planning, design, implement, and manage and measure. In the first phase, the contextual and conceptual architectures are created by forming security principles and requirements that are followed throughout the rest of the development process (Sherwood et al. 2009). In addition, the security service management planning is also started in this phase. In design phase, more detailed requirements of rest of the architecture domains are defined (Sherwood et al. 2009). The implementation phase consists of actual architecture implementation. Finally, the manage and measure phase focuses on setting target performance metrics, measuring system operations, and ensuring proper management processes for the systems (Sherwood et al. 2009).

The final key component of the framework is the SABSA business attributes profile. IT is a requirement engineering technique that provides linkage between business requirements and technology design (Sherwood et al. 2009). The tool gathers business requirements for IT and reforms them as business attributes. Each business attribute can then be mapped against certain security controls and measurement methods. This improves traceability between the decided security controls and original business requirements (Sherwood et al. 2009). Companies can use the tool for improving communications between business and security stakeholders. In addition, the business attributes profile provides a checklist of possible attributes to be utilized in requirement definition and enables effective selection of metrics used to define performance targets for systems (Sherwood et al. 2009).

3.4.3 The Open Security Architecture

The Open Security Architecture (OSA) is a framework which provides comprehensive set of principles, guidelines, and tools for EISA creation (The Open Security Architecture 2007). OSA is an open-source framework which relies on its community for publications and support. The framework relies on simple processes and promises companies an easy starting point in security architecture creation by utilizing peer-reviewed collection of best practices with high compatibility with other existing EA frameworks (The Open Security Architecture 2007). The framework is designed to be highly scalable in order to be usable in single systems and huge enterprise environments.

The OSA framework consists of four main components which are the OSA landscape, security patterns, security controls, and actors (The Open Security Architecture 2007). The OSA landscape provides a high-level representation of the entire security architecture. According to OSA, the landscape representation is required for identifying security topics with poor coverage and determining priorities for new security patterns (The Open Security Architecture 2010). The landscape consists of the architecture domains, corresponding security patterns, and security controls of the domains. The architecture domains presented in OSA landscape are governance, service, application, infrastructure, and security service domains (The Open Security Architecture 2010). The standard OSA landscape is described in figure 4.

A security pattern in OSA consists of optimal security solutions for a certain security problem. According to OSA, it is possible to have the best possible solution for certain security problem and this same solution can be generalized to help in all similar problems (The Open Security Architecture 2012). Therefore, OSA security patterns are reusable security solutions which can be utilized to solve reoccurring security problems. Security

patterns emerge through iteration eventually reaching the status of best practice for certain problem (The Open Security Architecture 2012).

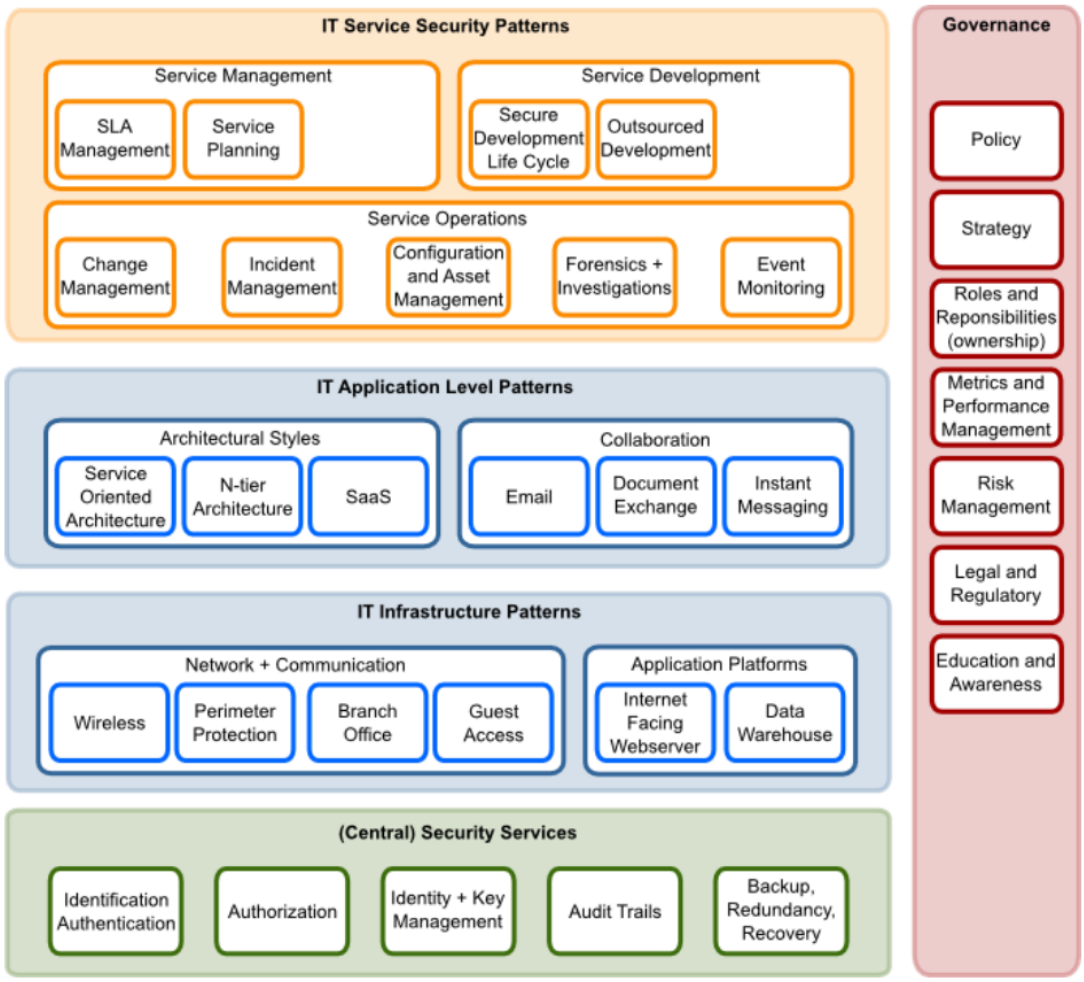

Figure 4 The OSA landscape and security design patterns (adopted from The Open Security Architecture 2010)

The standard OSA landscape contains several default security patterns. These patterns include for example secure development lifecycle, incident and change management, email, perimeter protection, and authorization patterns (The Open Security Architecture 2010). All OSA security patterns contain a set of security controls which need to be implemented in order to solve the related security problem. Security controls include for example documents, process descriptions, and technical controls such as firewalls and anti-virus programs (The Open Security Architecture 2015). There are almost 200 security controls in the OSA framework.

In addition, each security control is grouped by certain actors. Actors are people from the organization who should implement or whose input is needed for the implementation of the control (The Open Security Architecture 2007). There are in total 19 different actors

in the OSA framework including, security manager, asset owner, developer, architect, and quality manager.

The OSA framework emphasizes that it is not necessary to implement all the controls in a security patterns for successful security architecture. Companies can use the standard security controls of a pattern as a checklist or modify them to support the implementation security patterns in their own architecture environment (The Open Security Architecture 2016). This enables flexible use of the framework and ensures that companies can utilize OSA for their individual needs.

As described above, organizations can utilize the standard OSA landscape and the related security patterns and controls as such or they can modify the landscape to fit their specific needs in order to create a suitable target architecture. However, OSA does not provide a supported method for the development of security architecture. Companies utilizing OSA need to select other support models for managing EISA development and the transition between the current and future architecture states. OSA does provide some suggestions for creating and defining the security requirements and principles for the EISA but this process consists of mainly assessing the overall OSA landscape, defining appropriate security patterns, and deciding the related security controls (The Open Security Architecture 2010).

3.4.4 Other recent enterprise information security architecture frameworks

In recent years there have been several attempts to improve and complement current enterprise information security architecture frameworks. The recent frameworks are mostly based on the TOGAF model due to its position as widely utilized enterprise architecture framework. Such security architecture frameworks based on TOGAF include for example Secure Enterprise Architecture focused on Security and Technology-transformation (SEAST) by Ahmed et al. (2017) and Enterprise Architecture Security Assessment Framework (EASAF) by Alshammari (2017).

SEAST framework focuses on ensuring information security as part of technology transformation in the context of enterprise architecture (Ahmed et al 2017). It is based on the foundations of TOGAF and describes technology transformation related processes in selected TOGAF architecture domains. In addition to the TOGAF architecture domains, SEAST introduces a separate security architecture domain to address security of the overall technology transformation process (Ahmed et al 2017). SEAST also introduces several support processes to govern the lifecycle of technology transformation and security. Such processes include for example system modelling, migration planning, and change management (Ahmed et al 2017).

SEAST is designed to work as a process covering the whole lifecycle of technology transformation. The process starts from technology strategy where the strategic decisions for technology are made and moves via transformation and migration planning to technology implementation (Ahmed et al 2017). As part of this process the current enterprise and security architectures direct the implementation of the new technology. If necessary, EA and EISA are also updated during the technology implementation (Ahmed et al 2017).

Rather than creating separate perspectives for all architecture stakeholders during the process SEAST describes the technology transformation only in business and technology architecture domains. This enables focusing only on business and technology stakeholders which SEAST believes to be the key stakeholder groups in technology transformation (Ahmed et al 2017).

In addition to these architecture domains, SEAST also proposes a security architecture domain containing the necessary security controls to ensure security in technology transformation. The security architecture domain contains controls such as data classification, vulnerability management, and log management (Ahmed et al 2017). However, these security controls are only described on a similar level as the OSA design patterns and they lack detailed information about implementation. In addition, SEAST security architecture lacks the governance related controls present in traditional security architectures. Therefore, organizations need to utilize more detailed security control catalogues to apply sufficient security controls to the technology transformation (Ahmed et al 2017).

EASAF is a framework consisting of security related principles, artifacts and metrics which can be used for assessing and recognizing relevant security characteristics of an existing enterprise architecture environment (Alshammari 2017). The framework enables identifying architecture components that require security development.

EASAF implements security controls in the same business domains as TOGAF. However, it splits the business domain of TOGAF into separate employee and process domains. According to EASAF, these two domains are crucial in security architecture development and addressing them as part of the business domain does not ensure sufficient attention for the security controls related to employees and processes (Alshammari 2017). EASAF also provides an architecture development method which is based on the ADM of TOGAF. The secure ADM of EASAF follows the phases of ADM but each phase addresses specifically security elements in developing a security architecture framework.

EASAF describes all architecture domains in respective of the underlying security principle, EA principle, metrics, and artifacts. However, EASAF focuses on describing each architecture domain with only very few primary principles, metrics and artifacts (Alshammari 2017). Therefore, EASAF does not contain a comprehensive list of possible

principles, metrics, and artifacts but it provides only a limited visibility on certain security principle. For example, in technology domain an organization may have defined that the underlying security principle in their architecture environment would be defense in depth. This security principle would be based on the enterprise architecture principle interoperability. The metrics for these principles could then be secure interoperability of critical technology resources and as a result the produced artifacts would be environment and location diagrams. This approach chosen by EASAF provides good traceability and mapping between EA and EISA elements but lacks the holistic overview of all enterprise architecture components. Also, it does not provide a comprehensive set of security controls to support security architecture development.

3.4.5 Challenges of current enterprise information security architecture frameworks

All above discussed enterprise information security architecture frameworks contain typical challenges of enterprise and security architecture. For example, the structures of the most Zachman and TOGAF based models are quite complex, or they contain a large amount of different management processes which make understanding and managing the architectural setup based on the frameworks more difficult. In addition, from security perspective these models all lack enough detail in their security controls for them to act as concrete standalone support tool for security architecture. For example, SABSA, SEAST and EASAF all lack comprehensive security control catalogue for security architecture improvement.

Although FEAF includes more detailed security related processes and artifacts than rest of the Zachman and TOGAF based frameworks, the complexity related to the structure and processes apply to FEAF as well. The Zachman and TOGAF based models and FEAF all also lack proper modularity of improving security architecture. These frameworks work the best when they are applied as such which makes the related implementation projects large and complex. Therefore, the changes required to the existing enterprise architecture environments based on these frameworks tend to have a large impact on the environment. Without proper change control and planning, these large changes may cause operational disruptions and security problems in current processes and systems.

From the security architecture frameworks presented in this thesis, the OSA model is the only framework able to avoid most of the above discussed problems. The OSA model contains the most detailed and comprehensive security control catalogue. These security controls have also been arranged in modular design patterns which enable implementing them as smaller portions to the current enterprise architecture.

However, OSA model has some challenges that the other security architecture frameworks do not have. For example, the structure of OSA model does not completely match the structure of common enterprise architecture frameworks. It lacks some of the common security domains or represents them from a different perspective than the traditional frameworks. In addition, there are also some insufficient security controls in the OSA model which are covered from more holistic perspective in other security architecture frameworks. This lack of detail in some of the security controls might be caused by insufficient or unfinished control review of the OSA community (The Open Security Architecture 2007). OSA also lacks the most support and development processes which are in place in other EISA frameworks.

As seen above, the information security architecture frameworks discussed in this thesis all have some challenges. Challenges in these common frameworks make organizations hesitant to utilize them and actively develop their security architecture. This makes organizations more prone for common security threats. Therefore, there is a high demand for an improved security architecture model.

In order to solve the challenges of the security architecture frameworks discussed above, the next chapter introduces a novel enterprise information security architecture model. The proposed model utilizes the best practices of the common EA and EISA frameworks and combines them into a simplified, flexible and easy to use tool serving as basis for security architecture creation and development. The next chapter first introduces the structure of the proposed LEISA model and then moves forward to present the approaches for applying the model. The chapter also discusses the limitations of the LEISA model.

4 A LIGHT ENTERPRISE INFORMATION SECURITY ARCHITECTURE MODEL

4.1 Creating the light enterprise information security architecture model

4.1.1 Creation methodology

As discussed in previous chapters, there are several problems in the existing information security architecture frameworks which make them ineffective and hard to implement. This makes organizations prone for common security threats. In order to solve challenges of the current EISA models and to provide organizations an effective method for improving their security posture, a light enterprise information security architecture (LEISA) model is created.

The proposed LEISA model is based on the EA and EISA best practices discussed in the previous chapters. This ensures compatibility of LEISA with the existing EA models and enables holistic approach for improving security. The purpose of the model is not to act as a comprehensive EISA framework but to collect key security architecture elements into a single tool to be used as basis for security architecture creation and improvement.

In chapter 1 the research methodology utilized by this thesis was described. As discussed in the chapter, the creation of the LEISA model is done with qualitative research methods and the data collection is based on a literature review of the most common enterprise and security architecture frameworks. The relevant literature of EA and EISA frameworks were already introduced in chapters 2 and 3. In the following subchapters the EA and security elements from those frameworks will be gathered and formed into a light enterprise information security framework.

4.1.2 Structure of the light enterprise information security architecture model

The creation of the light enterprise information security model starts by choosing a proper level and detail for architecture representation. Since the aim of the LEISA model is to give a high-level representation of the security components which both the business and IT can understand, a representation approach similar to the logical architecture from SABSA is most appropriate for the model. The logical architecture, or designer's view describes fundamental security concepts, elements, processes and principles which guide the implementation of later architecture elements (Sherwood et al. 2009). This level of

detail acts between the business and IT providing enough detail for both parties to be able to communicate effectively (Sherwood et al. 2009). The logical architecture also provides concrete enough EISA elements which organizations can utilize for creating and improving their own security architecture.

Since SABSA is based on the Zachman framework, the architect's view of SABSA can be mapped against the architect and engineer perspectives of Zachman. The logical architecture representation is also very similar to the standard architecture representations presented in TOGAF, EASAF, and OSA. It provides the same architecture view as TOGAF's high-level content meta model and OSA's standard landscape.

Since the LEISA model aims to give a security architecture representation on high and generalizable level, the focus of the model is limited mostly on representation of the EISA elements on logical architecture. However, in order to maintain the connection with business requirements, LEISA borrows also some elements from the contextual architecture perspective. These elements are discussed more in the following subchapters.

Next, the LEISA model requires a sufficient way of representing the logical architecture. For this purpose, the representations similar with TOGAF content metamodel, EASAF, and OSA landscape are utilized. These models focus on displaying the architecture elements within their respective architecture domains. This enables architecture elements to be captured, recorded, and represented in a way that supports consistency, completeness, and traceability (The Open Group 2017). In addition, using a representation method which is clear and easy to understand helps stakeholders to communicate and coordinate their activities (The Open Security Architecture 2010).

The TOGAF content metamodel uses entities to describe architectural elements while the OSA landscape utilizes security patterns for the same task. EASAF uses a different approach here as it describes only the underlying security principle in each architecture domain (Alshammari 2017). From these models the content metamodel offers the most versatile way of displaying the elements. For example, the content metamodel separates different elements into application and technology components, data entities, functions, organizational units, and processes (The Open Group 2017). The content metamodel also enables describing the relationship of these elements in varying level of detail depending on the chosen scope.

The EASAF and OSA landscape, being high-level EISA models, lack the capability to represent complex element relationships. However, the OSA landscape combines different levels of abstractions into easily understandable and usable representation (The Open Security Architecture 2010). EASAF fails in this since it describes the architecture domains only from the perspective of underlying EA principles. OSA does not aim to give the most accurate representation of architectural element relationships but emphasizes simple and high-level representation of commonly used security elements

(The Open Security Architecture 2010). This same principle is the very core target for the proposed LEISA model.

The highest-level representation of TOGAF content metamodel is very similar to the OSA landscape. On this level, both frameworks describe the architecture for business decision makers and system owners (The Open Group 2017; The Open Security Architecture 2010). For the other EISA frameworks discussed in this thesis, Zachman based frameworks do not provide similar sufficient ways for forming a practical EA representation. The same holds true also for FEAF. These frameworks depend on borrowing possible architecture modelling practices from other frameworks and focus on more holistic overview of security architecture. Therefore, in order to ensure a practical architecture representation usable by most stakeholders, the architecture representation shared by high-level TOGAF content meta model and OSA landscape is chosen as primary representation method for the LEISA model.

4.1.3 Architecture domains of the light enterprise information security architecture model

Next, the LEISA model requires the necessary architecture domains in which it describes the related security architecture components. As discussed in chapter 2, the typical architecture domains include business, data, application, and technology domains. For example, TOGAF follows this exact same categorization (The Open Group 2017). FEAF and Zachman cover the same domains with a bit different taxonomy while also adding areas such as security and strategy as architecture domains (Ylimäki & Halttunen 2005; The U.S Federal CIO Council 2013). The security architectures discussed in chapter 3 also focus mainly on the same domains.

EASAF is slightly different from rest of the models since it separates business domain into employee and process domains (Alshammari 2017). Both SABSA and OSA also additionally cover security services domains which focus on the security controls and processes related to IT operations and service management (Sherwood et al. 2009; The Open Security Architecture 2010). This kind of operational thinking is covered in other architecture frameworks usually with other stakeholder perspectives or abstraction views and not as a separate architecture domain.

SABSA considers the security services domain as an intersecting domain with all the other architectural domains. This is because according to SABSA, the security services domain related controls and activities should be managed at each level of the architecture (Sherwood et al. 2009). The OSA model does not see security service domain as intersecting. In OSA, the security services are represented as domains among other domains within the OSA landscape. While SABSA considers security services to take a

holistic overview of both operational and technical services, OSA separates the operational and technical service security into separate architecture domains.

In addition, OSA does not recognize business architecture domain as such. The corresponding tasks and controls of a typical business domain are included into the OSA governance and IT service security domains (The Open Security Architecture 2010). OSA represents the governance domain as intersecting with the rest of the domains. In addition to the standard business architecture artifacts such as high-level responsibilities and strategic decision making, the OSA governance domain contains also more detailed security controls. Such controls include for example security education and awareness, and risk management which both need to address all the other architectural domains (The Open Security Architecture 2012).

Based on the discussion above about the typical architecture domains of enterprise and security architecture frameworks, the domains chosen for the proposed LEISA model are governance, service, application, data, and infrastructure. These domains follow the typical taxonomy of common enterprise and security architecture frameworks and ensure the maximum compatibility of the LEISA model with most EA frameworks.

The security service domains proposed in SABSA and OSA are divided in LEISA into the service and infrastructure domains. These domains contain security services related to both operational and technology processes. The service and infrastructure domains also represent the business and technology domains of traditional enterprise architecture.

In addition to the traditional domains, a governance domain is also included into LEISA. In accordance with the OSA model, the governance domain is represented as intersecting with all the other domains and it contains elements from the business domain. This approach is chosen because the governance domain contains many security controls that set principles for the controls in the other domains and therefore these governance controls need to be addressed in all domains.

4.1.4 Security patterns and controls of the light enterprise information security architecture model

Next step in creating the light enterprise information security architecture model is to define the security controls and an appropriate method of representing them in each architecture domain. For choosing the appropriate representation, the most architecture frameworks discussed in the previous chapters do not offer simple methods of bundling and presenting the security controls of each architecture domain. Majority of the architecture frameworks choose to list their different security controls as separate appendices or artifacts. This approach is used for example by TOGAF, SEAST, FEAF and SABSA.

The only framework offering a holistic approach for presenting the security controls is the OSA model. The OSA model design patterns provide a simple methodology for representing and categorizing security controls in each architecture domain. As discussed in chapter 3, design patterns contain security controls which focus on solving a specific security problem. This approach makes it easier to focus EISA improvement on certain security topic and enables better communication between different stakeholders (The Open Security Architecture 2010). This representation method also enables modular security control implementation and reduces the risks of EISA implementation causing business and IT process disruptions. Therefore, design patterns are chosen as a representation method of security controls for the proposed light enterprise information security architecture model. The LEISA design patterns are categorized and represented in their respective architecture domains.

Despite that the OSA model is the only security framework utilizing security patterns as method of categorizing security controls, other security frameworks also use varying level of categorization. For example, FEAF uses a high level of categorization for security controls which is very similar to the design patterns found in the OSA model (The U.S Federal CIO Council 2013). SABSA also uses a sort of security control categorization which is based on the stakeholder views of the framework (Sherwood et al. 2009). Based on the analysis of security controls and their categorization in the discussed security architecture frameworks, 29 security patterns were identified for the LEISA model. These security patterns as well as the high-level description of the LEISA model can be seen in figure 5 below.

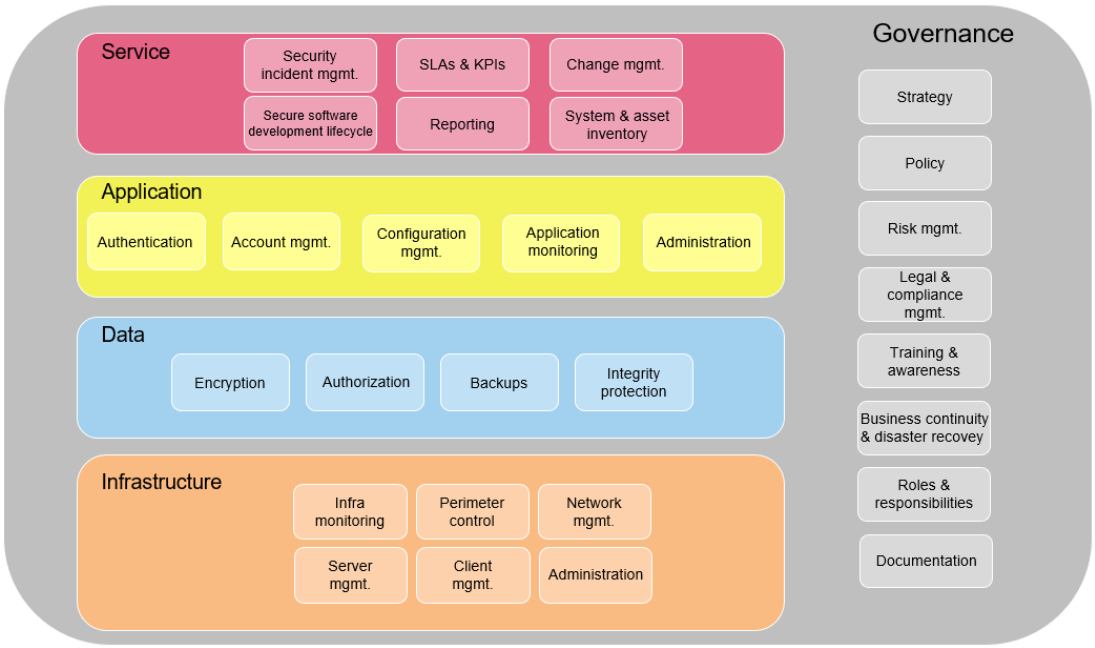

Figure 5 A high-level overview of the light enterprise information security architecture (LEISA) model

It must be noted that traditionally the logical architecture representation of SABSA and similar levels of representation in other EISA frameworks do not contain design patterns and controls for defining strategy. The strategy definition is typically done in the higher levels of EISA stakeholder perspectives. However, since the LEISA model does not contain additional stakeholder perspectives or views in order to maintain simple representation it is not possible to refer to business and IT strategies elsewhere in the model. Therefore, in order to ensure the direct link to business requirements LEISA borrows elements from higher stakeholder perspectives and includes them as design patterns and related controls for security strategy creation. As with other EISA frameworks, the security strategy should be based on the company business and IT strategies in order to confirm that the chosen security elements support the needs of business.

Most security architecture frameworks presented in this thesis contain a variety of security controls aimed to help in defining and implementing a security architecture for organizations. However, the level of detail of these security controls varies significantly between the frameworks. For example, the OSA model contains very comprehensive and detailed catalogue of security controls in which most the controls are explained in detail. In accordance, FEAF also contains a comprehensive list of security controls although these controls lack the same detailed explanation that OSA has. TOGAF and SEAST also contain some security controls or artifacts but they are mainly included into the frameworks as a separate list. The security controls of other TOGAF based security frameworks, SABSA, and security versions of Zachman are defined in more abstract level as they are often categorized based on certain stakeholder view or architecture artifact.

Based on the discussion above, the security controls of the LEISA model are mostly based on the controls defined in OSA, TOGAF, SEAST, and FEAF in order to make the controls concrete and easily understandable. However, the controls of other security frameworks have also been reviewed and controls missing from OSA, TOGAF, SEAST and FEAF have been added to LEISA. In addition, all of the chosen security controls have been reviewed and if necessary adjusted to cover more specific focus on the respective security topic based on the scoping of the original security frameworks. As a result, the LEISA model contains 350 security controls in total. LEISA presents the security controls as a separate list in which the controls are categorized based on their respective design pattern. The comprehensive list of all LEISA model security controls is available in appendices of this thesis.

4.2 Options for applying the light enterprise information security architecture model

As agreed by most EA and EISA frameworks, architecture development should always be based on the company business and IT strategy. The company strategy should set direction and principles for EA development and gradually realize into business processes, related IT systems and in the case of EISA into security controls protecting these processes and systems. This applies to the light enterprise information security architecture model as well. Therefore, when developing security architecture with the help of the proposed LEISA model all decisions related to design pattern and security control implementation should have a valid business justification.

There are two options for applying the LEISA model. These options are applying the model as such to create a completely new security architecture or using it as a reference model for improving an existing security architecture. The first approach is quite straightforward since LEISA is used as such to adopt a new security architecture for the implementing organization. This approach is most suitable for organizations without a proper security architecture or with a very simple and unmatured architecture model.

The implementation of the first approach starts by assessing the compatibility of the LEISA model with the possible current security architecture and enterprise architecture frameworks. At this point it is also suggested that the organization performs a high-level analysis of the possible current security architecture in order to ensure that the old design patterns and controls are not left outside of the new security architecture. This review is not mandatory part of the implementation process since the proposed LEISA model works also as a standalone model, but the review ensures that possible organization specific old security controls are also included into the new security architecture model.

Next, if the LEISA model is compatible with the rest of the existing EA framework, then the organization can adapt all design patterns and security controls of the LEISA model as such. Finally, the organization needs to review the new security architecture and adjust it to fit the possible specific needs of the organization. This adjustment consists of possibly removing some design patterns and security controls or transferring them to other organizational units depending on the structure, processes, roles, and responsibilities within the adapting organization.

The second option for applying the LEISA model is to use it as a reference architecture for improving an existing security architecture. This approach is best for organizations having a complex and mature security architecture setup and which are interested in improving and refining their existing architecture setup. As with the first approach, this approach also starts applying the model by assessing the compatibility of the LEISA model with the current security and enterprise architecture models. In this approach LEISA does not have to be fully compatible with the current architecture setup since

individual security controls and design patterns can be picked from LEISA and utilized in the current setup. However, the underlying structure of the models including the utilization of design patterns and security controls should be somewhat similar.

If the structures of the models are similar, then the next step is to perform a detailed analysis of gaps in design patterns and security controls between the models. In this step the implementing organization reviews what design patterns and security controls of the LEISA model are missing in their current architecture. In addition, the organization must decide on how to add the missing security components into their existing architecture setup. This task may require significant effort from the organization since it may not be easy to find proper place from the current setup for the missing components. For example, some design patterns of the LEISA model might be found in the existing architecture as security controls or similar components which may require relocating all or some of the related security controls to other parts of the security architecture. This problem is discussed more in chapter 4.3.

Finally, after performing the analysis and possible changes to the current architecture setup, the new security architecture is ready. There is no need for a similar second round of review of organizational processes and responsibilities as in the first implementation approach since the LEISA model was already adjusted to the needs and structure of the organization during the throughout analysis of this implementation approach.

After the LEISA model has been applied the implementing organization has an updated security architecture which can be used as basis for understanding the gaps and maturity of their current architecture setup. Based on the possibly missing security design patterns and controls organizations can start planning and prioritizing future architecture development.

As with many other enterprise architecture frameworks, the architecture domains of the light enterprise information security architecture model are not limited to certain order of implementation. Organizations can start implementing their individual security architecture from any of the architecture domains. Each of the domains and design patterns can be considered as separate areas that can be improved individually. However, it is still advisable that organizations consider the LEISA model as whole since many design patterns and controls especially in the governance domain have dependencies with patterns and controls in other domains. This approach reduces the amount duplicate work and helps organizations to understand the impact of changes to the overall security architecture.

It has to be noted that the proposed light enterprise information security architecture model provides only a starting point and initial roadmap for improving the overall security posture of the organization. Even though the proposed LEISA model acts as a tool for creating a new or refining an existing security architecture, organizations must still actually implement the possibly missing security design patterns and controls themselves.

This requires planning, prioritization, budgeting, and resources. Organizations are responsible for making the final decisions on how a certain security control will be implemented and what actions the organizations still have to make in order to finalize their security architecture. Therefore, it is suggested that the organization has a well-thought security strategy which sets guidance for the overall security improvement within organization prior starting the security architecture implementation or changes to current architecture. This security strategy helps defining the target state for organizational security controls and prioritizing the architectural improvement tasks.

4.3 Benefits and limitations of the light enterprise information security architecture model

Utilizing the proposed light enterprise information security architecture model provides many benefits when compared to the existing security architecture frameworks. Since LEISA is based on the widely used enterprise and security architecture frameworks and utilizes their best practices, it provides a wider coverage of security controls that are needed for organizations to mitigate modern security threats than any other current EISA framework.

In order to promote usability and flexibility, the security controls of the model are categorized into different security patterns that can be used to address specific security topics within an organization. This modular structure allows organizations to focus on the security challenges that they are struggling with the most and utilize only the relevant security patterns of the LEISA model to improve their lacking security areas. Due to the structure of the model, it is also easily customizable for different EA environments. Organizations can add or remove security patterns and controls in order to modify the model to match their specific needs. Most current EISA frameworks do not offer this functionality. Since technology and therefore information security is constantly developing, the structure of the model can be adjusted to cover new technology and security trends also in the future. Therefore, the model is not static but enables continuous evolution as per the needs and trends of the industry.

The proposed light enterprise information security architecture model also has some limitations. One of such limitations is related to defining the security design patterns and controls of the model. Since there is no commonly shared definition about security patterns among the current security architecture frameworks or security literature, it is not always trivial to define which security topics should be defined as design patterns and which as security controls. For example, asset management could be included as a design pattern into infrastructure domain or as a security control into client and server management design patterns. The same applies also for other security controls and design

patterns such as vulnerability management and patching. There is a lot of variance among the security architecture frameworks in defining the proper level for each security topic. This may cause problems especially for organizations using the second implementation option of the LEISA model in which the model is used as a reference architecture and alignment between the old and proposed LEISA model is required.

In the proposed LEISA model, the chosen security patterns and controls are categorized based on the scope of each security topic defined in the security architecture frameworks presented in previous chapters. Topics that have been raised as important or holistic in these frameworks have been categorized as design patterns in the LEISA model. The security controls have also been included into the related design pattern of the proposed LEISA model as per their original definition in the security architecture frameworks. The security patterns and controls might not be properly categorized for some organizations, but the flexibility of the model allows modification as per organizations' needs and therefore compensates the possible problems caused by the structure of the proposed LEISA model.

Another possible problem of the LEISA model is the chance that the model is missing some critical security control from its current list of security controls. Not all security controls and design patterns from the existing security architectures were included into LEISA as such since their scope in the original framework were either unclear or overlapping with other security controls and design patterns. The security architecture frameworks used as the basis for the LEISA model may lack some critical security controls as well. Therefore, there is a possibility that some critical security controls are missing in the LEISA model. However, based on the review of the current frameworks the security control coverage should be on sufficient level for comprehensive security architecture implementation and improvement. As stated above, the LEISA model also enables adding security controls and design patterns after implementation which helps improving the security control coverage afterwards if needed.

Finally, there are some challenges with the level of description for each security control included in the LEISA model. Since the controls have been collected from different security architecture frameworks their definition and level of detail vary as well. Some controls may lack the sufficient detail on how they should be implemented. For example, the controls gathered from OSA model are consistently detailed but the controls from FEAF are mostly detailed only on high level.

Defining a detailed explanation for each security control is not in the scope of this thesis and therefore organizations utilizing LEISA need to rely on their security experts and refer either to the original EISA frameworks or to other security guidelines to define detailed instructions and scope for implementing security controls in their individual architecture environment. This requires a certain level of maturity from the implementing organization.

In the next chapter the feasibility and usability of the light enterprise information security architecture model is demonstrated by applying it into an existing enterprise architecture environment of a globally operating IT company. First, the chapter introduces the company and its current enterprise and security architecture environments on a high level. Next, an improved security architecture is created for the company by applying the proposed light enterprise information security architecture model into the current company architecture setup. Finally, the chapter discusses the results and limitations of applying the LEISA model and highlights some possible future improvement suggestions for LEISA.

5 APPLYING THE LIGHT ENTERPRISE INFORMATION SECURITY ARCHITECTURE MODEL INTO AN EXISTING ARCHITECTURE ENVIRONMENT

5.1 Introduction to the target company

5.1.1 Mission and strategy of the target company

Tieto Corporation is a leading technology company in the Nordics with over 15 000 employees in almost 20 countries (Tieto Corporation 2019). Tieto's customers include large companies offering a variety of services to global businesses and consumers working in several industries such as finance, telecom, healthcare, and public sector. Tieto offers their customers consultancy and IT services such as hybrid infrastructure hosting, software development, security services, and product development support (Tieto Corporation 2019). The mission of the company is to enable their customers' everyday business and to help them create future success through smart adoption of technology and utilization of data. In 2018, Tieto was nominated as a Global 100 Tech Leader by Thomson Reuters (Tieto Corporation 2019).

In their strategy, Tieto envisions a future in which data is the biggest driver of continuously increasing societal and economic value. As digitalization gains speed and personalized services become the new normal there will be an increasing demand for data-driven innovations and solutions (Tieto Corporation 2018). Therefore, the company focuses its business into facilitating customers' innovation and renewal plan by addressing service experience by design, smart use of data, architecture adoption and application renewal (Tieto Corporation 2018). In order to achieve its mission, the company applies these same principles to itself by implementing adaptive hybrid infrastructures, utilizing leading technology platforms, and creating partnerships to ensure business agility and cost optimization (Tieto Corporation 2019).

5.1.2 Current IT service model and enterprise architecture environment

Tieto operates in a way in which the internal IT organization provides the core IT services for the whole corporation. This includes for example providing workstation and work equipment services, internal network services, and internal applications that are consumed by the company employees (Tieto Corporation 2008). Such applications include for example customer relationship management systems, company intranet,

payroll related systems, and HR systems. The systems and services provided by Tieto internal IT organization are mostly hosted on the company internal network, but there are also services which have been migrated and outsourced to different vendors and cloud-based solutions (Tieto Corporation 2008).

Although Tieto IT organization has been centralizing the hosting of all internal IT services into dedicated internal network, the overall network setup of the company is quite complex. Most Tieto business units have their own networks and business specific applications which are either located in the same network as the internal Tieto services or have a direct access to these services (Tieto Corporation 2008). This complexity and uncontrolled network expansion are caused mostly by legacy systems and projects from the time when there were no centralized and mature management processes for IT services. Tieto internal IT organization has also difficulties in managing the IT policy compliance in the IT networks and systems of the business units since these units are under individual management and the IT organization has no real jurisdiction within them (Tieto Corporation 2008).

The existing enterprise architecture model of Tieto consists of four main architecture domains; the business architecture, information architecture, application architecture, and infrastructure architecture (Tieto Corporation 2008). In addition, Tieto EA model contains two additional architecture layers which intersect with the rest of the architecture domains. These architecture layers are security and governance (Tieto Corporation 2008). Tieto enterprise architecture model is originally based on the principles of TOGAF. However, the model is not fully following TOGAF principles since it has evolved throughout the years adapting to the changing business needs and IT strategies of the company (Tieto Corporation 2008).

Despite Tieto having a high-level model for EA, the maturity of different architecture domains and layers vary significantly. For example, in recent years there has been a strong focus on improving the business and applications architecture domains of the model. This is due to the company's recent strategy moving towards more business unit centric services and cloud-based applications (Tieto Corporation 2008). The Tieto EA model's governance layer has also achieved a decent level of maturity during the recent years because of the IT organization's plan of improving the overall EA governance of the company (Tieto Corporation 2008).

However, there are also architecture domains and layers with low maturity levels. For example, the infrastructure domain and security layer have not received sufficient attention throughout the years. The reasons for this lack of maturity include gradually integrated legacy IT systems and lack of expertise and resources for arranging holistic infrastructure and security architecture development (Tieto Corporation 2008). This varying level of maturity has driven the Tieto IT organization into improving their current EA practices. In addition, the company's renewed strategy for hybrid infrastructure and

adapting leading technology platforms causes problems for the immature EA domains and pushes the organization for developing a more holistic and adaptive EA model.

5.1.3 Current enterprise information security architecture

As discussed above, Tieto enterprise architecture model contains a security layer intersecting with all the EA domains of the model. Despite that the Tieto security architecture layer is not directly based on any specific security architecture model it borrows content from SABSA and other common security frameworks (Tieto Corporation 2009).

The security layer consists of security areas which are similar to the principle of design patterns presented by OSA model. The security areas focus on describing a certain area of security in the context of Tieto IT environment (Tieto Corporation 2009). These security areas include for example server management, perimeter protection, log management, encryption, and vulnerability management areas. The security areas are assigned to specific architecture domain as defined in the Tieto enterprise architecture model. Each architecture domain has a set of security areas which describe the security topics related to that specific domain. This enables business and systems owners of each architecture domain to easily understand what security components they need to take care of in their daily work (Tieto Corporation 2009).

All security areas consist of security requirements that define how a specific security topic needs to be implemented within Tieto (Tieto Corporation 2009). These requirements are often related to either documentation, certain technologies, or processes which are part of the security area. For example, server management security area contains requirements such as hardening, segregation of duties, and antivirus protection. These requirements are mandatory for the business and system owners to implement in their respective area of responsibility in order to ensure security compliancy to Tieto standards (Tieto Corporation 2009). In total there are 16 security areas with total of 64 security requirements within the Tieto security architecture layer. It has to be noted that detailed and comprehensive information about these security areas and the related requirements will not be disclosed in this thesis due to their confidential nature.

As with many other architecture domains of Tieto enterprise architecture model, the security layer has also evolved throughout the years without strong and holistic governance. This makes the security layer unsuitable for Tieto's recent strategic demands for IT and information security. Most security areas of the security layer are outdated and do not contain sufficient security requirements to address their respective security topic comprehensively. This is also visible in the company provided documentation about their EA posture (Tieto Corporation 2008; Tieto Corporation 2009) which date back to a

decade ago. The security areas are also quite vast by definition and when making changes to the security layer it is sometimes difficult to define which new requirements should belong to which security areas (Tieto Corporation 2009). When analyzing the current security areas against modern IT topics and services, many areas would need reorganizing or new areas and requirements would need to be introduced into the model in order to address the current security and technology trends.

Yet another challenge of the current security architecture layer is the missing security governance area. The main reason for the missing dedicated security governance area is that the governance related topics are addressed in the governance layer of the overall enterprise architecture model (Tieto Corporation 2008). The missing security governance area has led into a practice where many related processes are either addressed separately in other security areas or they are included as subtopics in the general EA governance layer (Tieto Corporation 2009). This often results in security governance related topics to be included only to some of the security areas or even being completely ignored (Tieto Corporation 2009).

The underlying reason for most of the problems discussed above is the lack of proper ownership of the Tieto security architecture (Tieto Corporation 2009). There has not been a sufficient amount of resources throughout the years to take the ownership over the architecture. The ownership of the security architecture has been changing between the past enterprise architects and security managers of Tieto IT organization. This has resulted in an outdated security architecture due to either lack of understanding information security or not having the proper responsibility over the security architecture layer. For example, during the time when the security manager has not been the owner of security architecture, the company IT security policy has been the primary place where changes to existing security practices have been made (Tieto Corporation 2009). These changes have not been reflected to the overall security architecture making the security architecture layer an outdated representation of the company's security practices.

5.2 Creating an improved security architecture with the light enterprise information security architecture model

5.2.1 Methodology for applying the model

As discussed in chapter 1, applying the LEISA model into Tieto's EA environment utilizes research methods similar to typical quantitative research. This part of thesis aims to prove that LEISA can be used to simplify and create a security architecture in an existing architecture environment. Although it is not possible to perform quantitative data

analysis in the scope of this thesis due to the limited amount of implementation data available, the findings of applying the model are analyzed from the perspective of generalizing them also into other architecture environments. This resembles the research methods of quantitative research.

As discussed earlier, Tieto has several different business units and related IT systems and networks. This results in the company having several different enterprise architecture environments. In this thesis the scope for applying the light enterprise information security architecture model is limited to Tieto internal IT organization's EA environment. Therefore, the other EA environments owned by Tieto business units are ignored in applying the EISA model here.

The following subchapters discuss applying the LEISA model into Tieto's architecture environment. The new security architecture created with LEISA replaces the existing Tieto security enterprise architecture and is taken into use within the company. After the new security architecture model has been created the company is able to understand the missing security controls of their current environment and start planning possible future security architecture improvements.

5.2.2 Applying the light enterprise information security architecture model

The light enterprise information security architecture model and Tieto security architecture model are very similar to each other in structure. Both models have four main architecture domains which are similar by content. The business, information, application, and infrastructure domains of Tieto EA model can be directly mapped into the service, data, application, infrastructure domains of the LEISA model. Both models also have a governance domain or layer. However, the Tieto EA governance layer focuses on a more general EA governance for the whole Tieto EA model whereas the LEISA model's governance domain is dedicated for security related governance. Both security architecture models also consist of larger security entities which have been broken down into smaller security components. Tieto security layer consists of security areas which contain security requirements, while the LEISA model consists of security patterns containing security controls. Both ways of representation can be easily mapped to each other.

The main reason for similarities in structure between the two models is that they are both based on same architectural frameworks and foundations. For example, the foundations of TOGAF in both models explain the models' similar architecture representation and content of domains. In accordance, both models share a similar representation for security patterns and controls which is explained by their foundations being in widely used security architecture models.

The biggest difference between the current Tieto EA security model and LEISA model is in their comprehensiveness. There are quite significant differences between the levels of detail in security areas and design patterns of the two models. As discussed earlier, the security areas of Tieto security layer are quite vast by definition and some of them lack proper security requirements to cover the respective security area sufficiently. This also explains the limited number of security areas and requirements in Tieto EA model when compared to the amount of design patterns and controls of the LEISA model.

As described in chapter 4, there are two approaches for applying the LEISA model into Tieto EA model. The first approach is to apply the proposed LEISA model as such. This approach is quite straightforward as the LEISA model can be utilized as it was created without a need for modifying the old security architecture by defining appropriate security areas for the new security components. Some alignment of the current and new security controls is still needed in this approach to ensure that none of the old controls are left out of the new architecture but the approach still lacks the heavy process of modifying and reviewing the current security architecture since all security controls are already categorized under appropriate design patterns.

The second approach for applying the LEISA model is to combine the models in a way that the old security areas would be kept as such and the new security design patterns and controls from the LEISA model would be introduced and mixed into the current security areas. In this approach the current Tieto security architecture would be complemented with several new security areas and requirements. Selecting this approach requires significant effort in reviewing the existing and new security requirements and areas, deciding what new areas and requirements to add, and defining a proper place for them in the current security architecture.

When considering the difference between the comprehensiveness of current Tieto EA security model and the proposed LEISA model it is apparent that the most suitable approach for applying the LEISA model in Tieto's current architecture environment is to apply the model as such. As discussed above, the current Tieto security architecture lacks quite many security patterns and controls which are included in the LEISA model. The current model also lacks a governance related security domain and the related security requirements are scattered within different security areas and general EA governance layer. Therefore, defining new security areas, modifying old security areas and assigning variety of security requirements to them would require a significant amount of work. In addition, due to the similarity of structures of the two models applying the LEISA model as such is relatively straightforward work. After the implementation of LEISA, the new Tieto security architecture is still fully compatible with the rest of the Tieto enterprise architecture model.

Since the approach of applying the proposed LEISA model as such into the current Tieto security architecture was selected, the creation of improved Tieto security EA

model is a relatively simple process. After the first step of implementation, the improved model has all the same architectural domains and design patterns that the LEISA model has. By applying the model as such the amount of security areas in Tieto security EA model will increase significantly. The improved model has a total of 29 security areas as in the proposed light enterprise information security architecture model while the old Tieto security EA model had only 16 security areas.

In order to ensure that no old security areas are left outside of the new Tieto security EA model, it is suggested that the old and new security areas are aligned and reviewed on a high level for any significant differences in content. A minor challenge for performing this cross-check is the difference in detail between the current Tieto security EA model and the proposed LEISA model. For example, some of the security areas of Tieto model can be found as security controls in the LEISA model. Also, many security areas of the old Tieto model lack detailed security requirements which are found in the LEISA model.

When comparing the contents of the two models it can be confirmed that all security areas and requirements of the old Tieto security EA model are covered in the light enterprise information security architecture model. Therefore, the LEISA model can be applied to the current Tieto security EA model as such without significant compatibility problems.

Applying the proposed LEISA model into Tieto security EA model significantly increases the amount of security requirements in the model. The current model has 64 security requirements in total and the LEISA model contains 350 security controls. This makes the improved Tieto security EA model much more detailed in describing the security requirements of each security area and architecture domain.

After applying the LEISA model to the old Tieto security EA model, it is still necessary to review the structure of the new security EA model. Despite the fact that the LEISA model can be applied as such to different architecture environments, it is always necessary to adjust the model to match the structure, processes, and responsibilities of the target organization. This review of the new model is similar to the second option of applying the LEISA model as discussed in chapter 4.2 which would use the model as reference architecture for improving an existing more matured architecture. However, in the first implementation approach this review has much more limited scope thus ensuring a straightforward and cost-effective implementation of the LEISA model.

Based on review of the organizational structure and process responsibilities of Tieto, some adjustments need to be made to the new improved Tieto security EA model. For example, Tieto has organizational units for handling legal matters, and mergers and acquisitions separated from their IT organization. Hence the ownership of the related security processes is also separated from the IT organization. The same applies for some of the company's security policies as well. The main responsibility of several security policies in Tieto belongs to their corporate security unit and not to the IT organization.

Therefore, there are some security controls which need to be adjusted within the improved Tieto security EA model. For example, controls such as personnel security policy and physical security policy from the policy security area need to be transferred to other parts of organization. In accordance, mergers and acquisitions and vendor security management related controls need to be assigned to respective organizations within the company. After aligning the improved Tieto security EA model with the organizational structure, processes, and responsibilities, the final number of security areas of model remains at 29 and the number of security requirements is narrowed down to 326.

5.3 Discussion

By applying the LEISA model into the existing security EA model Tieto was able to create and adopt a new security architecture for managing information security within the company. With the help of the improved security architecture model, the IT organization of Tieto was able to create a holistic view of the currently lacking security requirements and is now able to more easily prioritize future architecture improvements. It is apparent that due to the low maturity level of the old Tieto security EA model there are at the moment several lacking security controls in the current architecture setup of Tieto. This was also partly confirmed during the analysis performed in the implementation of LEISA although a full gap-analysis was not performed as part of this thesis. However, with the help of LEISA the company has now an updated and simplified security architecture to which they can base their future improvement decision making.

The results of applying the light enterprise information security architecture model to Tieto architecture environment suggest that the LEISA model is mature enough for creating and improving security architecture models for different organizations. Especially the approach of applying the model as such enables organizations to establish and improve their current security architecture setup in efficient and simple manner. By utilizing this approach Tieto was able to efficiently create and adopt a new security architecture model which due to its modular structure is easy to keep updated in the future as well.

The second option for applying the LEISA model as a reference architecture was tested only with a limited scope as part of the selected implementation approach in this thesis. However, using the second approach should also provide an efficient method for organizations to improve their current security architecture setup. This is because LEISA utilizes the common security architecture best practices and contains a comprehensive set of security principles from the existing information security architecture models. This set of best practices and principles acts as a comprehensive security control catalogue which can be used as a basis for both partial and holistic security architecture improvement.

Since the LEISA model's structure is based on the structure of common EA frameworks it is also compatible with most architecture frameworks following the common industry standards.

In the case of old Tieto security EA model presented in this thesis it was apparent that the best solution for applying the LEISA model was to use it as such. The old model contained only a limited number of security areas and requirements which could not response to the modern needs of information security. Therefore, utilizing the LEISA model as such was the most efficient method for creating an improved security architecture model for Tieto.

The results of applying the LEISA model to an architecture environment such as in the case of Tieto suggest that the fluent utilization of the model is dependent on the maturity of the old security architecture model. In cases where the existing model can be completely rebuilt it is easier to apply the LEISA model as such. Aligning and comparing the old and new security controls can take significant effort from organizations with already mature and complex security architecture models. Due to the shared architecture foundation of LEISA and Tieto EA model, the structure of improved Tieto security EA model was also directly compatible with the rest of the Tieto architecture environment. In general, the shared architecture foundation and low maturity of the old security architecture made applying the LEISA model into Tieto security EA model quite straightforward and cost-effective task.

Based on the case of applying the proposed LEISA model to Tieto's security architecture, several benefits can be generalized from the utilization LEISA. The model provides organizations an easy and cost-effective method for creating a completely new security architecture or improving their current security architecture. Since LEISA is based on the common enterprise and security architecture frameworks, it is compatible with majority of existing EA frameworks. Due to the model's simple design and structure organizations do not need to spend significant resources in familiarizing themselves with the model and typical complex development processes offered by other EA frameworks. In addition, the simple and modular design of LEISA also enables making only small adjustments to organizations' current security architecture without having a significant impact on all business and IT processes. This reduces the risk of disrupting these processes as part of EISA changes.

All these features of the light enterprise information security architecture model reduce the overall amount of resources needed for security architecture creation and renewal. As discussed in previous chapters, this results in competitive advantages for example by improving resource optimization and internal stakeholder collaboration. In addition, effective security architecture enables integrating security processes into other business and IT processes and thus improves the company overall security posture. Therefore, with

the help of LEISA companies can gain competitive advantages and improve the security of their daily business operations.

The results of applying the light enterprise information security architecture model indicate that the model can contribute significantly to the previous enterprise information security architecture research. The LEISA model provides a flexible and easy to use model for creating and improving security architecture for organizations. It simplifies the methodologies used in common security architecture frameworks and provides organizations a model for detecting gaps in their current security architecture and creating a roadmap to fix these gaps. Since the structure of LEISA is based on modular design patterns and security controls it provides organizations a novel method for improving their existing security architecture without impacting the rest of the enterprise architecture thus lowering the total costs of the overall improvement process. Such models gathering security best practices from the existing security and enterprise architecture methodologies and combining them into a modular security architecture model have not received much attention in the previous enterprise architecture research. The LEISA model and the results of applying it can also be used as basis for future research of efficient and modular enterprise information security architecture.

There are also some limitations in the proposed LEISA model that need to be considered when assessing the results discussed above. First, the model is proved to work effectively when an organization adapts it as such. However, the workload related to applying the LEISA model may increase significantly if the organization has a very complex architecture environment or the structure of the current architecture model is different from LEISA. This is because of the increasing difficulty of aligning and combining the different security patterns and controls with the existing architectural components of large and complex architecture environments.

Due to the structure of Tieto's old security architecture, applying the LEISA model in a complex environment was not possible in the scope of this thesis. However, a fragment of the related workload was seen as part of performing the high-level review the components of the old Tieto security EA and the LEISA models. Choosing the second approach for applying the LEISA model might have an impact on the practical usability of the model. In accordance, choosing the first approach of applying the LEISA model as such may give a false impression of high usability.

Second, the purpose of the LEISA model is to be easily usable and highly flexible which is mostly achieved with the removal of heavy processes and frameworks typically related to enterprise architecture frameworks. However, such processes do have a purpose as part of the overall EA improvement. They support and help organizations as part of the EA improvement process in order to define roles and responsibilities and avoid typical implementation problems. The processes also guide organizations to act and use the framework as intended by the creators of the frameworks. Since there are no extensive

support processes for LEISA, organizations might struggle during the implementation if they face challenges in using the model. Organizations utilizing LEISA need to be mature enough to define the roles and responsibilities related to security architecture, as well as to prioritize and organize the improvement roadmap after the model has been successfully applied. This again may have an impact on the overall usability of the model in organizations with low maturity. To help with problems related to lack of support processes, organizations could consider borrowing related practices from other EA frameworks.

Finally, as discussed in chapter 4.3 some security controls described in the LEISA model may not be able to provide a universal solution on how to address certain security topics within a specific architecture environment. This leaves the responsibility of defining the exact way of implementing the control in the organization's environment to the organization itself. This requires effort and specific knowledge from the IT and information security staff to adjust the controls to match the organizational needs. Depending on the skills and maturity of the IT and security staff, organizations may need to rely on external support material and guidelines in order to utilize LEISA efficiently in their own architecture environment.

Despite these limitations, this thesis shows that the light enterprise information security architecture model provides a practical and flexible method for organizations to create and develop security architecture fitting their specific organizational needs. Further studies of the topic should focus on improving the support processes related to the model such as defining roles and responsibilities for ownership of the security controls and helping organizations to create a prioritized roadmap for further security architecture development. The security controls of the LEISA model also need more detailed description, mapping towards available industry best practice literature, and instructions on how they should be implemented within the specific organizational context. By further improving the light enterprise information security architecture model it could be possible to introduce it as standardized enterprise information security architecture framework for wider audience to complement the current existing enterprise architecture frameworks.

6 CONCLUSION

This thesis studies creating and improving enterprise information security architecture frameworks with a flexible and easy to use model. Even though there are enterprise information security architecture frameworks available in the industry, these frameworks are often complex and require significant effort and resources for successful implementation. The difficulty and high costs of implementation make organizations often hesitant to actively develop their security architecture which results in insufficient security management practices. This makes organizations more prone to information security threats such as data leaks and hacking. The findings of this thesis help organizations to improve their existing security architecture by enabling practical and flexible refining of their current security controls.

The thesis presents a light enterprise information security architecture model which is compatible with various enterprise architecture models following the industry standards. The study utilizes mixed research methods and a literature review for creating the model and analyzing the findings of applying the model. The proposed model is based on the best practices of common enterprise information security architecture frameworks such as SABSA and Open Security Architecture. It consists of security design patterns and security controls which aid in solving security problems related to certain business or IT areas. Such areas include security incident management, encryption, network management, security strategy, and compliance management. The proposed security architecture model provides a practical and modular methodology which can be applied to different architecture environments and tailored as needed.

In order to demonstrate the usability of the light enterprise information security architecture model, this thesis applies it into an existing security architecture of a large IT organization. Based on the results, there are two feasible options for applying the model. The security architecture model can be applied as such to create a new and improved security architecture or it can be used as reference model for refining the existing security architecture. From these options, the first one is more straightforward and easier to implement while the second option may require more effort and resources in refining the existing security architecture. Organizations may choose which ever implementation option they prefer. However, the results of this study suggest that the first option is more suitable for organizations with low architecture maturity while the second option is preferred for more complex architecture setups with higher maturity.

This thesis contributes to the previous enterprise information security architecture research significantly as it provides a flexible and modular model for creating and improving security architecture in different architecture environments. Even though there are commonly used security architecture frameworks available, they are often difficult to use and implementing them requires changes to the whole enterprise architecture

environment. The model presented in this thesis combines the industry security best practices while maintaining the high level of usability and integrability. Therefore, the model can be used by organizations to create or improve their security architecture in efficient manner without a need for changing the overall enterprise architecture environment. Such security architecture models have not received much attention in the previous studies of enterprise architecture and the results of this thesis can be used as basis for future research of enterprise information security architecture.

There are few limitations in the proposed light enterprise information security architecture model and the related findings of this thesis. First, applying the model as reference model into a complex security architecture was not performed in full scope in this thesis. Therefore, the feasibility of this approach in very complex architecture environments cannot be fully confirmed at the moment. Second, in order to achieve flexibility and high usability the model lacks most of the typical support processes often provided by other enterprise and security architecture frameworks. The absence of these processes may impact the implementation success of the model in cases where organizations face problems during the implementation. This may have an impact on the overall usability of the model. Finally, some of the security controls of the model may not be able to provide a universal solution for addressing certain security topics within a specific architecture environment. This leaves the responsibility of deciding the exact way of implementing these controls to the organization itself. Depending on the maturity of the organization the model might not efficiently fulfill all specific needs of the organization. However, by further studying the possible support processes related the light enterprise information security architecture model and mapping the design patterns and security controls of the model towards common industry guidelines and best practices, it could be possible to introduce it as a standardized enterprise information security architecture framework to complement current existing enterprise architecture frameworks.

REFERENCES

Ahmed, T. U. – Bhuiya, N. I. – Rahman, M. (2017) A Secure Enterprise Architecture Focused on Security and Technology-transformation (SEAST). *Proceedings of the 12th International Conference for Internet Technology and Secured Transactions ICITST*, Cambridge, UK, December 11–14, 2017.

Alshammari, B. M. (2017) Enterprise Architecture Security Assessment Framework (EASAF). *Journal of Computer Sciences*, Vol 13, Issue 10, 558–571.

Architecture Center (2019) The Four Types of Enterprise Architecture Framework: Which Is the Best Type For You? 25.2.2019. <https://architecture-center.com/blog/112-the-four-types-of-enterprise-architecture-framework-which-is-the-best-type-for-you.html>, retrieved 11.11.2019.

Avolution (2019) How to Choose an Enterprise Architecture Framework. 4.7.2019. <https://www.avolutionsoftware.com/news/how-to-choose-an-enterprise-architecture-framework/>, retrieved 11.11.2019.

Bel, H. – Bongers, L. – Borger, L. (2009) Security architecture: a new hype for specialists, or a useful means of communication? *PvIB Expert Letter June 2009*, Volume 2, No. 1.

British Computer Society (BCS) (2016) Enterprise Architecture Frameworks: The Fad of the Century. 28.7.2016. <https://www.bcs.org/content-hub/enterprise-architecture-frameworks-the-fad-of-the-century/>, retrieved 9.9.2019.

Chuvakin, A. (2018) Security Architecture Frameworks – Yay or Nay? *Gartner Blog Network*, 24.10.2018. <https://blogs.gartner.com/anton-chuvakin/2018/10/24/security-architecture-frameworks-yay-or-nay/>, retrieved 11.11.2019.

Creswell, J. W. (2003) Research design: Qualitative, quantitative, and mixed methods approaches. Sage Publications Inc: Thousand Oaks, CA.

DeLooze, L. (2001) Applying Security to an Enterprise using the Zachman Framework. SANS Institute InfoSec Reading Room. <https://www.sans.org/reading-room/whitepapers/modeling/paper/367>, retrieved 8.8.2019.

Ertaul, L. – Movasseghi, A. – Kummar, S. (2011) Enterprise Security Planning with TOGAF-9. *Proceedings of the International Conference on Security and Management (SAM)*, Nevada, US, July 18–21, 2011.

Galliers, R.D. – Leidner, D.E. (2009) Strategic Information Management: Challenges and Strategies in Managing Information Systems. Routledge: New York, NY.

Heaney, J. – Hybertson, D. – Reedy, A. (2002) Information Assurance for Enterprise Engineering. *Proceedings of Pattern Language of Programs Conference PLoP*, Nashville, US, September 8–12, 2002.

Heikkilä, J. – Kella, T. – Liimatainen, K. – Seppänen, V. (2010) FEAR Governance Model for Public Service Development. University of Jyväskylä, FEAR project.

Henning, R. R. (1996) Use of the Zachman architecture for security engineering. *Proceedings of 19th NIST-NCSC National Information Systems Security Conference*, Baltimore, US, October 22–25, 1996.

Iacob, M. E. – Meertens, L. O. – Jonkers, H. – Quartel. D. A. (2014) From enterprise architecture to business models and back. *Journal of Software and Systems Modeling (SoSyM)*, Vol 13, Issue 3, 1059–1083.

Kaisler, S. – H. Armour, F. – Valivullah, M. (2005) Enterprise Architecting: Critical Problems. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS)*, Hawaii, US, January 3–6, 2005.

Koning, P. (2017) The Best Framework for Security Architecture. *LinkedIn*, 18.1.2017. <https://www.linkedin.com/pulse/best-framework-security-architecture-pascal-de-koning>, retrieved 11.11.2019.

Lehong, S. M. – Dube, E. – Angelopoulos, G. (2013) An investigation into the perceptions of business stakeholders on the benefits of enterprise architecture: The case of Telkom SA. *South African Journal of Business Management*, Vol 44, Issue 2, 45–56.

Liimatainen, K. – Hoffmann, M. – Heikkilä, J. (2007) Overview of Enterprise Architecture work in 15 countries. Ministry of Finance Finland. FEAR project.

McGovern, J. – Ambler, S. – Stevens, M. – Linn J. – Sharan V. – Jo K.E. (2003) A Practical Guide to Enterprise Architecture. Prentice Hall: Upper Saddle River, NJ.

Oda, S. M. – Zhu, Y. (2009) Enterprise Information Security Architecture A Review of Frameworks, Methodology, and Case Studies. *2nd IEEE International Conference on Computer Science and Information Technology*, Beijing, CC, August 8-11, 2009.

Pavlak, A. (2006) Enterprise Architecture: Lessons from Classical Architecture. *Journal of Enterprise Architecture*, Vol 2, Issue 2, 20–27.

Peltier, T. R. (2016) Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. CRC Press: Boca Raton, FL.

PWC (2018) The Global State of Information Security Survey 2018. <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html>, retrieved 5.5.2019.

Ross, J.W. – Weill, P. – Robertson, D.C. (2006) Enterprise Architecture as Strategy: Creating a Foundation for Business Execution. Harvard Business School Press: Boston, MA.

Safari, H. – Faraji, Z. – Majidian, S. (2016) Identifying and evaluating enterprise architecture risks using FMEA and fuzzy VIKOR. *Journal of Intelligent Manufacturing*, Vol 27, Issue 2, 457–486.

Shariati, M. – Bahmani, F. – Shams, F. (2011) Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science,* Vol 3, 537–543.

Sherwood, J. – Clark, A. – Lynas, D. (2005) Enterprise Security Architecture: A Business-Driven Approach. CRC Press: Danvers, MA.

Sherwood, J. – Clark, A. – Lynas, D. (2009) SABSA Enterprise Security Architecture. <https://sabsa.org/white-paper-requests/>, retrieved 7.7.2019.

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

Sowa, J. – Zachman, J. A. (1992) Extending and formalizing the framework for information systems architecture. *IBM Systems Journal*, Vol 31, No. 3, 590–616.

Tahajod, M. – Iranmehr, A. – Darajeh, M. R. – Branch, D. – Branch, S. (2009) A Roadmap to Develop Enterprise Security Architecture. *2009 IEEE International Conference for Internet Technology and Secured Transactions, (ICITST)*, London, UK, November 9–12, 2009.

Tamm, T. – Seddon, P. B. – Shanks, G. – Reynolds, P. (2011) How Does Enterprise Architecture Add Value to Organisations? *Communications of the Association for Information Systems,* Vol 28, Number 1, 141–168.

The Open Group (2011) Security Architecture and the ADM. (2011) <https://pubs.opengroup.org/architecture/togaf91-doc/arch/chap21.html>, retrieved 7.7.2019.

The Open Group (2016) Integrating Risk and Security within a TOGAF Enterprise Architecture. <https://publications.opengroup.org/g152>, retrieved 7.7.2019.

The Open Group (2017) TOGAF Content Meta Model. <http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap30.html>, retrieved 4.6.2019.

The Open Group (2018) TOGAF Introduction. <https://pubs.opengroup.org/architecture/togaf9-doc/arch/>, retrieved 4.6.2019.

The Open Security Architecture (2007) The OSA vision. <http://www.opensecurityarchitecture.org/cms/index.php>, retrieved 10.10.2019.

The Open Security Architecture (2010) OSA landscape. <http://www.opensecurityarchitecture.org/cms/foundations/osa-landscape>, retrieved 10.10.2019.

The Open Security Architecture (2012) OSA IT Security Patterns. <https://www.opensecurityarchitecture.org/cms/definitions/security_patterns>, retrieved 10.10.2019.

The Open Security Architecture (2015) OSA Control Catalogue. <http://www.opensecurityarchitecture.org/cms/library/0802control-catalogue>, retrieved 10.10.2019.

The SABSA Institute (2018) The SABSA Executive Summary. <https://sabsa.org/sabsa-executive-summary/>, retrieved 6.6.2019.

The U.S Federal CIO Council (2012) The Common Approach to Federal Enterprise Architecture. <https://obamawhitehouse.archives.gov/omb/e-gov/FEA>, retrieved 5.5.2019.

The U.S Federal CIO Council (2013) Federal Enterprise Architecture Framework version 2. <https://obamawhitehouse.archives.gov/omb/e-gov/FEA>, retrieved 5.5.2019.

Tieto Corporation (2008) Tieto Enterprise Architecture model. Company Confidential document.

Tieto Corporation (2009) Tieto Security Architecture. Company Confidential document.

Tieto Corporation (2018) Strategy. <https://www.tieto.com/en/investor-relations/investing-in-tieto/strategy/>, retrieved 15.10.2019.

Tieto Corporation (2019) Our Company. <https://www.tieto.com/en/about-us/our-company/>, retrieved 15.10.2019.

Trochim, W. M. – Donnelly, J. P. – Arora, K. (2016) Research methods: The essential knowledge base. Cengage Learning: Boston, MA.

U.S. Government Accountability Office (2001) A Practical Guide to Federal Enterprise Architecture. <https://www.gao.gov/products/P00201>, retrieved 8.8.2019.

Urbaczewski, L. – Mrdalj, S. (2006) A comparison of enterprise architecture frameworks. *Issues in Information Systems*, Vol 7, Issue 2, 18–23.

Ylimäki, T. – Halttunen, V. (2005) Method engineering in practice: A case of applying the Zachman framework in the context of small enterprise architecture oriented projects. *Information, Knowledge, Systems Management*, Vol 5, Issue 3, 189–209.

Zachman International Inc. (2008) About the Zachman Framework. <https://www.zachman.com/about-the-zachman-framework>, retrieved 10.10.2019.

Zachman, J. A. (1987) A framework for information systems architecture. *IBM Systems Journal*, Vol 26, No. 3, 276–292.

APPENDICES

APPENDIX 1.0 Light enterprise information security model security controls: Service domain

Service		
Security incident mgmt.		**Change mgmt.**
Incident monitoring	Contacts with security groups	Configuration change control
Incident response testing	Incident handling	Monitoring configuration changes
Incident response plan	Incident response assistance	Change approval
Incident response training	Penetration testing	Change request
Secure Software Development Lifecycle		**System & asset inventory**
System security plan	Security categorization	Security categorization
Privacy impact assessment	Security engineering principles	System and asset location
Risk assessment	Developer configuration management	System and asset ownership
Developer security testing	Object reuse protection	System and asset identificator
Application partitioning	Error handling	Supervision and review
Security function isolation		Software inventory
SLAs & KPIs		System inventory
Security measures of performance	Patch management	Asset inventory
Audit storage capacity	Vulnerability scanning	System component inventory
System component inventory	Malicious code protection & alerts	**Reporting**
Contingency plan testing	Account management	Compliance reporting
System backup		Incident reporting

APPENDIX 1.1 Light enterprise information security model security controls: Data domain

Data		
Encryption		**Backup**
Use of external systems	Cryptographic key establishment & management	System backup content
Cryptographic authentication	Use of cryptography	System recovery
Authenticator management	Session authenticity	Backup frequency
Transmission confidentiality		Backup protection
Integrity protection		**Authorization**
Account mgmt.	Separation of duties	Account management
Access enforcement	Least privilege	Access enforcement
Information flow enforcement	Automated marking & labeling	Separation of duties
Continuous monitoring	Information reuse protection	Least privilege
System backup	Boundary protection	Remote access
User identification & authentication	Use of cryptography	System connections
Input restrictions	Output handling & retention	User identification & authorization
Information accuracy & completeness	Transmission integrity	Device identification & authorization
Information validity & authenticity	Session authenticity	

APPENDIX 1.2 Light enterprise information security model security controls: Governance domain

Governance		
Strategy	**Roles & responsibilities**	**Risk mgmt.**
Security strategy	Accountability processes	Risk assessment
Plans of actions and milestones	Security roles	Privacy and security impact assessment
Contacts with security groups	System owner	Security categorization
Security alerts and advisory	Contacts with security groups	Risk mitigation
	RACII	Risk approval
Documentation	**Business continuity & disaster recovery**	**Legal & compliance mgmt.**
Information system documentation	Information system recovery	Continuous monitoring
System security plan	Contingency planning	Security accreditation
Document classification	Contingency training	Security assessment
Document access control	Contingency plan testing	Mergers and acquisitions
Automated marking & labeling	Alternate storage site	Vendor security management
Document storage	Alternate working site	External information system services
Policy		**Training & awareness**
Access control policy & procedures	Roles and accountability	Security process awareness
Security training & awareness policy	Audit procedures	Security policy training
Contacts with security groups	Security assessments	Training records
Security certifications	Contingency planning policy	Position categorization
Monitoring procedures	Identity and authentication policy	Role based training
Configuration management policy	System maintenance policy	System training
Security incident response procedure	Personnel security policy	Access based training
Asset classification policy	Vulnerability scanning procedure	Third-party personnel security
Physical protection procedure	System & service acquisition policy	Personnel sanctions
Risk management policy	Baseline configuration	
Documentation baseline		

APPENDIX 1.3 Light enterprise information security model security controls: Application domain

Application			
Authentication		**Application monitoring**	
Account management	Remote access	Account management	Auditable events & content
Access enforcement	User identification & authentication	Information flow enforcement	Audit monitoring & analysis
Concurrent session control	Device identification & authentication	Remote access	Configuration change control
Auditable events & content	Authenticator management	Continuous monitoring	Monitoring configuration changes
Authentication feedback		Information system recovery	Vulnerability scanning
Account mgmt.		Incident monitoring	Software usage restrictions
Access control policy	Access enforcement	Security categorization	Malicious code protection & alerts
User identification & authentication	Account management	User identification & authentication	Device identification & authentication
Separation of duties	User identification & authentication	Boundary protection	Protection of audit information
Supervision and review	Auditable events & content	Software & information integrity	Audit record retention
Identifier management		Unsuccessful login attempts	System connections
Configuration mgmt.		Security alerts and advisory	Error handling
Security functionality verification	Least functionality	**Administration**	
Least privilege	Authentication feedback	Account management	Concurrent session control
Session lock	Authenticator management	Access enforcement	Supervision and review
Session termination	Application partitioning	Least privilege	Separation of duties
Remote access	Security function isolation	Remote access	Patch management
System connections	Object reuse	Configuration change control	System component inventory
Baseline configuration	Session authenticity		
Configuration change control	Information input restriction		
Error handling	Penetration testing		

APPENDIX 1.4 Light enterprise information security model security controls: Infrastructure domain 1

Infrastructure			
Perimeter control			**Administration**
Information flow enforcement	Session termination	Network disconnect	Account management
Least privilege	Auditable events & content	Remote access	Access enforcement
Unsuccessful login attempts	Audit storage & retention	Session authenticity	Separation of duties
Access enforcement	System use notification	Continuous monitoring	Least privilege
Audit monitoring & analysis	Boundary protection	Malicious code protection & alerts	Concurrent session control
Audit information protection	Vulnerability scanning	Unsuccessful login attempts	Supervision and review
System connections	DDoS protection		Remote access
Access enforcement policy	Use of external systems		Configuration change control
Network mgmt.		**Client mgmt.**	
Access restriction	Use of cryptography	Access enforcement	Baseline configuration
Auditable events & content	System connections	Least privilege	Configuration change control
Continuous monitoring	Wireless access restrictions	System lock	Least functionality
User identification & authentication	Access enforcement	Session termination	Security functionality verification
Device identification & authentication	Information flow enforcement	User identification & authentication	System monitoring
Vulnerability scanning	Least privilege	Use of cryptography	Lifecycle support
Least functionality	DDoS protection	Controlled maintenance	Software usage restrictions
Remote access	Certificate management	Media access	Malicious code protection & alerts
Use of external systems	Session termination	Device identification & authentication	Certificate management
Transmission confidentiality	Session authenticity	User installed software	Software inventory
DNS service		Patch management	

APPENDIX 1.5 Light enterprise information security model security controls: Infrastructure domain 2

Infrastructure		
Server mgmt.		
Access enforcement	Concurrent session control	Continuous monitoring
Separation of duties	Previous logon notification	Physical access control & protection
Least privilege	Session termination	Information access
Unsuccessful login attempts	Auditable events & content	Vulnerability scanning
Application partitioning	Public access protections	Error handling
DDoS protection	Controlled maintenance	System connections
Device identification & authentication	Patch management	Software usage restrictions
Audit storage & retention	Baseline configuration	Use of cryptography
Audit monitoring & analysis	Configuration change control	Resource priority
Audit information protection	Least functionality	Network disconnect
User identification & authentication	System component inventory	Software and information integrity
Malicious code protection & alerts	System monitoring	Security functionality verification
Lifecycle support	DNS service	
Certificate management	Software inventory	
Infra monitoring		
Account management	Auditable events & content	Monitoring configuration changes
Information flow enforcement	Audit monitoring & analysis	Unsuccessful login attempts
Remote access	Configuration change control	Boundary protection
System monitoring	Continuous monitoring	Software & information integrity
System connections	Error handling	Honeypots
Information system recovery	Vulnerability scanning	Device identification & authentication
Incident monitoring	Software usage restrictions	Protection of audit information
Security categorization	Malicious code protection & alerts	Security alerts and advisory
User identification & authentication	Audit record retention	