Sara Larno

# A METHOD FRAMEWORK OF INTEGRATING INFORMATION SECURITY INTO THE ENTERPRISE ARCHITECTURE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

# TIIVISTELMÄ

Larno, Sara
A Method Framework of Integrating Information Security into the Enterprise Architecture
Jyväskylä: Jyväskylän yliopisto, 2019, 74 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Seppänen, Ville

Tietoturvan sisällyttämiseksi osaksi kokonaisarkkitehtuuria on kehitetty useita menetelmiä ja malleja. Tarjolla olevat mallit on kuitenkin usein koettu raskaiksi ja työläiksi käyttää, eivätkä ne kata kaikkia kokonaisarkkitehtuurin osa-alueita. Jotta tietoturva olisi mahdollista integroida kokonaisarkkitehtuuriin sen kaikille osa-alueille, yhtenä mahdollisena lähestymistapana on esitetty tietoturvan integroimista kokonaisarkkitehtuuriperiaatteista käsin. Tässä tutkielmassa raportoidaan suunnittelutieteellisellä menetelmällä kehitetty menetelmäkehys, jonka avulla voidaan luoda kokonaisarkkitehtuurin tietoturvaperiaatteita. Tutkimusaineistona on käytetty valmiita asiantuntijahaastatteluja, joissa 26 haastateltavaa vastasi Suomen julkisen hallinnon kokonaisarkkitehtuurin tilaa koskeviin kysymyksiin. Näistä poimittiin tarkasteltavaksi tietoturvaa koskevat osiot, joita käytettiin yhdessä kirjallisuuslähteiden kanssa määrittelemään lähtökohtia menetelmäkehyksen suunnittelulle. Menetelmäkehyksen luomisessa on hyödynnetty sekä tietoturvaperiaatteiden että kokonaisarkkitehtuuriperiaatteiden luomisen metamalleja ja se on mallinnettu ArchiMate-notaatiolla. Menetelmäkehyksen arvioimiseksi toteutettiin yhdeksän asiantuntijahaastattelua, joiden perusteella kehys muokattiin lopulliseen muotoon. Menetelmäkehyksen avulla tietoturva voidaan integroida osaksi kokonaisarkkitehtuurityötä jo työn varhaisessa vaiheessa, jolloin vältetään hankalaksi ja työlääksi koettu tietoturvavaatimusten ja kokonaisarkkitehtuurityön yhdistäminen.

Asiasanat: kokonaisarkkitehtuuri, tietoturva, suunnittelutieteellinen tutkimus

# ABSTRACT

Larno, Sara
A Method Framework of Integrating Information Security into the Enterprise Architecture
Jyväskylä: University of Jyväskylä, 2019, 74 p.
Information Systems, Master's Thesis
Supervisor: Seppänen, Ville

Several methods and models have been developed to integrate information security into the enterprise architecture. However, the models available are often difficult and laborious to use and do not cover all aspects of the enterprise architecture. In order to integrate information security into the enterprise architecture for all its components, one possible approach is to integrate information security from the enterprise architecture principles. This thesis reports a method framework developed by a design science method that can be used to create information security principles for the enterprise architecture. The research material used in this thesis is consists in part of ready-made expert interviews, where 26 interviewees answered questions about the state of the enterprise architecture of Finnish public administration. These included sections on information security that were used in conjunction with literary sources to determine the basis for designing a method framework. The method framework has been built using meta models from both information security principles and the creation of enterprise architectural principles and is modelled with ArchiMate notation. In order to evaluate the method framework, nine expert interviews were conducted on the basis of which the method framework was finalized. With the method framework, information security can be integrated into the enterprise architecture work in an early state, avoiding the difficult and laborious combination of information security requirements and enterprise architecture work.

Keywords: enterprise architecture, information security, design science research

# FIGURES

# TABLES

# SISÄLLYS

# 1 INTRODUCTION

New technologies, for example cloud services and virtualization, have brought new challenges in security, privacy, operations and data warehousing (Kaisler & Armour, 2017). It has been argued that in order to meet these challenges within Enterprise Architecture (EA), the security and privacy mechanisms and related practices should be designed in all aspects of the architecture instead of relying only on the underlying systems software and its means to provide these features (Kaisler & Armour, 2017). EA methods generally include some risks and safety-related sections. However, the integration of these sections into a holistic approach is still inadequate. (Jonkers & Quartel, 2016.)

The National Audit Office of Finland evaluated the steering of the operational reliability of the electronic services in the Finnish public sector in 2017 (The National Audit Office of Finland, 2017). The use of the EA in the Finnish public sector is mandatory and information security efforts in the Finnish public sector are partly related to the EA. In the report of The National Audit Office, several problems were discovered in both information security and EA fields. For example, the report states that even though EA descriptions would serve as a tool for evaluating, for example, criticality and importance of the electronical services, the EA effort has not been properly taken on in management. In addition, it was found that the criticality and mutual importance of the services and systems are not regularly checked, although there are a lot of changes in the operating environment. Furthermore, goals of the administrative sectors on information security are often a responsibility of ICT units only. (The National Audit Office of Finland, 2017.)

Practical information security in the Finnish public sector is governed by the VAHTI guidelines provided by the Government Digital Security Management Board. VAHTI guidelines are known to the public administration responsible for information management, but not necessarily in detail, because the guidelines are very extent. It has also been stated that the VAHTI guidelines are directed only to individual authorities and do not consider the new requirements and needs of a more networked society. That is why in the audition report it is recommended that the VAHTI guidelines should be made easier to maintain and utilize and updated to better respond to network-based service production. (The National Audit Office of Finland, 2017.)

At present, EA practice is well-established and has clear extensions from software architectural practices. Nightingale and Rhodes (2004), however, point out that, according to the dominant view of EA, IT is still the focus. This works well when the company's structure is simpler, and the EA is designed to align processes and technology with organizational structure. However, in the context of more complex corporate structures, EA's IT orientation is a limiting factor. Even though the study of Nightingale and Rhodes (2004) is fifteen years old, the separated role of IT, and silo mentality in general, is still a problem in the Finnish public sector. It is not only a problem in the EA field, but also in the information security efforts. The information security in Finnish public sector is still conceived as a responsibility of the IT sector, even though there are efforts to align it with the EA in different organizational aspects. (The National Audit Office of Finland, 2017.)

There have been several studies regarding the Finnish public sector EA (E.g. Dang & Pekkola, 2017; Lemmetti & Pekkola, 2012; Lemmetti & Pekkola, 2014; Niemi & Pekkola, 2016; Penttinen, 2018; Penttinen & Isomäki, 2010; Seppänen, Penttinen & Pulkkinen, 2018). In VARKIT2 research (see chapter 4) a total of 26 experts were interviewed regarding EA in the Finnish public sector. The results are in line with the evaluation of The National Audit Office. EA and information security are often separated fields with separated actors: "It is also often the case here that there is […] silos among experts" (Interviewee 2).

VAHTI guidelines are criticized for their complexity and extent, which makes the guidelines difficult to use. Information security is not always present in the EA efforts from the beginning, but instead, information security demands are attached afterwards, which can also be a sign of the silo mentality between EA and information security efforts. Regarding the opinion of the interviewees in VARKIT2 research, instead of a top-label solution, information security should be an integrated part of EA: "But it's just that, keep the security in all architectural solutions through all the layers" (Interviewee 3). "Well it should be, by design, right from the beginning, that it must be right at the beginning, in one aspect, something to keep in mind from the upper level to the detail" (Interviewee 1).

There has been several methods and guidelines for integrating information security to EA, but none of them has proved themselves to be functional solution for the issue. One of the interviewees of VARKIT2 research states, that "security must be considered from the beginning in the same way as the whole architecture work. Security cannot be glued on, but it must be a design principle." (Interviewee 1.) Enterprise architecture principles are "fundamental propositions that guide the description, construction, and evaluation of enterprise architectures" (Stelzer, 2009). Based on these, it seems that to design information security in all aspects of the architecture, it could be beneficial starting point to consider the information security issues from the point of view of EA principles instead of constructing heavy and rigid guidelines and methods. Design science addresses the need to build and evaluate artefacts for identified business need (Hevner et al., 2004).

Objective of this study is to create a method framework that integrates EA and information security. As was stated before, the integration should start from the beginning of the architecture work, which means, that it must be started from the principle level. In this work, the artefact to be built is a method framework for developing the EA information security principles.

The remainder of the thesis is structured as follows: Chapter 2 introduces the theoretical background. Because there is a lack of EA research from the information security point of view, theoretical background comes from both EA and information security fields of research.

Chapter 3 introduces the Design Science Research Method (DSRM) used in this study, and chapter 4 presents the gathering of the research material. Then, chapter 5 defines the objectives for the method framework, and chapter 6 describes the method framework development. In chapter 7, the method framework is evaluated, and chapter 8 presents the results of the evaluation along with the complete method framework. Chapter 9 is for discussion and limitations of the study and gives suggestions for the further research. Final chapter concludes the work.

# 2 THEORETICAL BACKGROUND

## 2.1 Enterprise Architecture

Defining Enterprise Architecture can start from looking at the two concepts it merges: enterprise and architecture. An enterprise is a collection of organizations with common goals. In this way, it can be considered as referring, for example, to a company, company parts, more than one company or a government agency. (Josey, 2018) Architecture refers to a structure. It can be thought of as referring to a system consisting of components, their relationship to each other and the environment. Architecture also has a functional dimension, where architecture refers to the design and development of these components and their relationships. (IEEE-SA Standards Board, 2000.)

IEEE Recommended Practice for Architectural Descriptive of Software Intensive Systems defines architecture as "The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution" (IEEE-SA Standards Board, 2000). The Open Group Architecture Framework (TOGAF) defines architecture similarly: "The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time"(Josey, 2018). Both definitions recognize principles as an essential part of the architecture.

Companies are multifaceted systems that consist of processes, organizations, information, and supporting technologies and have complex dependencies with each other. Understanding, designing, and managing these social, technical, and infrastructure-related perspectives are crucial to delivering and maintaining the efficiency of a business. (Nightingale & Rhodes, 2004.) The EA has been developed to support the operation of such complicated systems. Having a holistic approach, the EA focuses not only on technical aspects, but also on the various aspects of the company where IT systems work. With the help of the EA, it is possible to identify parts of the company, such as human resources, business processes, technologies, information, or various other resources and their interaction with one another. Along with these, the EA examines information systems and how the information systems work firmly in the business. (Kaisler, Armour & Valivullah, 2005.) It means that the EA serves several purposes. For example, it can be used for providing direction to the design, deployment and assessment for both technological and managerial developments. EA can also help to analyse and represent organizations substantial elements, and integration of fragmented information systems and business processes. EA can also provide means to develop coherent information infrastructures and help to develop guidelines for the evaluation of technology plans. This means that the EA does not only concentrate on the technology and the information systems aspect of an organization but can also help to direct the organizations development comprehensively. (Stelzer, 2009.)

## 2.2 Information Security

Organizations should consider many aspects of information security in their operations. The rapid growth of the emerging technologies is creating new threats to the field of the information security, that are difficult to anticipate. It is possible that cyberattacks executed to damage or modify data, can affect critical infrastructure even without any awareness of a data owner. It is noteworthy that at the same time as the threats have changed with emerging technologies, an increasing amount of threats are nowadays still coming from inside organization, whereas external threats to the organization's information security have reduced. Because of that, most of the literature on the information security, from the point of view of the information systems, is focused on the user's perspective and how the user of an information and the technology resources can prevent, detect and respond to the security threats by their actions. (Cram, Proudfoot, & D'Arcy, 2017.)

Information security vulnerabilities contain a significant risk, not only for the operations of an organization, but also from the point of view of the organization's reputation, and financial and legal requirements. To this end, several organizations have been increasingly focusing on developing safety-related policies and aligning them with non-organizational regulations. Academic research has also paid a lot of attention to the creation, implementation and efficiency of the information security. In addition, to address a broader perspective on the information systems research, the issue has also been approached from the perspective of individual aspects such as an information security culture and compliance. (Cram et al., 2017.)

Regardless of the growing interest towards the information security issues, the information security remains conceptually problematic. The main problem lies between the concepts of information security and cyber security, which are, in some definitions, also seen as synonyms to each other. In the definition of Von Solms and van Niekerk (2013), information security includes both the knowledge or information itself and the technology enabling the information to be processed. Instead, cyber security does not only aim to secure information, but also safeguard those who work in cyberspace, whether they are individuals, organizations, or nations. (Von Solms & Van Niekerk, 2013.) According to Mitnick et al. (2011), information security should not only be some techniques, but a process, which includes people and management. In this definition, information security becomes a sub-concept of cybersecurity. (Von Solms & Van Niekerk, 2013.)

Information security also covers data sources that are not covered by cyber security. Information that is based on physical documents or employees' knowledge can be a target to an information security threat. (Von Solms & von Solms, 2018.) For example, individual knowledge refers to the knowledge that is only in the mind of the individual and therefore must be distinguished from the knowledge stored in the technical information system (Shedden, Scheepers, Smith & Ahmad, 2011). Still, individual knowledge is an organization's advantage that needs to be protected from potential threats and vulnerabilities. Thus, in this definition, the information security is a top concept, which also includes the cyber security, but is not limited to digital representation. (Von Solms & von Solms, 2018.)

It can also be argued that the cyber security is a higher concept, which includes, among other things, the information security. The cyber security can be seen from the point of view that in fact all the cyber threats do not threat the information security. The final aspect is to see the information security as an obsolete concept, which should be replaced with cyber security. (Von Solms & von Solms, 2018.)

The interaction of the concepts of information security and cyber security can be represented with a Venn diagram (FIGURE 1) (Von Solms & Van Niekerk, 2013). The diagram shows that cyber security is an ICT related concept that includes also non-information based assets. Information security covers diverse types of information, but the information does not necessarily need to be ICT related. For example, operational reliability is an important aspect of cyber security, but could be related to information indirectly.

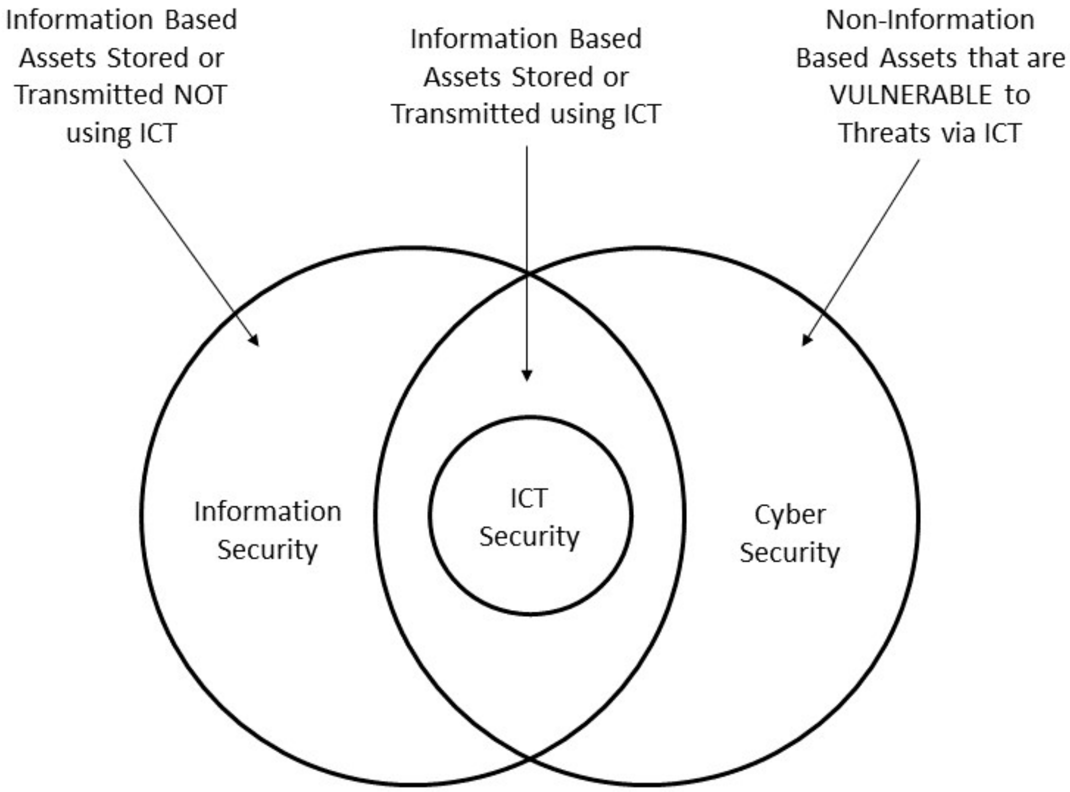

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
ICT Security
Cyber Security

FIGURE 1 Information Security, ICT security and Cyber Security (Von Solms & Van Niekerk, 2013, 101)

In this study, the non-information based assets are excluded. The term information security in this study refers to information based assets that are stored and transmitted both using and not using ICT.

## 2.3 Risk and Security Viewpoints in the Enterprise Architecture

Even though there have been significant efforts to treat the information security as a part of the EA, it seems that both the research and the practical guidance are concentrating only in limited issues. In many cases, the information security is seen from the information systems and a risk management points of view only. Many of the EA methods include sections that are risk- or security-related. Still, the holistic approach to security in the EA lacks. (Jonkers & Quartel, 2016.) The Open Group has published a white paper that analyses how to model the enterprise risks and security concepts using ArchiMate 2.1. The white paper is not only concentrating on the security risks, but covers also strategic and financial risks and risks related to projects and information security. (Band et al., 2014.) The focus of the paper is in Enterprise Risk Management (ERM). ERM is also discussed in the paper by Barateiro, Antunes and Borbonha (2012), where the risk information is proposed to be represented with EA descriptions. The authors see the EA as a mean to mitigate the silo mentality that traditional Risk Management (RM) possesses. The EA descriptions can also give a better understanding on how an asset and its value can be affected by a manifestation of a risk. (Barateiro, Antunes & Borbinha, 2012, 3305.) One of the recent efforts to combine the EA management and the IS security risk management is EAM-ISSRM integrated model (Mayer et al., 2018). The model focuses only on the IS assets, so it does not cover all of the organizational aspects.

Innerhofer–Oberperfle and Breu (2006) have introduced an information security metamodel and security management process that is based on the EA. The metamodel and the security management process are mainly aimed to assess and analyse the IT-related risks in organizations and projects. (Innerhofer - Oberperfler & Breu, 2006.)

The Zachman framework (Zachman, 1987) has also been considered as a starting point for the information security planning in the EA, for example by Ertaul and Sudarsanam (2005), who aimed to integrate the information security in every part of an organization, and converge the information security and the physical security using the Zachman Framework as a logical structure for organizing the management of an enterprise (Ertaul & Sudarsanam, 2005). Even though the scope is to cover organization as a whole, it can be stated that the model of Ertaul and Sudarsanam (2005) is especially useful to help the security planning in the IT (Mayer et al., 2018).

SABSA is a methodology that aims to help developing risk-driven enterprise information security and information assurance architectures. It focuses on business outcomes, because the fundamental idea in the methodology is that the SABSA and The Zachman framework are significantly alike, even though they were developed independently from each other (Burkett, 2012). The SABSA model can thus be used with the Zachman framework to fill the missing security gaps (Burkett, 2012). The SABSA also incorporates security into the process of creating IT architecture solutions and therefore it is also possible to use it with the TOGAF. The TOGAF categorizes architecture in for domains: business, application, data, and technology, but security is not included in this categorization. The SABSA model can be used to add security in all of the four domains of the TOGAF. (Burkett, 2012.)

There are also other EA related security standards. ISO/IEC 27001:2013 specifies requirements for establishing, implementing, maintaining and improving an information security management system, but covers also an information security risks related requirements. ISO 31000:2009 standard introduces principles, framework and risk management process to be used in any type of an organization. COBIT 5 for Information Security is based on the COBIT 5 framework and gives a detailed and practical guidance for the information security management. The Open Enterprise Security Architecture (O-ESA) standard is a reference security architecture that guides the building of a security program and contains sections of information security governance, security principles, and technology components and services. It also supports the implementation of security and risks in EA. The Open Information Security Management Maturity Model (O-ISM3) standard is a process-based approach to build and operate an Information Security Management System (ISMS). The Open FAIR Body of Knowledge is a combination of the Risk Taxonomy (O-RT) Standard and the Risk Analysis (O-RA) Standard. It is developed to help organizations measure both the information security and the operational risks. (The Open Group, 2016.)

It is noteworthy that the majority of these methods, frameworks and standards are concentrating on the risk management aspect of the information security. In some of them, for example in Enterprise Architecture-Based Risk and Security Modelling and Analysis (ERSM), there are principles included, but no guidance for the development of the principle itself (Jonkers & Quartel, 2016). Even though the risk management aspect of the information security is not in the centre of this study, it seems that it is a significant part of the EA approach to information security and for that, it needs to be considered in the method framework development.

## 2.4 Enterprise Architecture Principle

Based on the research conducted by Aier, Fischer and Winter (2011), it seems that only in a minority of organizations EA principles are defined and comprehensively. One problem of defining the EA principles is that there is no consensus of definition of the EA principle neither in the scientific nor in the practical literature. (Aier et al., 2011.)

TOGAF defines a principle from an organizational viewpoint: "Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission" (The Open Group, 2011a). TOGAF sees principles dependent on the organizational context and therefore possibly established within different domains and at distinct levels. TOGAF divides principles in two key domains: the Enterprise Principles and the Architecture Principles. (The Open Group, 2011b.)

Enterprise Principles "provide a basis for decision-making throughout an enterprise and inform how the organization sets about fulfilling its mission" (The Open Group, 2018). Enterprise Principles can also be divided further based on the business or the organizational unit. Different principles can be formed, for example, for the needs of IT, HR, domestic operations, or overseas operations (The Open Group, 2011a).

Architecture Principles "govern the architecture process, affecting the development, maintenance, and use of the Enterprise Architecture" (The Open Group, 2011a). For example, the JHKA defines ten Architecture Principles, for example: "Better decisions, solutions, and services are implemented trough EA" and "New solutions make an extensive use of common services and solutions" (Valtiovarainministeriö, 2017).

The Enterprise Principles and The Architecture Principles have a hierarchical connection: Architecture Principles must reflect the consensus across the organization and be informed and constrained by the enterprise (The

Open Group, 2011a). The problem in this definition is, that it is broad, and it does not distinct Enterprise Principles and Architecture Principles in a requisite accuracy.

In some papers published by the Open Group, the concept of Business Principle is also used. Sometimes it is used in two forms. It can refer to Architecture Principles that address the Business Architecture or to overall Business Principles that do not necessarily have an architectural context. (The Open Group, 2011b.)

The EA principles, that guide the evolution of architecture from an as-is state into a to-be state, are often neglected in the scientific literature (Winter & Aier, 2011). The lack of research can be one reasons why there are many inconsistencies also in the scientific literature regarding the definition of the EA principle. The EA design principles are often mixed up with the EA representation principles, design rules and guidelines. Sometimes architecture principles, business principles and IT principles are mixed together. (Stelzer, 2009.) It is also noteworthy, that principles described in the literature are mostly organization specific and not generalized (Stelzer, 2009).

In practice, the EA principles are widely formulated in organizations and used, for example, for reviewing projects based on those principles. That is why it is essential to document and communicate the EA principles in an organization. Documentation should include, as a profound element, clear definition of principles´ structure and the relations it has with its environment. (Aier, Fischer & Winter, 2011.)

Stelzer (2009) sees that there are three major purposes for the EA principles in an organization. First, the EA principles are needed to describe the current state of an organization (description purpose). Second, the EA principles are for prescribing the target state of an organization (prescription or design purpose). Third, the EA principles can help to evaluate the EA or its elements (evaluation or assessment purposes). (Stelzer, 2009.) Hereby, the EA principles cannot be separate from other principles an organization might have. Stelzer (2009) states that organizational principles combine a network, where the EA principles, IT principles, technology/infrastructure principles, data principles, software architecture principles, application principles, organization principles and business principles can all interact with each other. It depends on the organizational context, which principles exists, how the principles are named and distinguished from one another, and what kinds of a hierarchal relations the principles possess. (Stelzer, 2009, 25.) It is noteworthy that Stelzer (2009) does not see the information security principles as a distinct part of the network of the organizational principles.

Stelzer (2009) uses an Architectural Triangle (FIGURE 2) to clear the concept of the EA principle. With the triangle, Stelzer (2009) distinguishes an architectural design from an architectural representation. The Architectural Triangle is based on an idea, that every system has an architecture, whether it is explicitly represented or not. In the Architectural Triangle, the architectural design refers to a system. System is also described by the architectural representation, that symbols the architectural design. The architectural principle can refer either to the architectural design or the architectural representation. (Stelzer, 2009.)

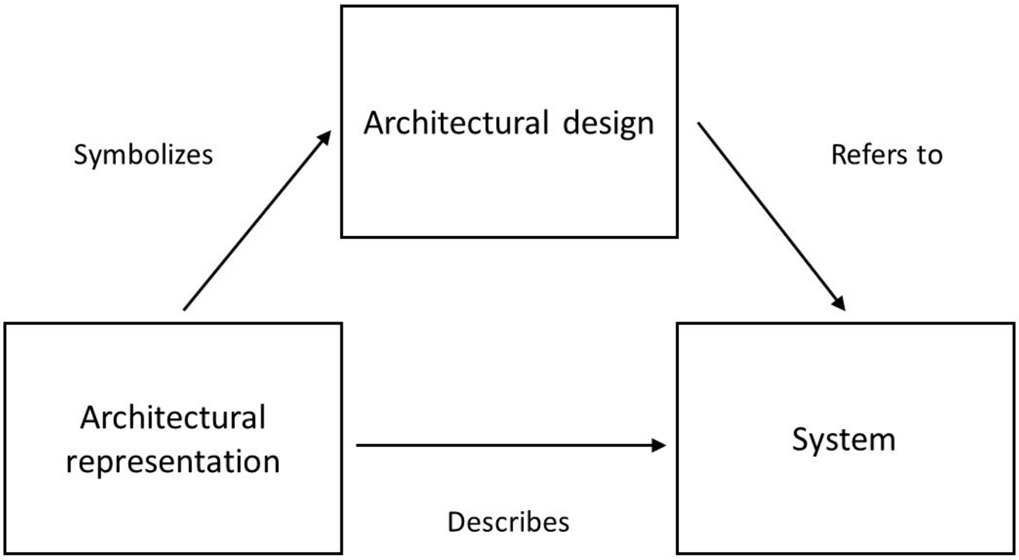


FIGURE 2 The Architectural Triangle (Stelzer, 2009, 14)

Design principles are meant to guide the construction and evaluation of the EA. Representation principles are for describing and modelling architectures and evaluating the architectural representations. Both types of the principles are usually abstract and high-level propositions that are used to guide the development or evaluation of a system. To meet this goal, the principles needs to be specified. This is usually done in a form of rules or guidelines. (Stelzer, 2009.)

Based on a broad literature review, Stelzer (2009) found out that current EA principle literature was not able to provide an acceptable definition of the EA principle. To solve the inconsistency and variety of definitions, Stelzer (2009) proposes a definition that considers both design and representation side of the concept: “Enterprise architecture principles are fundamental propositions that guide the description, construction, and evaluation of enterprise architectures. Enterprise architecture principles fall into two classes: Design principles guide the construction and evaluation of architectures. Representation principles guide the description and modelling of architectures, as well as the evaluation of architectural representations.” (Stelzer, 2009, 31.)

In the EA literature, representation issues, such as notations and meta-modelling, are widely discussed. Instead, design activity issues, and especially design principles, are often neglected. (Aier, Fischer & Winter, 2011.) This is surprising, because, for example, Hoogervorst (2004) sees design principles as a core element of the EA. He claims that the EA can be divided into four interacting domains: organization, business, information and technology, which have distinguished design principles associated to each. Together these design principles form the EA. (Hoogervorst, 2004.)

According to the above studies, we define that the EA design principles govern the architecture process and guide the construction and evaluation of the architectures.

## 2.5 Information Security Policy

Flowerday and Tuyikeze (2016) argue that the current literature on information security policies focuses primarily on describing structures and content, but usually fails to describe a detailed development process. Therefore, people who are involved in the development of the information security policy have little knowledge of the processes they should follow. Due to the lack of the development guidance, those who develop the information security policies and practices often rely on guidelines developed by other organizations, commercially available sources or public sources found in the Internet. However, these guidelines are not necessarily able to guide the organization in the best possible way and recognize and answer to the information security threats and challenges of that particular organization. (Flowerday & Tuyikeze, 2016.) Today's organizations are often young but also very much linked to other organizations. Generic standards for managing the information security usually fails to consider the differences between different organizations and the divergent requirements for the information security. (Baskerville & Siponen, 2002). It can be argued that the EA could be a mean to identify both organization related aspects and multi-organizational relations of the information security.

Despite the fact that many organizations have an organization-level security policy (Goel & Chengalur-Smith, 2010), varies those between organizations on their priorities, accuracy and content. The differences depend, for example, on the value and sensitivity of the information and the technology resources to be protected, and on the impact of any damage, change or disclosure of the information. That means that also the term information security policy varies depending on the context in which it is used. There are also numerous definitions and related concepts that can be found in the literature. (Cram et al., 2017.)

Generally, the concept of the information security policy is divided into three categories of abstraction. At the lowest level of abstraction, information security is looked at from a technical point of view (Baskerville & Siponen, 2002). At this level, it is about the security architecture of the technical systems, which is not published in written, user-shared documents, but is intended to combine the standards and procedures for system configuration or maintenance. At this level, for example, access control lists or firewall rules can be defined. (Cram et al., 2017).

At the next level of abstraction, information security is viewed from the user's point of view (Baskerville & Siponen, 2002). At this level, certain areas of technology, such as email, internet or social media, can be dealt with. These may include instructions and procedures that employees must observe in their daily interaction with information and technology resources. At the same time, penalties may also be described for a breach of acceptable use. Many of the literature sources of the information security principles are looking at the security policies through an individual abstraction level and most of the research literature of the topic deals with this, operational level. (Cram et al., 2017.)

At the highest level of abstraction, information security is dealt with from the senior management point of view. (Baskerville & Siponen, 2002.) At this level, instead of the actual operative principles, it is focusing on the senior management's view of the strategic direction of the organization and the extent and nature of security objectives. These guide the development, implementation and management of the security program and assign responsibilities to the various security areas at the most abstract, philosophical level. (Cram et al., 2017.)

In literature, the information security principle and the information security policy are often used as synonyms. For example, Mayer and Feltus (2017) are modelling an information security principle with an ArchiMate Principle construct and treating it as a synonym to the information security policy. (Mayer & Feltus, 2017). This raises the question of the suitable abstraction level of the EA information security principle.

TOGAF does not include information security principles as a distinct area of the principles but treats them as a part of an integration between TOGAF and SABSA (OpenGroup, 2011b). With the integration, it recognizes that the information security principles should be determined in the Preliminary phase of ADM. This Preliminary Phase is about defining "how we do architecture" in the enterprise concerned. There are two main aspects: defining the framework to be used; and defining the architecture principles that will inform any architecture work. (OpenGroup, 2011b). This implies that the abstraction level of the information security principles should be quite high and not include specific guidelines for users or regarding technology.

To make sure that an organization can function effectively, three matters must be considered when constructing the information security policy. First, an organization must be able to compile and update its information security policy in an agile manner. This is especially important when the organization strives for change that may conflict with the existing information security policy. However, this does not mean that the information security objectives should be ignored, but the information security elements should, as quickly as possible, be aligned with the changed requirements. The goal is that the organization is both capable of effectively seeking change, but also capable of achieving an appropriate level of the information security. This kind of agile aspect is essential, as organizational change can also help meet the information security requirements. Therefore, the principles for managing the information security must always be synchronized with the organizational priorities and the processes that support these goals. (Baskerville & Siponen, 2002.) That aligns well with the goals of EA.

Another matter is a political simplicity. Especially in new organizations that are seeking their shape, the organization's policies might be in constant change, complicated and difficult to manage. Therefore, changes in the information security policy should be carefully thought out and justified. On the other hand, if the information security policy is rigid and difficult to adapt to meet other organizational needs, there is a risk that, for example, management decides to ignore the information security policy in secret. (Baskerville & Siponen, 2002.) Because the EA can be seen as a mean to govern systems that are complicated and difficult to manage, it can provide means to govern also the information security issues in complex systems.

Thirdly, an information security policy must implement existing criteria that can be obtained, for example, from legislation or organization's own priorities. It should be noted, however, that if these criteria are not detailed, it is permissible for policy makers to have a better chance of responding flexibly in modifying the organization's information security policy so that the organization can react efficiently in the organizational changes. (Baskerville & Siponen, 2002.)

Even though the EA can provide means to identify changes, measures to react to the changes, and insight to how the changes are related in various organizational aspects, the EA principles cannot be constantly changing when there is a change either in an environment or inside the organization. To be able to conduct rapid changes, the organization must make quick decisions and actions. The EA principles should be generic enough to enable these changes. That means that the abstraction level of EA information security principle should also be relatively high.

# 3 DESIGN SCIENCE AND ITS IMPLEMENTATION IN THIS STUDY

Gregor (2006) has distinguished five theory types in the information systems research (TABLE 1). The fifth type, Design and action, "says how to do something". Instructions for doing something are given in the form of a design artefact. Even though the prime or only contribution of design science is the created artefact itself, it has a connection with other theory types, because Design and action theory can be informed by the other types. (Gregor, 2006.)

TABLE 1 A Taxonomy of Theory types in Information Systems Research (Gregor, 2006, 620)

| Theory type | Distinguished attributes |
|---|---|
| Analysis | Says what is.<br>The theory does not extend beyond analysis and description. No causal relationships among phenomena are specified and no predictions are made. |
| Explanation | Says what is, how, why, when, and where.<br>The theory provides explanations but does not aim to predict with any precision. There are no testable propositions. |
| Prediction | Says what is and what will be.<br>The theory provides predictions and has testable propositions but does not have well-developed justificatory causal explanations. |
| Explanation and prediction | Says what is, how, why, when, where, and what will be.<br>Provides predictions and has both testable propositions and causal explanations. |
| Design and action | Says how to do something.<br>The theory gives explicit prescriptions (e.g. methods, techniques, principles of form and function) for constructing an artefact. |

To be able to create a method framework for developing the EA information security design principles, Design Science Research Methodology (DSRM) was found to be the most suitable approach. DSRM artefacts are represented in a structured form that may vary from software, formal logic, and rigorous mathematics to informal natural language description (Hevner, March, Park & Ram, 2004).

Hevner et al. (2004) provide a seven-step guideline for the design science in information systems research (TABLE 2).

TABLE 2 The Design Science Research Guidelines (Hevner, March, Park & Ram, 2004, 83)

| Guideline | Description |
|---|---|
| Guideline 1: Design as an Artefact | Design science product must produce a viable artefact in the form of a construct, a model, a method, or an instantiation. |
| Guideline 2: Problem Relevance | The objective of design science research is to develop technology-based solutions to important and relevant business problems. |
| Guideline 3: Design Evaluation | The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods. |
| Guideline 4: Research Contributions | Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies. |
| Guideline 5: Research Rigor | Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact. |
| Guideline 6: Design as a Search Process | The search for an effective artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment. |
| Guideline 7: Communication of Research | Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences. |

First main aspect is that design science research must provide an artefact that works as a solution to an important and relevant business problem. The writers are referring to a technology-based solution, but not specifying what kind of an artefact they see as technology-based. Instead, they are explaining that any design science effort must meet its audience to be useful. For IS researchers the audience are those who plan, manage, design, implement, operate, and evaluate information systems. That is why any research effort must face the problems and opportunities from the interaction of people, organizations, and information technology. (Hevner et al., 2004.) That is why, in an EA context, it can be argued that artefact could also be technology related and does not necessarily need to be technology-based.

The other main aspect in the design science research guidelines is that the artefact must be strongly based on both existing theoretical knowledge and well-executed evaluation. The importance of an evaluation, and because of the evaluation, adjustment of an artefact can also be seen referring to the design science research as an iterative process. Perspective between design process and design artefact also needs to shift constantly. On one hand, the design artefact is a result of the design processes, on the other hand, the evaluation of the artefact gives feedback and provides a better understanding to improve both the artefact and the related design processes. That means that the design science process needs to be conducted iteratively. (Hevner et al., 2004.)

Even though the guidelines are practical in nature, they provide only a little knowledge of how the process of design science research should be conducted. For the purpose, there are several DSR methodologies to choose from. To find the most suitable methodology for this study, a methodology comparison method of Venable, Pries-Heje & Baskerville (2017) is used. Even though the authors state that the differences between six methodologies included in the comparison were for some parts minor, they suggest an approach to be used as a guideline for making a methodological decision (Venable, Pries-Heje & Baskerville, 2017).

First step is to analyze the paradigm and stance (Venable et al., 2017). The authors divide the DSR methodologies in two categories based on the underlying paradigm. The first one is seen positivist and objectivist and the second as interpretivist and subjectivist. Other paradigms are not considered.
The motivation for the subject of this thesis arises from a general need, which is the lack of an efficient method and theory for the EA security principle design. Because the goal is to produce a method framework, instead of a theory, to be able to estimate the suitability and problem-solving capability of the artefact, it needs to be evaluated and tested by experts. This means that the evaluation cannot be based on the interpretation by the researcher. Because of these reasons, objectivistic and positivistic stance was taken.

Second step is to decide, what kind of an artefact is the most suitable for solving the defined problem (Venable et al., 2017). Even though there is also a slack of theory base of the EA information security design principles development, the aim of this study is to create an artefact to be used in an organizational level. Because the scope is not in a specific organization, the artefact needs to be general enough to be implemented in various kinds of organizations. This means that the artefact must be adapted extensively to be used in a specific organization. Based on these qualifications, the most suitable DSR methodology was found to be the Design Science Research Methodology (DSRM) (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007).

DSRM (FIGURE 3) is aligned with DSR guidelines but gives more practical advice of how to conduct a research as a process. The process of the design science research can be divided into subtasks and different entry points depending on the objectives and the context of the research. The process of DSR is represented as a series of iteratively conducted sub-processes. The last two phases, Evaluation and Communication, can lead back to adjusting and developing the artefact. The interesting aspect in the methodology is that those last phases can also enlighten something new from the problem field itself. It means that the developed artefact might also resolve problems, that are recognized after the artefact is developed.

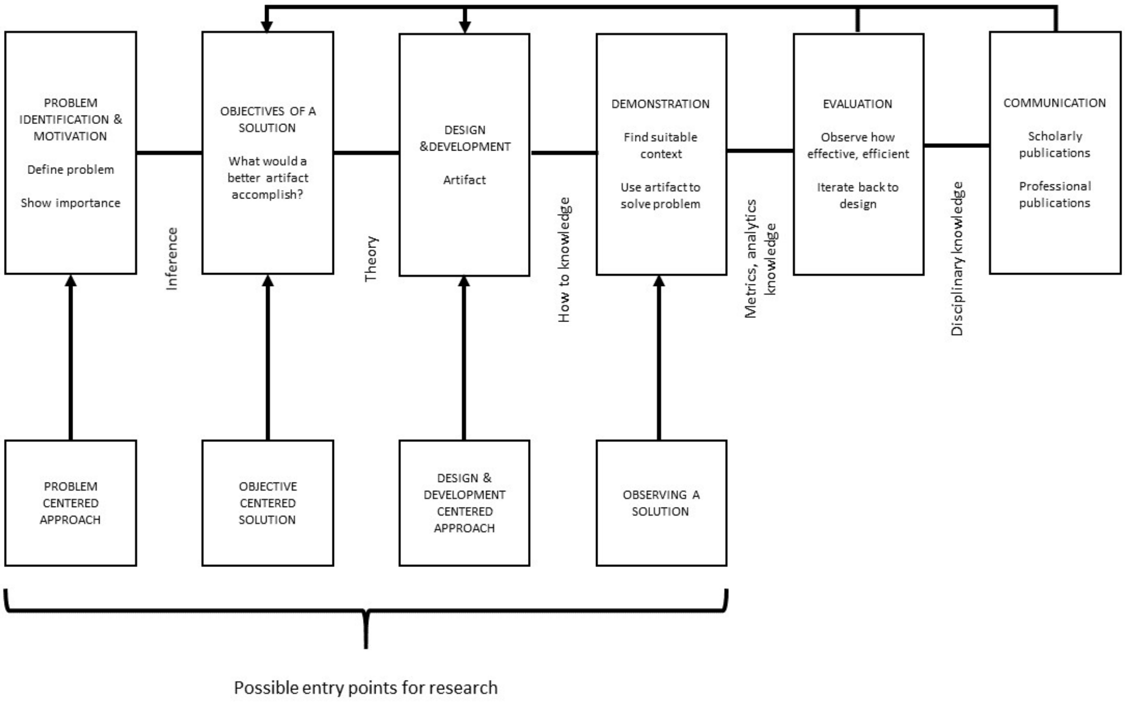

PROBLEM IDENTIFICATION & MOTIVATION
Define problem
Show importance
OBJECTIVES OF A SOLUTION
What would a better artifact accomplish?
DESIGN &DEVELOPMENT
Artifact
DEMONSTRATION
Find suitable context
Use artifact to solve problem
EVALUATION
Observe how effective, efficient
Iterate back to design
COMMUNICATION
Scholarly publications
Professional publications
Inference
Theory
How to knowledge
Metrics, analytics knowledge
Disciplinary knowledge
PROBLEM CENTERED APPROACH
OBJECTIVE CENTERED SOLUTION
DESIGN & DEVELOPMENT CENTERED APPROACH
OBSERVING A SOLUTION
Possible entry points for research

FIGURE 3 The Design Science Research Process (DSRP) Model (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007, 93)

The DSRM is to be conducted in six activities. Activity 1 is Problem Identification and Motivation, where the specific research problem needs to be defined and the value of a solution justified. Activity 2 is to Define the Objectives of a Solution, where the objectives should be referred from the previous phase. (Peffers et al., 2007.) Activity 3 is Design and Development. To be able to design an artefact, first the desired functionalities need to be determined. After that, the artefact is developed based on the objectives and theoretical knowledge. (Peffers et al., 2007.)

There have been numerous contributions to design science, but there are still some unsolved issues related to this methodology (Ostrowski, Helfert & Hossain, 2011). For example, it has been argued that some of the methods do not give specific guiding to artefact design. Even though the chosen method, DSRM, gives executable guidelines for conducting a research, it has been developed further by Ostrowski, Helfert, and Hossain (2011), specifying the activities of the design and evaluation based on distinct kinds of artefacts and the generalizability of the artefact to be designed.

artefacts can be divided into four types that differ from one another by the level of abstraction, but also because they have distinct characteristics. The artefact can be formed as a construct, a model, a method, or an instantiation (Hevner et al., 2004; March & Smith, 1995; Ostrowski et al., 2011). Constructs can be defined as concepts or conceptualizations (March & Smith, 1995) or as vocabulary and symbols (Hevner et al., 2004) mainly aimed for theorizing purposes (Ostrowski et al., 2011). Models are not as abstract as constructs. Instead, they represent a real-world situation. Method can be described as a series of steps or as a guideline for performing a task. Instantiation is the most situational one among the various kinds of artefacts. It can be, for example, an actual specific working system or a tool. (Hevner et al., 2004; March & Smith, 1995; Ostrowski et al., 2011.)

In this study, the aim is to build an artefact for designing EA security principles in an organization, so the result cannot be only a theoretical construct. Because the artefact is supposed to be generic, it cannot be instantiation either. The difference between a model and method is, that a model represents a design problem and its solution space and aids problem and solution understanding (Hevner et al., 2004), unlike a method, that includes actual set of steps (March & Smith, 1995). It can be argued, that because the artefact is supposed to include a principle designing process, it can be described as a method. In addition, it also has a model or framework aspect. Because one aspect is not enough by itself for the artefact to be useful, the artefact to be developed is referred as a method framework.

The outcome of the design research is design knowledge. Because of the iterative nature of the design science research process, the design knowledge can also be used in the design research. The design knowledge can be separated into two outcomes: abstract and situational design knowledge. The abstract design knowledge comes from a meta-design and produces abstract concepts, generic models, guidelines for design practices and systems abstractions with key properties. From the design practice comes situational design knowledge and results. Situational concepts may be applied and adapted from the abstract concepts, the situational models, parts of a situational system or process or instantiations such as prototypes or working IT systems. (Ostrowski et al., 2011.)

The aim of this thesis is to develop abstract design knowledge and a generic artefact instead of a situational one. Both design knowledge types need distinct kinds of designing and evaluation. Abstract design knowledge is reached through meta-design and artificial evaluation. Meta-design includes literature review, modelling and engagement scholarship (Ostrowski et al., 2011.) The method framework is created based on the literature from both research fields: the EA and the information security. Engagement scholarship was executed through interviews.

Both the meta-design and the design practice have diverse types of evaluation that should be conducted during the design and development phase. Venable (2006) has divided design science evaluation approaches into two forms: artificial and naturalistic evaluation. Artificial evaluation can be conducted with computer simulations, role playing simulations, field experiments and lab experiments. Naturalistic evaluation covers case studies, survey studies, field studies and action research. (Venable, 2006.) Ostrowski et al. (2013) has used the distinction of Venable (2006) to separate the evaluation types (FIGURE 4). Based on Venable (2006), Ostrowski et al. (2013) are also seeing the evaluation as a part of a design process which leads from meta-design to artificial evaluation and after that to design practice and naturalistic evaluation.

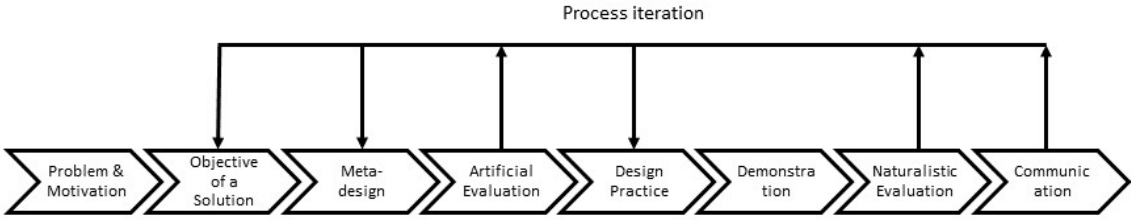


FIGURE 4 A Fragment of The Reference Model in the Design Science Research Methodology (Ostrowski, Helfert & Hossain, 2011, 3)

Artificial evaluation means that the evaluation situation is somewhat artificial compared to an evaluation done in real life situations, for example, by monitoring the use in an organization. (Ostrowski et al., 2011.) In DSRM, there are two evaluation related phases. Evaluation is activity 5 in DSRM, preceded by activity 4, Demonstration. The Demonstration can be implemented in several ways. Some of the possible approaches are experimentation, simulation, case study or proof. After Demonstration activity, the results are observed and measured to find out, how well the artefact acts as a solution to the problem. (Peffers et al., 2007.) In this study, the demonstration phase was conducted as a series of expert interviews. Interviewees were asked to evaluate the suitability of the method framework trough the objectives defined in activity 2 and the artefact was evaluated based on the views of the interviewees. In the DSRM, it is possible to iterate back to the activity 3 if necessary, based on the evaluation results (Peffers et al., 2007). In this case, there were two iterations. The model was modified first time after four interviews and second time after all the nine interviews were conducted.

Last phase of the DSRM, Activity 6, is Communication. The results of the research should be communicated to relevant audiences in suitable ways, such as in the form of research article or thesis, as done in this study.

# 4 RESEARCH MATERIAL

In this study, the Problem Identification and Motivation comes from several sources and is introduced in Chapter 1 (Introduction) of this study. Introduction chapter displays some of the viewpoints of experts interviewed for a VARKIT2 research (for the details, see Penttinen, 2018). This part of the research data was originally gathered for a research project that examined the implementation of the Finnish national enterprise architecture method (FINEA). The research was conducted qualitatively and longitudinally, and for that, there were two semi-structured interview rounds organized. For our study, the second-round interviews, conducted during the summer 2017, were used. The interview questions dealt with the past, present and future situations of EA. The total number of the interviewees was 26. (for the details, see Penttinen, 2018.) For the purposes of this study, an information security related questions and answers were separated from the rest of the interview material. One of the interviews did not address the information security and therefore the number of interviews used in this study was 25. Interviewees represented different levels and sectors of the Finnish public administration as well as IT companies. Interviewees were selected with purposeful sampling (Patton, 1990). Introduction chapter also presents information security and EA efforts in the Finnish public sector. Chapter 2 (Theoretical background) offers the theoretical background of this study and introduces some methods, frameworks and standards designed to integrate the EA and the information security.

Based on the evaluation of these research material sources, it seems that there has been a lot of effort to integrate the information security in the EA. However, as pointed out also in the literature, it seems that both the research and the practical guidance concentrates only in limited issues. Usually the information security is seen from the IS systems and the risk management point of views, even though there are several methods that include risk- or security-related sections. Still, the holistic approach to the information security in the EA is missing. (Jonkers & Quartel, 2016).

The second activity of the DSRM is to determine the Objectives of a Solution. The objectives were also derived from the research material gathered for VARKIT2 research and introduced in the Chapter 5 (Objectives).

The Design and Development phase of the method framework was conducted based on the objectives determined in the previous phase of the methodology. To be able to consider both the information security and the EA principles, metamodels of principle development were selected from both fields and used as a starting point for the development. The metamodels of the principle development also deepen the theoretical background, which is introduced in the Chapter 2 (Theoretical background).

The Demonstration end Evaluation phases were conducted in the form of expert interviews. Informants for the themed interviews were selected with purposeful sampling. When conducting a qualitative research, the size of a sample, or in this case, the amount of the informants, is usually relatively small. Instead of aiming to generalizability that is reached through a large sample in quantitative research, small, purposefully selected samples are chosen to give profound insights of the phenomena. (Patton, 1990.) In this study, the informants were selected based on a criterion sampling. In the criterion sampling, cases are selected on predetermined criterion of importance. (Patton, 1990). All the informants of this study are experts on the EA, the information security or both, with several years of working experience.

Some of the interviewees could be possible to identify by their specific professional titles. To ensure the anonymity of the interviewees, only occupational position, if their field of expertise is enterprise architecture (EA), information security (IS), or both, and working years in the field of expertise are listed (TABLE 3).

TABLE 3 The Interviewees

| Occupational position | Field of expertise | | Working years in the field of expertise |
|---|---|---|---|
| | EA | IS | |
| CDO | X | | 9 |
| CIO | X | X | 20 |
| Enterprise architect | X | | 4 |
| Enterprise architect | X | X | 25 |
| Manager | X | X | 15 |
| Manager | | X | 8 |
| Manager | | X | 15 |
| Researcher | | X | 30 |
| Specialist | X | X | 2 |

The informants were interviewed in the summer 2018. The functionalities of the method framework were demonstrated to the interviewees. After that, they were asked to analyze in detail the usefulness and suitability of the method framework in the context of their own field of expertise and advised to give propositions for improvements. The interviews lasted between 40 and 90 minutes. All the interviews were tape-recorded and transcribed with the permission of the interviewees. TABLE 4 summarizes the research material used in different DSRM Activities.

TABLE 4 The Research Material Used in the DSRM Activities

| DSRM Activity | Research material used in the Activity |
|---|---|
| Problem identification and Motivation | VARKIT2 |
| Objectives of a solution | VARKIT2 |
| Design & Development | Literature |
| Demonstration | Expert interviews |
| Evaluation | Expert interviews |

# 5 OBJECTIVES FOR DESIGNING THE METHOD FRAMEWORK

The DSRM has four possible entry points of the research. In this study, the Problem Identification and Motivation, discussed in the chapter 2, was the entry point. The problem to be solved is the lack of an efficient yet comprehensive method framework to design the EA information security principles. The problem is derived from both the lack of the theory of the area, but also from the lack of the method framework itself. As was stated in the chapter 2, current methods that introduce the information security to the EA are complex, difficult to use and often offer a superimposed solution, where the information security is considered after all other EA efforts.

To be able to determine the objectives of the solution, one must clarify, what would a better artefact accomplish (Peffers et al., 2007). Some of the objectives can be directly derived from the Motivation phase, where the problem is identified. To be able to get more precise objectives, the interview data from VARKIT2 research was used for the purpose.

Even though the aim of this study is not to produce a theory, but a method framework, grounded theory was found to be the most relevant approach. In grounded theory, the aim is not to test an existing theory, but to create a new one inductively based on the research material. In the content analysis based on grounded theory, elements included in the research material are grouped under different classifications. (Charmaz, 1996.) It means that the material is first fractioned and then reassembled under relevant coding.

Because the interview material for VARKIT2 research included mainly topics that were not information security related, the first task was to separate answers related to the information security. Second phase was to find themes underlying the answers of interviewees. The found themes are listed in the TABLE 5.

TABLE 5 Themes of Information Security in the Context of EA

| Theme | Informant | Example from an interview |
|---|---|---|
| Information security should be included in every aspect of EA | 1, 3, 5, 9, 10, 13, 14, 19, 22 | I 3: "Information security must be taken into account in all architectural solutions through all layers." |
| Information security should be included in EA design principles | 1, 12 | I 1: "Security cannot be glued on, but it must be a design principle." |
| Risk management should be included in EA method | 1, 2, 5, 20 | I 20: "Yes, we have been focusing attention on the fact that there is a risk management [in EA method] where information security and risk management are guided." |
| Information security should be adapted to the purpose of an organization | 5, 8, 15, 23, 25 | I 5: "And that is also really what should be planned out of action, that is, what are the needs of action, business or other activities. And what are the risks. And then it combines what kind of information protection or security you need at any point. So, you do not always need to do it categorically through the hardest." |
| Silo mentality should be dismantled | 2, 6, 7, 19, 21 | I 2: "But it is also often the case here that there are silos among experts, that the interaction is needed. And in a way, of course, the EA work is a pretty good place, yes, to create that discussion." |
| EA is a mean to deal with legislative demands | 3, 5, 11, 16, 17, 19, 26 | I 19: "the laws are very extensive, they have complex and big requirements, so EA is just an appropriate tool for dealing with them." |
| Changes in the operating environment can influence information security | 13, 17, 18, 20, 24, 26 | I 26: "I think that more and more cloud-based solutions or hybrid solutions where some of the information is stored locally and part of the cloud. So be sure to change, ways to do the job. And the perceptions of retaining knowledge and utilizing knowledge." |

Several informants stated that to manage the information security effectively, it should be included in every aspect of the EA. An informant noted, for example, that whenever something new is created, information security should be built-in in every requirement (I 9). In the context of the Finnish public sector, it was stated that when developing JHS179, an EA method which is based on TOGAF and used in the Finnish public sector, information security was not built inside the method, but instead, it was acknowledged only in some references. Because the information security guidelines exist mainly in the Government Information Security Management Board's Vahti instructions[1], the information security in the EA often comes out as a glued-on solution and therefore disconnected entity. (I 14.) From this theme, arises Objective 1: *Information security needs to be integrated into all aspects of the EA*.

As defined in the Motivation phase, the best approach to integrate the information security in the EA, was determined to be considering it as a part of the EA design principles. That was also one theme arising from the interview material. It was stated that this could be a beneficial approach, and even though the approach has been considered in the Finnish public-sector EA work, it is not being implemented. (I 12.) From that arises Objective 2: *Information security needs to be managed from EA design principles*.

The third theme is the risk management. It was stated that it is an important aspect to manage the information security. One interviewee was stating that the risk management is something that has been already a part of the EA work at some organizations (I 20). Risk management was also seen as a way to line the information security with the function of an organization, so that the information security efforts do not end up guiding the operations of the organization: "Through risk analyzes is certainly a way. Then there is an assessment of the risks and, secondly, the benefits, the weighing, so that we would not go too much safety above." (I 2.) From that, Objective 3 can be derived: *Risk assessment needs to be a part of the EA design principle development model*.

The fourth theme is related to the previous quotation and theme. The information security should be considered trough business functions. Different organizations demand distinct kinds of information security, based on their goals, information they possess and handle, but also based on the risks that the information security violations may cause to the operations of the organization. "This dimension [information security] as well as nothing else should not be a dogma, but it should be able to live just under the terms of its organization, which would make it meaningful" (I 25). Therefore, Objective 4 is: *Information security needs to be aligned with organization's objectives*.

The fifth discovered theme is operational silos, that are a problem both in the EA and the information security field. Based on the interviews, some of the silos in some organizations seems already been dismantled regarding the EA, but still strongly existing in the information security field. This also means that the EA and the information security are not effectively co-operating, even though the EA work was seen as a suitable place for co-operation (I 2). For

[1] For more information, see https://vm.fi/julkaisut/vahti.

example, there has to be expert knowledge to be able to meet the demands of the legislation: "The laws are really extensive, they have complex and big requirements, so architecture is just a good tool for dealing with them. Especially, when all of them intersect several organizations and there are several functions inside, then no one can stand in a silo to handle it. There should be working groups for all of them. And then we must wonder together how it makes sense to implement." (I 19.) This theme can be divided into two objectives. First, Objective 5: *Legislation needs to be considered in information security context* and Objective 6: *All the relevant stakeholders must be involved in EA work*.

Theme seven arises from the changes in the operational environment that can have a negative influence on the information security. Those can be issues originating outside the organization, for example, hackers or spyware, but also changes within the organizational domain, for example, innovative technology solutions or lack of skills and knowledge in the organization. An objective can be derived from these changes: Objective 7: *Changes in the operational environment must be considered with respect to information security*. As a summary, there are seven objectives to be met when designing the functionalities for the method framework to design EA information security design principles:

1. Information security needs to be integrated into all aspects of the EA.
2. Information security needs to be managed from EA design principles.
3. Risk assessment needs to be a part of the EA design principle development model.
4. Information security needs to be managed from organizations objectives.
5. Legislation needs to be considered in information security context.
6. All the relevant stakeholders must be involved in EA work.
7. Changes in the operational environment must be considered with respect to information security.

# 6 DEVELOPMENT OF THE METHOD FRAMEWORK

## 6.1 Metamodels for the Enterprise Architecture Principle Design

Principles are means that are used for meeting certain ends. In the EA design, the principles are for achieving goals that business, IT or architecture has. Besides the goals, there can also be limitations arising from business or IT that are restricting applicability or validity of the principles. Those limitations can come, for example, from strategy, finances or technology. (Stelzer, 2009, 24.)

Even though the importance of the EA design principles has been widely recognized, there is not very much scientific research about how the principles should be formed. In Stelzer's (2009) literature review, a total of eleven articles about the EA principles were discovered and only six of them covered the EA design principles (Stelzer, 2009). Based on the literature review by Stelzer (2009), Fischer, Winter and Aier (2010) build a metamodel to illustrate of what concepts different authors see as building blocks of the EA design principles (Fischer, Winter & Aier, 2010). Aier, Fischer and Winter (2011) also made a Consolidated meta-model of EA principles (FIGURE 5), that combines the metamodels from distinct researches (Aier et al., 2011).

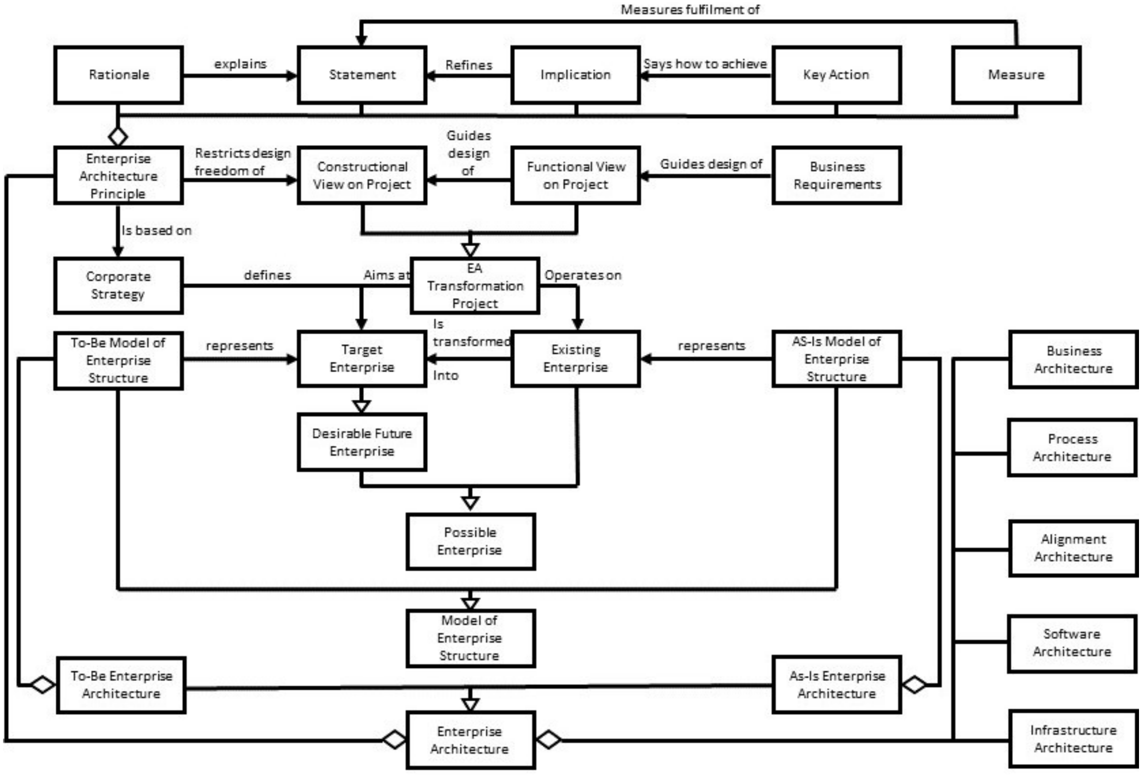


FIGURE 5 The Consolidated Metamodel of EA principle (Fischer, Winter & Aier, 2010, 316)

In the metamodels, both in the consolidated metamodel and in the metamodels based on single researches, it is notable, that there is not very much information about how the principles should be developed.

The models can be divided into two distinct aspects: First, some of the metamodels are showing the different inputs needed for the development. Second, some of the metamodels are illustrating what are the domains the principle impacts, and some are referring to both aspects. To be able to build a method framework to design EA information security principles, the most important aspect is to recognize the inputs needed. That is why the impacts described in metamodels are left out from the development of the method framework in this study.

There are also differences between syntax and semantics in the metamodels. Syntax refers to if we got the principles right and semantics refers to if we get the right principles (Lindström, 2006). This means that syntax is dealing with the form of the principle and semantics with the meaning. To develop a principle, we must distinguish these two. Next, the metamodels are introduced based on the form the principle should be communicated (syntax), and the inputs needed in development (semantics).

In a study by Richardson, Jackson and Dickson (1990), the EA design principles are attributed to four layers: organization, applications, data and infrastructure. There are three aspects to be documented in each layer. First, the Principle itself, second, a Rationale that explains how the principle is assumed to work, and third, concrete Implications. (Fischer, Winter & Aier, 2010;

Richardson, Jackson & Dickson, 1990.) Richardson et al. (1990) do not distinguish the inputs or impacts of the principle, but rather how the principle should be communicated.

In Hoogervorst (2004) a similar metamodel can be found, but with an additional component. Both researches see that Principle, or Principle Statement as named in the metamodel based on Hoogervorst's (2004) study, should be explained by Rationale and refined by Implication. In Hoogervorst's (2004) study there can be also found a component of Key Action that says how to achieve the implication. The Implication conveys how the relevant stakeholders are affected. Key Actions is based on an assumption by Hoogervorst (2004), that all the principles cannot be applied immediately, but there are conditions that must be fulfilled before a principle can be implemented. The Key Actions are therefore guidelines that says how to achieve the Implication. (Fischer et al., 2010; Hoogervorst, 2004.)

In the study by Lindström (2006), the syntax of the architectural principles is defined in four components. Firstly, Statement tells what to improve. Secondly, Motivation gives a reason why the Statement is important. Thirdly, Measure tells how the fulfillment of the Principle can be measured and fourthly, Implication is about what must be done, when, and who should be responsible. These are the aspects that constitute the syntax of Architecture Principle. (Fischer et al., 2010; Lindström, 2006.)

The syntax of the EA design principle defines how the principle should be presented. The semantics describe what are the contents of the principle. The semantics can also be seen as topics for inputs of the principle design. In a metamodel based on publication by Armour, Kaisler and Liu (1999), the EA design principle is driven by Vision, that defines goals and objectives, and that can be further divided into Business Vision and IT Vision (Armour, Kaisler & Liu, 1999; Fischer et al., 2010, 1999).

Another metamodel can be found from a study of Lindström (2006). The starting point of the metamodel is Business Principles that are a base for Enterprise Strategy. Enterprise strategy is a starting point to define an Architecture Principle. (Fischer et al., 2010, 203; Lindström, 2006.)

The problem with these definitions is that they are very broad and do not offer any specific guidelines of which contents to use to develop EA design principles. It can be stated that functional principles need to be derived from the unique needs and characteristics of each individual organization. Because of that, the guidelines cannot be too precise. Another problem with comprehensive instructions is that they might become too laborious to use in an organization. Because of that, to be able to determine specific instructions for principle design, there should be components that are common for all organizations.

Next, we are going to define what are the components of the information security principle design. To create a method framework, those components must be considered and aligned with the components of EA design principle.

## 6.2 Metamodels for the Information Security Principle Design

The purpose of a metapolicy is to control a policy making: how it is created, implemented and how it is controlled (Baskerville & Siponen, 2002). As was stated before, there is not very much guidance available for the organizations to control the policy making (Flowerday & Tuyikeze, 2016). Flowerday and Tuyikeze (2016) respond to this research need by providing a Policy Development Framework (FIGURE 6) for organizations to create an information security policy. However, the framework is not limited to the creation stage only. The authors argue that, to be effective, the information security policy must be manageable throughout its lifecycle. Their framework responds to this challenge. (Flowerday & Tuyikeze, 2016.)

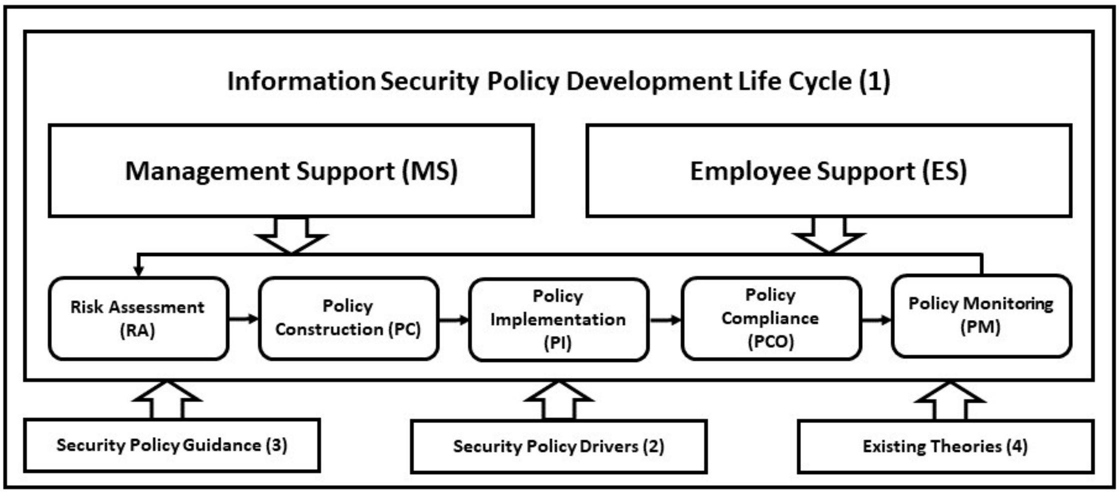


FIGURE 6 The Policy Development Framework (Flowerday & Tuyikeze, 2016, 173)

Even though the Policy Development Framework refers to the information security policy, the writers do not explicit what they mean by information security and what are the topics, concepts and aspects the information security includes. In the article of Flowerday and Tuyikeze (2016), security policy and information security policy are sometimes also used as synonyms. As stated earlier, the difference between the concepts of information security, cyber security and ICT security are sometimes used as synonyms and often lack explicit definitions in the literature. Even though the Policy Development Framework is practical in nature, it operates in a higher abstraction level. That is why the framework has also aspects that can refer to security issues that are not information related.

To build the Policy Development Framework, Flowerday and Tuyikeze (2016) identified ten codes for the development and use of the security policy based on existing literature and expert interviews:

1. Risk Assessment
2. Policy Construction

3. Policy Implementation
4. Policy Compliance
5. Policy Monitoring
6. Management Support
7. Employee Support
8. International Security Standards
9. Policy Stakeholders
10. Legislations Requirements (Flowerday & Tuyikeze, 2016, 170).

The authors state that the first seven of these codes are the processes needed to construct and implement the information security policy and therefore these seven codes form a model of Information Security Policy Development Life Cycle (ISPDLC) (Flowerday & Tuyikeze, 2016). The ISPDLC model is the first component of the Policy Development Framework.

Second component of the framework is Security Policy Drivers. This component consists of the threats that drive the organization to implement mechanisms to protect their information. These threats can come both from inside and outside of the organization. Internal threats are coming from the employees inside the organization. They are usually employees who put the information at risk with their behavior. External threats include, for example, hackers. Security policy development can also be driven by the necessity to comply with government legislative requirements. (Flowerday & Tuyikeze, 2016.)

Third component of the framework is the Security Policy Guidance. This component consists of the security standards that guide the organization with the security policy development.

Fourth and last component consists of the Existing Theories. The Existing Theories can be used to understand employee behavior in relation to the information security. For example, behavioral theories such as General Deterrence Theory and Theory of Planned Behavior can play a key role in understanding the employees behavioral thinking, attitudes, subjective norms and so on. (Flowerday & Tuyikeze, 2016.)

Flowerday and Tuyikeze (2016) focus primarily on examining the ISPDLC model. For this purpose, they statistically examined the relationship between the codes that are forming the model. Based on a statistical analysis, the researchers found that the key factor in the development of information security policy is the Risk analysis. That is why the authors also suggest that risk analysis should be carried out as a first step in the development of the information security policy. For this, it is important to identify the threats and vulnerabilities that need to be minimized. The next most relevant code in the framework is the Management support. With the statistical analysis, the researchers found that the increase in the Management support positively influences other aspects of the model. As an example, the resources provided by the management led to increased information security. A similar relation was also found between the Employee support and other aspects of the framework. (Flowerday & Tuyikeze, 2016.)

Knapp, Morris, Marshall and Byrd (2009) have also explored the creation and use of the security policy from the perspective that it should be a continuous process in the organization. The framework they created, called Comprehensive Information Security Policy Process Model (CISPPM) (FIGURE 7), has similarities with the framework of Flowerday and Tuyikezen (2016), but it takes a closer look at what both internal and external factors affect the security policy throughout its lifecycle. As external factors, the authors identified Economic Sector, Technology Advances, Industry Standards, Legal & Regulatory Requirements regulations, and External Threats. Within the organization, internal factors include Senior Management Support, Business Objectives, Organizational Culture, Technology Architecture, and Internal Threats. (Knapp, Morris, Marshall & Byrd, 2009.)

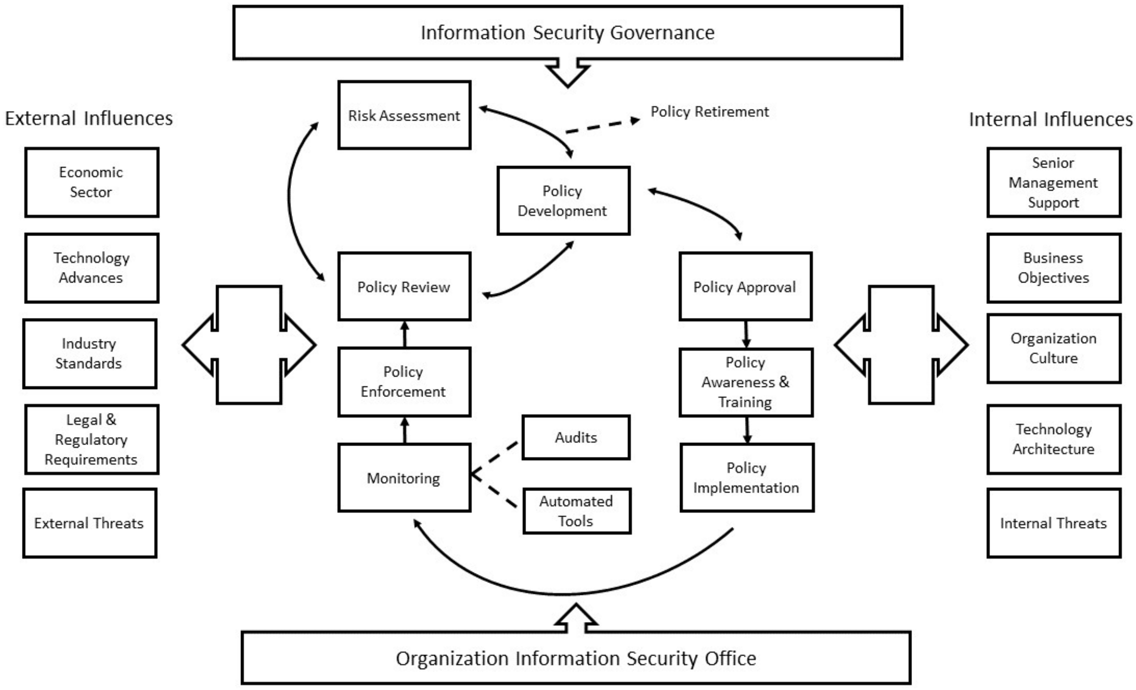


FIGURE 7 The Comprehensive Information Security Policy Process Model (Knapp, Morris, Marshall & Byrd 2009, 499)

Both models focus on the process nature of the security policy formulation and they have a lot of similarities. The biggest difference between the models is, that the CISPPM (Knapp et al., 2009) sees risk assessment as a somewhat distinct subprocess that can lead to the policy review without necessarily leading straight away to the policy development.

## 6.3 Stakeholders needed in the process of policy making

The development of an effective security policy should be conducted with a combination of different skills gained from different stakeholder expertise. The inclusion of many stakeholders in the development of the security policy is also crucial because it gives the whole organization the sense of ownership that can facilitate the acceptance and adoption of the policy. (Flowerday & Tuyikeze, 2016.) Next, the stakeholders needed in the process are introduced.

**Management**
One of the research findings of Flowerday and Tuyikeze (2016) was that management support plays a significant role in the success of the security policy (Flowerday & Tuyikeze, 2016). It means that the management is in a highly influential position when the security policy is being prepared. Maynard, Ruighaver and Ahmad (2011) have listed stakeholder groups in the process of developing a security policy. According to them, the involvement of senior management, in particular, is relevant to the success of any strategic initiative. Thus, the support and involvement of the management is also a key factor in the development and implementation of the information security policy. (Maynard, Ruighaver & Ahmad, 2011.)

**End-users**
In addition to user that is being seen as a natural person, such as an employee in an organization, users can also be seen to consist of groups of people with different tasks in the organization (Maynard et al., 2011). It is essential for end-users to be included in the early preparation of the information security policy. When end-users are offered the opportunity, they can take part of identifying the mistakes and difficulties of the security policy being prepared. At the same time, the users might be more committed to security measures by having an experience of ownership. (Flowerday & Tuyikeze, 2016.)

As a major part of the organization's security threats comes from internal actors in organizations (Mitnick et al., 2011), it is important to have the users engaged in security efforts. Engagement can be seen to cause a positive influence for the user's motivation to comply with security enforcement practices. By creating understandable, adoptable and usable security documents, for example, it is possible to reduce security breaches that are not caused of intentional behavior.

**Legal counsel**
Legal counsels are important because they provide information on existing laws and the anticipated legal requirements (Flowerday & Tuyikeze, 2016).

**Technical staff**
For the information security policy to be functional and effective, a number of issues needs to be taken into account, such as regulatory requirements, complexity of new technologies, and external and internal threats (Flowerday &

Tuyikeze, 2016). Technical staff members usually have technical knowledge that a security policy development team might be lacking. It would be beneficial for technical security specialists to be involved in the development of the security policy development primarily because of their expertise. (Flowerday & Tuyikeze, 2016.)

**Human resources**
Information security policy should be aligned with existing organizational practices. These can include, for example, the use of email, physical security and other topics defined in organization´s HR policy. To make sure that these policies are not conflicting, human resources department should also be a part of the information security development process. (Flowerday & Tuyikeze, 2016.)

**External representatives**
External representatives also play a role in the development of a security policy, especially when the activity of the stakeholders depends on organizational information systems (Flowerday & Tuyikeze, 2016). Recognizing the impact of the external stakeholders is also important if the organization cooperates with other organizations, for example in subcontracting.

## 6.4 ArchiMate as a tool for constructing

ArchiMate (The Open Group, 2017) is an Open Group standard, that offers an open and independent modeling language for EA. It is widely known and used in different consulting firms and supported by several tool vendors. The ArchiMate language consists of modelling elements that represents real life entities and of relationships between them. Active Structure Elements are entities that can perform behavior. Behavior Elements are units of activity that is performed by Active Structure Elements. Active Structure Elements perform behavior upon Passive Structure Elements. (Band, Engelsman, Feltus, Paredes, Hietala, Jonkers, Koning & Massart, 2017.)

The relationships between modelling elements can be categorized into four core sets. Structural relationships represent static construction or composition between the elements. Dependency relationships describe how the elements support other elements. Dynamic relationships are used to model behavioral dependencies between the elements. Outside these categorizations are the relationships of specialization and association. (Band et al., 2017.)

The ArchiMate language is also defining three main layers to work with. A Business layer can be used to model products and services of the described organizations. An Application layer can be used to model application services, realized by software applications, that serve the Business layer functionalities. A Technology layer provides infrastructure services realized by hardware and system software. Outside these core layers is a Physical layer that is an extension of the Technology layer. It adds structural and physical elements, like facilities, equipment and materials. (Band et al., 2017.)

In addition to these elements, there are also three other types of elements in the ArchiMate Specification. Motivation elements motivate enterprise design and operation. An Implementation and Migration elements can be used to model the implementation of all aspects of EAs, but also the migration between different generations of implemented architectures. Strategy elements support the planning and modelling of the business strategy and capabilities. (Band et al., 2017.) The structure of the ArchiMate language can be summarized in framework represented in FIGURE 8 (Band et al., 2017).

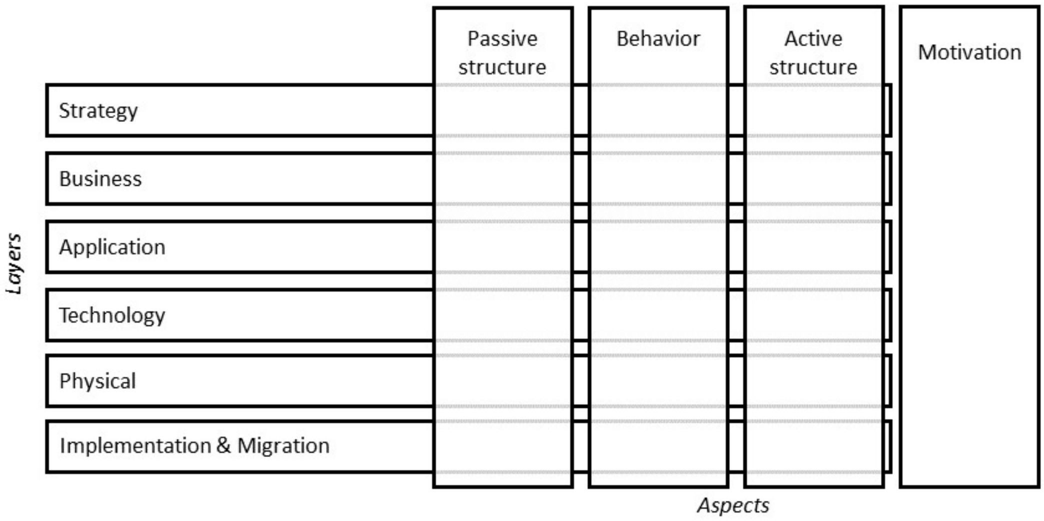


FIGURE 8 The Full ArchiMate Framework (Band et al., 2017, 20)

There are several reasons to model the method framework of EA security design principle constructing in the ArchiMate language. First, the ArchiMate is widely known and used in EA, so the concepts are likely to be familiar. Second, if the ArchiMate is used as a modelling language in an organization, it is possible to combine different views together and describe the dependencies between principle-related and other structures. That can, for example, be beneficial when measuring the impact and realization of the principle. Third reason is, that the ArchiMate is well aligned with different EA methods and frameworks, so the use of the ArchiMate does not set restrictions on the method used in an organization.

Fourth argument on behalf of using the ArchiMate is, that it already has a Principle element and elements related to the Principle. The Principle element can also benefit information security modelling as Grandry, Feltus and Dubois (2013) state: "[T]he security guidelines that are very common in the security domain […] can benefit from this modeling element." (Grandry, Feltus & Dubois, 2013). The Principle element can also be aligned with the concept of policy: "At the design level, a policy may map to a principle from the ArchiMate Motivation elements. The ArchiMate language does not have the concept of operational policy" (Band et al., 2017).

There can also be some possible counter arguments for the use of the ArchiMate language as a modelling tool for the EA security design principle. As stated before, there should be several stakeholders involved in the principle construction. On one hand, the ArchiMate language can be somewhat difficult to understand for those stakeholders that are not familiar with it in advance. On the other hand, the stakeholders are not alone responsible for the principle development, because the principle is aimed to serve EA purposes. The role of the stakeholders is mainly to provide information and perspective and the role of an architect is to assemble the principle suitable for the EA purposes. That is why it can be argued that is not essential for the stakeholders to be familiar with the modelling language, but this unfamiliarity needs to be considered when co-operating with different stakeholders.

Second possible argument against the use of the ArchiMate language is, that there is a risk that it can drive the architecture development process to a direction, where models become unnecessary complicated. That can be the case if different models and views are combined without clear view of the purpose and target of the modelling efforts. Even though the principles developed should be comprehensive enough to consider all aspects of the architecture design, there needs to be clear understanding of the level of needed accuracy of the elements when developing the principle.

In this study, the Motivation aspect elements (The Open Group, 2017) are used as a language for the method framework modelling. Because the method framework introduces also a process for the EA information security design principle development, additional elements from the Business level of the ArchiMate are also used. TABLE 6 presents the ArchiMate elements used in the method framework.

TABLE 6 The ArchiMate Elements (The Open Group, 2017, 47 – 48, 68 – 69)

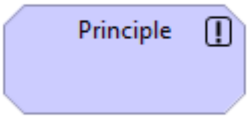
| ArchiMate 3.0.1 element | Definition of the ArchiMate element | Example of the ArchiMate element | Enterprise Architecture Information Security Design Principle Method Framework element | Content of the Enterprise Architecture Information Security Design Principle Method Framework element |
|---|---|---|---|---|
|  | A qualitative statement of intent that should be met by the architecture. | "Systems should be customer facing", "Customers should have a great experience" | Principle | EA information security principle |

TABLE 6 continues

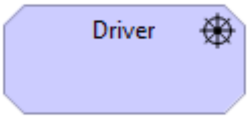
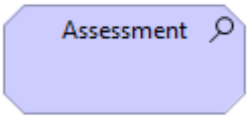
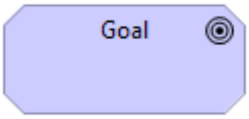
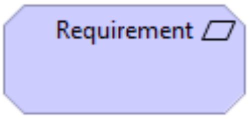
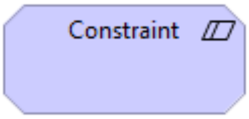
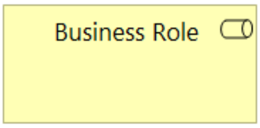
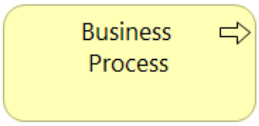
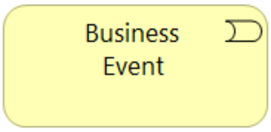
| | | | | |
|---|---|---|---|---|
|  | An external or internal condition that motivates an organization to set goals and implement changes. | Economic changes, Changing legislation, Increased competition | Concern | Changes in enterprise, Changes in legislation, Changes in economic sector, or Changes in technology |
|  | The outcome of an analysis of a Driver that may reveal strengths, weaknesses, opportunities, or threats. | "Complaining customers", "Leaving customers", "Long waiting queues", "High service times" | Threat | Internal threats, external threats |
|  | An end state that a Stakeholder intends to achieve or a direction a Stakeholder wants to move in. | Increase profit, reduce waiting times at the helpdesk, lower IT costs | Goal | Business objectives, IT objectives |
|  | A statement of need that must be met by the architecture. Requirements represent the "means" to realize goals. | "Assign personal assistant", "Provide on-line portfolio service", "Provide on-line information service", "Use open source software" | Requirement | Legal & regulatory requirements, Security standards, Industry standards, Business requirements |

TABLE 6 continues

| | | | | |
|---|---|---|---|---|
|  | A restriction (for example time or budget) on the way in which a system is realized. | "Application should be realized in Java", "Cost should be below budget", "iPad only version", "Must use MIT license" | Constraint | Business constraint, IT constraint |
|  | A Business Role performs internal behavior described in a Business Process. | Customer, Insurer, Supplier, Lecturer, Administrator, Buyer | Stakeholder | Legal Counseling, Technical Staff, HR, External Representatives, Management, Senior Management, End-users |
|  | A Business Process is a unit of internal behavior or collection of causally-related units of internal behavior intended to produce a defined set of products and services. | Receive request, Register, Pay, Create contract, Sign agreement | Process | Risk Assessment and risk analysis process, Evaluation, Construction, Implementation, Compliance, Monitoring |
|  | Business Processes and other business behavior may be triggered or interrupted by a Business Event. Unlike Business Processes, a Business Event does not have duration. | Request for Insurance, Claim Received, Application Form Received, Send Product Portfolio | Event | Need to design a to-be state |

The Enterprise Architecture Information Security Design Principle Method Framework elements and their contents, shown in the Table 5, are derived from the information security policy metamodels introduced in the chapter 6.2. Even though the method framework elements and the ArchiMate elements were very similar with their contents, some adjustments were needed. First, the Principle element in the method framework refers only to the EA information security design principle. Second, the ArchiMate Driver element is named Concern. Even though both elements have very similar definitions and contents, the Driver element refers also to positive drivers. In information security context, and based on the information security metamodels, it was more appropriate to delimit the element on concerns. Third, Assessment element of the ArchiMate is also delimited to threats. The assessment element in the ArchiMate is an outcome of an analysis of the Driver. Because the Driver was limited only on concerns, the Assessment includes only the threats and not, for example, strengths and opportunities. Fourth, Business Role was defined as Stakeholders.

All the changes for the ArchiMate language served the purpose of focusing and delimiting the elements to suite better for the information security context. No changes to the meaning of the Elements were needed.

To be able to model the process of the principle development and also to be able to describe the relations between the Motivation and Business layer elements, the ArchiMate relationship elements (The Open Group, 2017) were used. TABLE 7 presents the relationship elements that were used in the method framework.

TABLE 7 The ArchiMate Relations (The Open Group, 2017, 34 – 35)

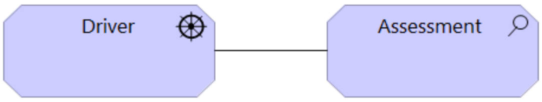
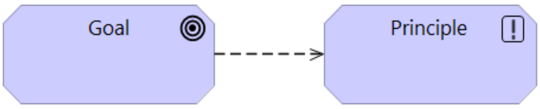
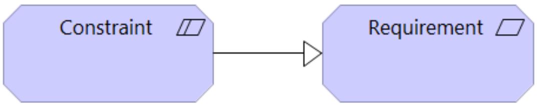
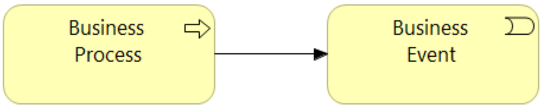
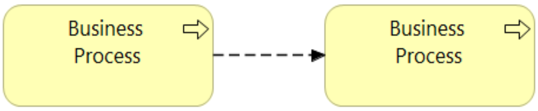
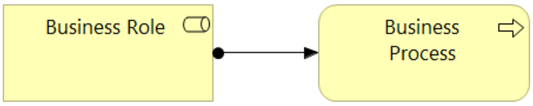
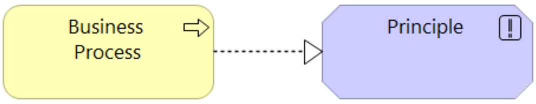
| ArchiMate 3.0.1 | Definition |
|---|---|
|  | The Association relationship models a relationship between objects that is not covered by another, more specific relationship. |
|  | The Influence relationship is used to describe that some motivational element may influence (the realization of) another motivational element. |
|  | The Specialization relationship indicates that an object is a specialization of another object. |

TABLE 7 continues

| | |
|---|---|
|  | The Triggering relationship describes the temporal or causal relations between processes, functions, interactions, and events. |
|  | The Flow relationship describes the exchange or transfer of information or value between processes, function, interactions, and events. |
|  | The Assignment relationship links active elements (e.g., Business Roles or Application Components) with units of behavior that are performed by them, or Business Actors with Business Roles that are fulfilled by them. |
|  | The Realization relationship links a logical entity with a more concrete entity that realizes it. |

The first version of the method framework (FIGURE 9) was designed by combining the metamodels of the enterprise architecture principle development and the metamodels of the information security policy development. After the development of the first version, the method framework was evaluated with the expert interviews. The next chapter presents the evaluation process and the changes to the method framework.

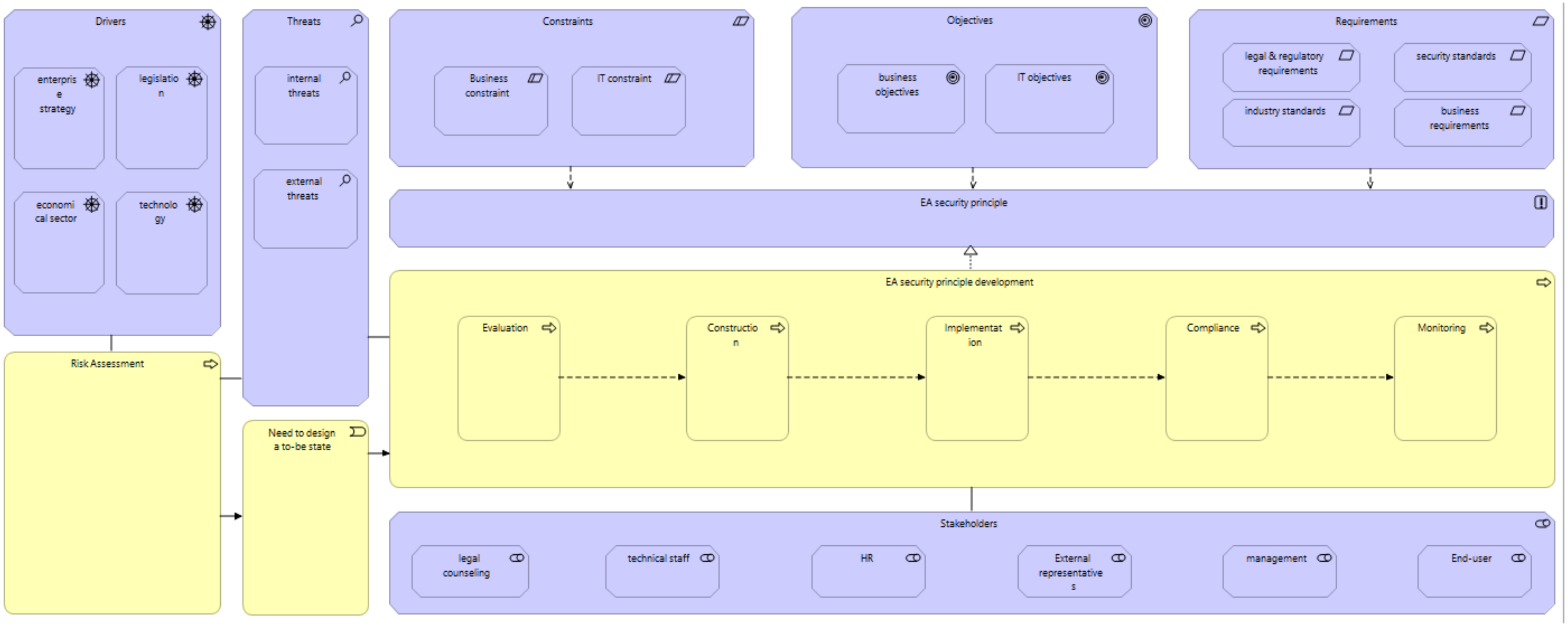


FIGURE 9 The First Version of the Method Framework

# 7 EVALUATION OF THE METHOD FRAMEWORK

The method framework was evaluated with expert interviews as described in chapter 5. To be able to determine the themes for the interviews, a Shell model (Tolvanen, 1998) was chosen to analyze what knowledge the method framework should include. In the Shell model (FIGURE 10), methods are based on concepts and their interrelations.

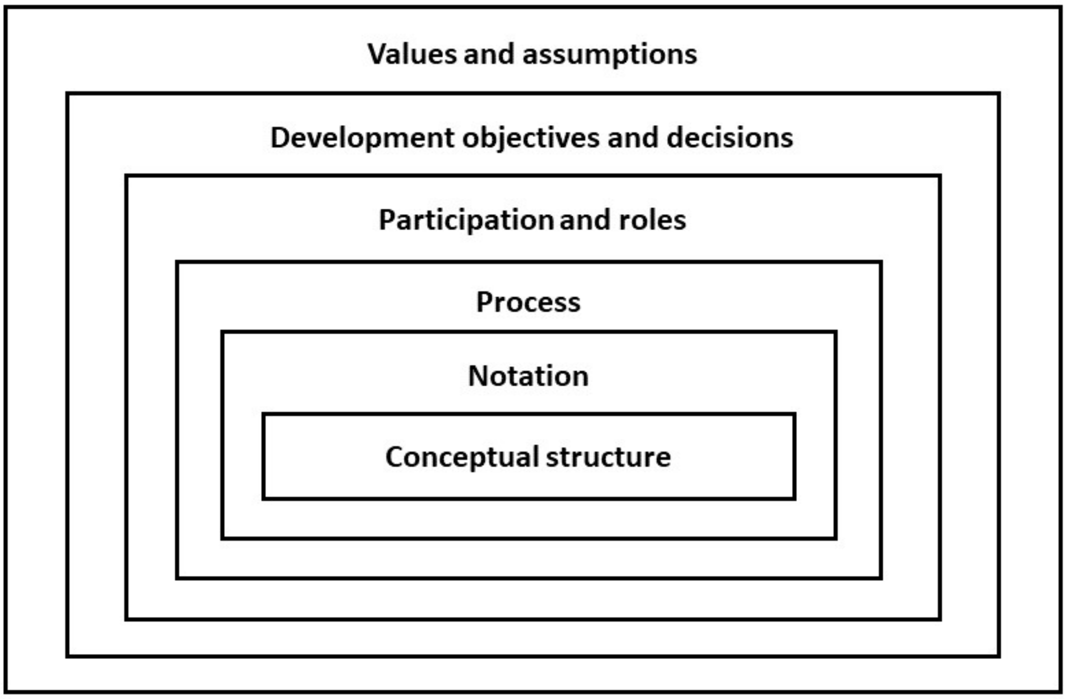


FIGURE 10 The Shell Model of Method Knowledge (Tolvanen, 1998, 35)

The conceptual structure is the basis for other types of method knowledge. Some of the concepts are applied directly in notations, some are related to the process, and some to the design objectives. (Tolvanen, 1998.) In this study, concepts of the method framework were adapted from the Information Security

Policy metamodels, the EA Principle metamodels and the ArchiMate notation. There are potential problems related to an approach where concepts are adapted from various sources. Main problem that can arise, is that concepts in different methods vary because of differences in domain and levels of rigor (Tolvanen, 1998). This is one aspect that should be considered in evaluation of the method framework.

When defining concepts as a part of the conceptual structure, they must be discussed and represented by using a notation. Association between notation and conceptual structure defines the semantics. This means that every notational construct must be a part of the conceptual structure. In an ideal situation, there is only one notational representation for each construct. (Tolvanen, 1998.) When using the ArchiMate as a notational representation, this can lead to some challenges. Because the method framework is constructed from concepts adapted from distinct sources, some alterations for the ArchiMate notation were needed. It means that same ArchiMate concept carries two different meanings in the method framework. This was noticed during the first two interviews. The interviewees had some difficulties to came over the ArchiMate notation and be able to understand the conceptual differences between ArchiMate concepts and concepts of the method framework. To overcome this challenge, the method framework was later represented in a different form.

Processes define in what order and in what way the techniques need to be used to produce methods. Processes must be based on the conceptual structure of the method to be useful. (Tolvanen, 1998.) To cover the process aspect of the model, the development process of the method framework was divided into subprocesses. Because the model should cover the needs of different organizations in distinct fields and sizes, the subprocesses were not modelled in detail.

Participation and roles were adapted from both information security and EA fields. It has been emphasized, that most methods do not describe organizational structures that are related to method use or roles (Tolvanen, 1998). To be able to cover the various aspects of an organization, there must be multiple stakeholders involved.

Development objectives are general statements of what types of solutions are considered desirable. Development decisions are more explicit and related to the use of the method. (Tolvanen, 1998.) Because of the objective of generalizability of the method framework, it does not give explicit guidelines for how it should be implemented in an organization. That is why the interviewees were asked to consider the suitability of the method framework in the context of their own organization.

Most of the methods do not explicitly define the assumptions or values, even though methods are always based on some underlying assumptions (Tolvanen, 1998). In this study, the basic assumption in the method framework development was that the EA, and especially the EA design principles, can be a beneficial approach to information security issues.

To be able to determine the themed interview questions, the method framework was analyzed based on these types of method knowledge. The results are represented in TABLE 8 with examples and interview questions derived.

TABLE 8 The Evaluation Questions

| Type of Method Knowledge | Examples | Questions |
|---|---|---|
| **Values and Assumptions** | EA is a beneficial approach to information security issues<br>EA principles and information security policies share similar approaches, goals and levels of abstraction to be treated together to develop an information security principle | Are the assumption correct?<br>Are the assumptions relevant for the issue?<br>Are there any other assumptions to be considered? |
| **Development Objectives and Decisions** | To make a method for EA information security design principle development | Could it be possible to develop an efficient EA information security design principle with the method presented?<br>Are the development decisions coherent? |
| **Participation and Roles** | Legal counseling<br>Technical staff<br>HR<br>External representatives<br>Management<br>End-user | Are there a stakeholder missing or too much? |
| **Process** | EA principle development and security principle development combined | Are the development sub-processes in a right order?<br>Are the sub-processes divided correctly?<br>Are there something missing or too much? |
| **Notation** | ArchiMate | Are the notational constructs understandably and correctly related to the concepts used? (fidelity, completeness, only one construct per concept)<br>Is the model clear enough to be understood? |
| **Conceptual Structure** | ArchiMate and Policy Development Frameworks | Are the concepts used meaningful and sufficient?<br>Are the relations between concepts meaningful and sufficient?<br>Is there something missing or too much?<br>Is the level of details adequate for the method to be used in various kinds of organizations? |

The evaluation of the method framework was conducted in two iterations. After the first interview round, there were minor changes made for the method framework (FIGURE 11). During the second interview round, the interviewees were asked to evaluate both of the models to survey the validity of the modifications. All the interviewees agreed, that the modifications were correct. The main modifications for the method framework were related to the representation. The first round interviewees stated that the ArchiMate symbols might be confusing if the notation is not known beforehand. As a result, the second round interviewees were also shown a more communicative method framework (FIGURE 12) that was not drawn with the actual ArchiMate symbols. The second round interviewees were also shown the ArchiMate drawn version of the method framework.

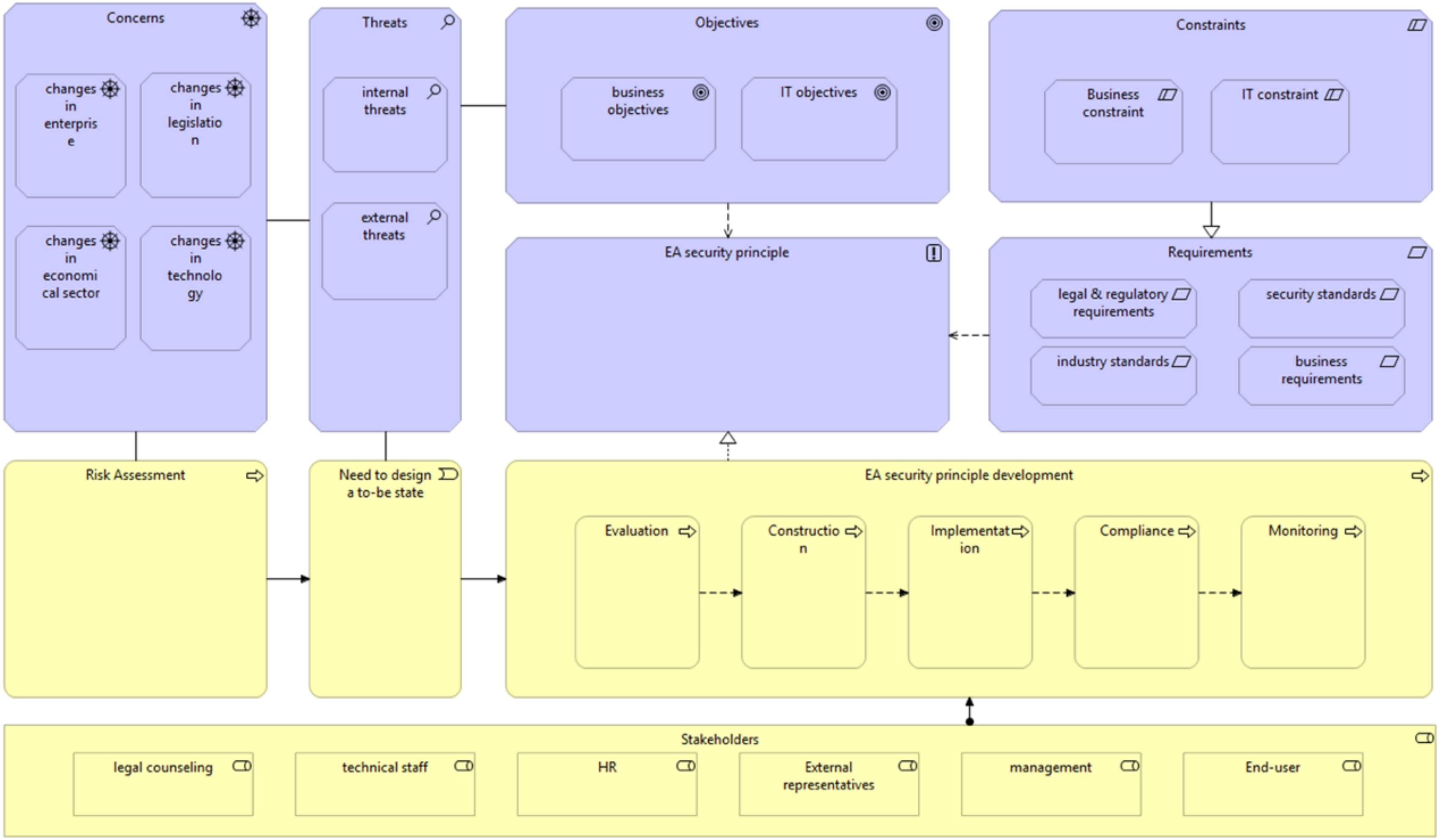


FIGURE 11 ArchiMate version of the Method Framework after the First Iteration

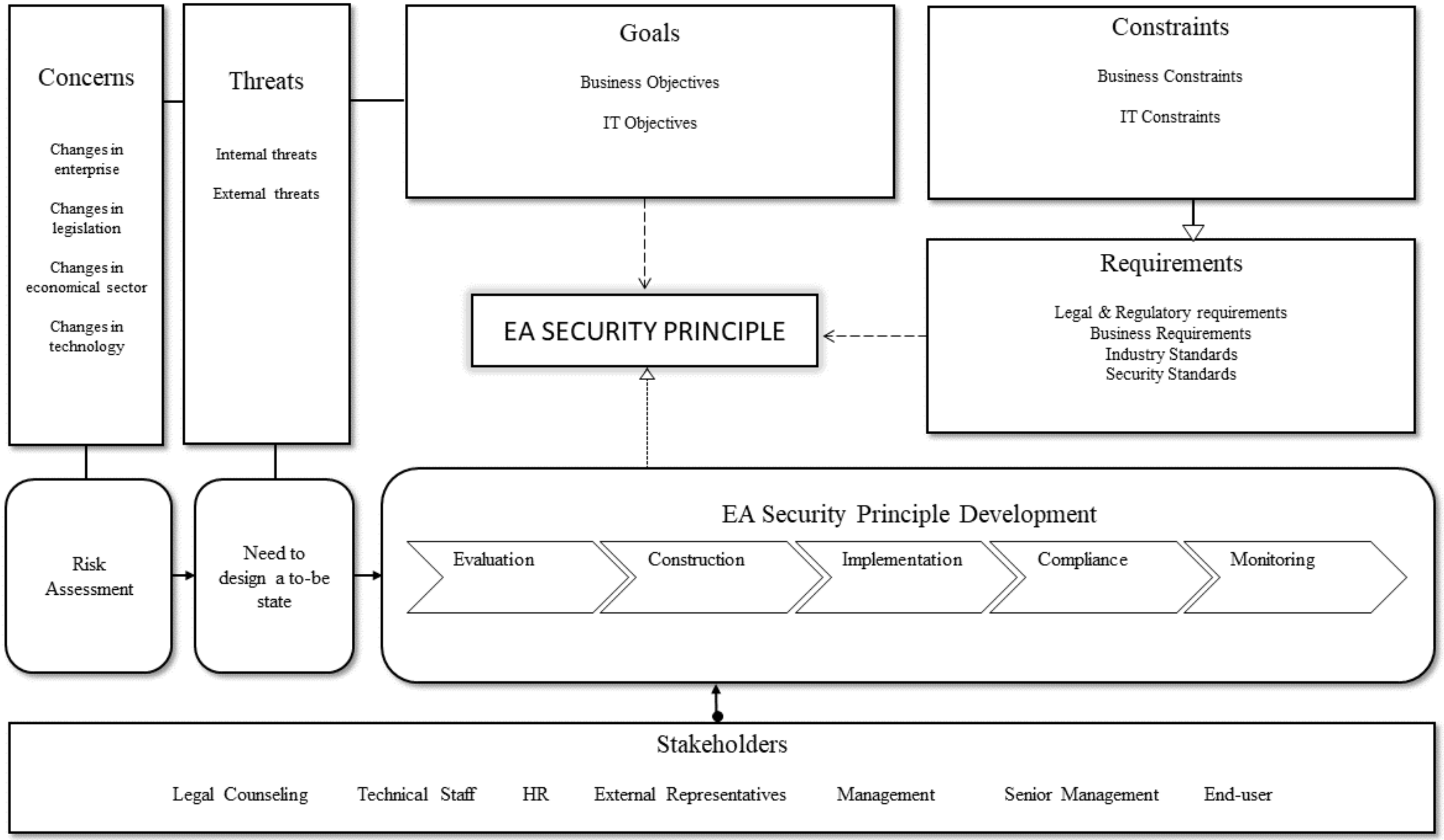


FIGURE 12 The Method Framework after the First Iteration

# 8 RESULTS

## 8.1 Results of the Evaluation

The results of the evaluation in the interview round 1 are presented in the TABLE 9. A plus sign in the table indicates that the interviewee had no opinion or no suggestions of improvement for the matters of that specific method knowledge type.

TABLE 9 The Results of the Evaluation in the Interview Round 1

| INTERVIEW ROUND 1 | | | | |
|---|---|---|---|---|
| TYPE OF METHOD KNOWLEDGE | Informant 1 | Informant 2 | Informant 3 | Informant 4 |
| Values and Assumptions | + | + | + | + |
| Development Objectives and Decisions | + | + | + | + |
| Participation and Roles | + | There are also threats that could come from the stakeholders, which should be included in the model. | + | + |

TABLE 9 continues

| INTERVIEW ROUND 1 | | | | |
|---|---|---|---|---|
| TYPE OF METHOD KNOWLEDGE | Informant 1 | Informant 2 | Informant 3 | Informant 4 |
| Process | The tool is right, but its implementation could be difficult. There is a risk that information security ends up guiding business activities. | Principles are not enough to guide an organization by themselves. There needs to be more specified guides and instructions. It can also be difficult to recognize the needed factors in an organization. | Method covers well the crucial elements, like risk assessment, that should be considered. | Suitability needs to be tested in case studies. |
| Notation | Some of the ArchiMate elements are not used as in their specification. | Some of the ArchiMate elements are not used as in their specification. | + | + |
| Conceptual Structure | Concepts are far away from one another so there should be additional layers between the concepts. Concepts should be more specified. | Abstraction level is detailed enough. | It can be difficult to make means of measuring because the abstraction level is high. | The level of abstraction is suitable for diverse kinds of organizations. Both objectives and constraints should define requirements. The process should be named development and deployment process instead of development process. |

The results of the evaluation in the interview round 2 are presented in the TABLE 10. A plus sign in the table indicates that the interviewee had no opinion or no suggestions of improvement for the matters of that specific method knowledge type.

Next, the results of the evaluation are presented by method knowledge types and the suggestions of improvements are analyzed.

TABLE 10 The Results of the Evaluation in the Interview Round 2

| INTERVIEW ROUND 2 | | | | | |
|---|---|---|---|---|---|
| TYPE OF METHOD KNOWLEDGE | Informant 5 | Informant 6 | Informant 7 | Informant 8 | Informant 9 |
| Values and Assumptions | + | + | + | + | + |
| Development Objectives and Decisions | + | + | It is difficult to make an efficient method with high abstraction level. | + | + |
| Participation and Roles | Leadership should be also covered in stakeholders , because it is a different stakeholder than management, but also crucially important. | + | + | + | Chief level roles should also be covered in stakeholders. |
| Process | There are all the needed aspects from the information security point of view. Balanced Score Card could be a tool to recognize needed factors. Also, SWOT-analysis could be useful with the model. | Model suits better for slow changes and improvements, not necessarily for rapid changes in an organization. | There should be more specific guidelines in the model to make it suitable in practical implementation. | Implementation is crucial but also problematic. Both management and EA actors should support the efforts. There is a risk that principles are just a bunch of paper somewhere on a shelf. | The process should be presented as a loop where monitoring leads back to constructing. It should be a continuous process. |

TABLE 10 continues

| INTERVIEW ROUND 2 | | | | | |
|---|---|---|---|---|---|
| TYPE OF METHOD KNOWLEDGE | Informant 5 | Informant 6 | Informant 7 | Informant 8 | Informant 9 |
| Notation | + | + | The model is difficult to understand without written explanations. | Accuracy of the ArchiMate notation is not important. The most important thing in describing is that it supports communication as much as possible. | + |
| Conceptual Structure | Abstraction level is suitable for the purpose. | The level of details does not cover two-speed IT but is suitable for slow changes. The model claims that a risk assessment could be done without the knowledge about possible threats. | Abstraction level is too high, so it is impossible to find proper elements from the organizational context with the model. | When implemented, one should think about the hierarchical model and examples of what level of things are in different concepts. Two-speed IT should also be considered. | Legislation is not only a requirement. It can also be a constraint. Risk assessment is not enough alone. Also risk analysis must be conducted. It should be written in the model. |

**Values and assumptions**

All interviewees agreed that EA is a usable starting point when managing information security in an organization. Information security should be integrated in all aspects of an organizations instead of being covered only by system features. Business functions, information systems and information security should be all aligned and managed together. EA is a beneficial approach to that.

### Development Objectives and Decisions

One of the interviewees pointed out that the method framework was too general to be useful in the EA information security principal development and that is why it is not possible to develop an efficient EA information security principle with the method framework. To be useful, it needs more details and the level of accuracy should be grater.

The abstraction level of the method framework is high because it is supposed to be generic enough to be used in organizations differing with size, business field and other characteristics. It can though be pointed out that the method framework might need adjustment within the organization to be suitable for the purpose.

### Participation and Roles

All the stakeholders identified were found to be correct. Two of the interviewees pointed out that there were chief level roles missing in the method framework. In addition to management level, also chief level should be included. Chief level support was valued as a crucial factor both in EA and information security implementation.

It was also stated that stakeholders can realize risks and that aspect should be integrated into the method framework. Because of the generic nature of the method framework, risks were presented only as internal and external risks without further separation. It can be pointed out that stakeholders can be both internal and external and are implicitly included in both categories.

### Process

The main phases of the process were found suitable. However, there were some concerns regarding the three last phases of the process. It was stated that implementation of the principle developed can be difficult in an organization. There is a risk that principles are constructed, but they are treated as a distinct area and never meet the practice of EA. There was also concerns regarding the monitoring of the principle. It can be challenging to find the suitable measurements and ways of monitoring.

The recognition of the organizational factors needed for the development of the principle can also be difficult. It depends on the maturity of organizations EA and on how appropriately organization's as-is state is described. To recognize the factors needed, Balanced Score Card and SWOT-analysis were proposed as information resources (Informant 5) There can also be other documents in an organization that might be important sources of information. For example, information security policies and guidelines can be useful for the purpose. One of the interviewees pointed out that here is also a risk that information security ends up guiding the business functions instead of supporting the achieving of business goals or being aligned with all aspects of an organization. The use of multiple documentations might also help preventing this threat.

It was also stated that the process should be more precise to be able to guide the development. All the sub-processed should be described in detail, because the principles as themselves are not enough to guide the organizations

EA efforts. There should also be more specified guides and instructions derived from the principles.

Concerns presented above should be considered when conducting the process. However, to be able to keep the model generic, modifications to the process were not made based on these.

It was pointed out that he development process should be iterative. After monitoring phase, there should be an iteration back to the evaluation phase of the process.

### Notation

The use of ArchiMate notation was mainly found suitable for the purpose. The first two interviewees suggested that the model could be more communicative if drawn without the actual ArchiMate blocks. Because of their suggestion, a more generally understandable model was drawn, and both versions were shown to following interviewees.

The first two interviewees also criticized the use of Driver elements. That is why one of the Drivers were modified to be more generic and named differently. Instead of seeing only enterprise strategy as a Driver for change, all organizational changes were included.

As it is stated in the ArchiMate notation, Driver "represents an external or internal condition that motivates an organization to define its Goals and implement the changes necessary to achieve them" (The Open Group, 2017). Based on that, it is reasoned to use Driver elements to represent changes. In ArchiMate notation, internal Drivers are often called Concerns. In the model, also external Drivers are treated as Concerns.

### Conceptual Structure

Some of the interviewees pointed out that the difference between levels of abstraction is too great and there should be additional layers between the concepts. One of the interviewees also commented that it is difficult to use the method framework and find the right organizational elements because the method framework is too abstract. High abstraction level can also make it difficult to find proper means of measuring to evaluate the suitability of the method framework. It was also suggested that when implemented, the hierarchical level should be considered to determine, what kinds of organizational matters belong to which element. Within the scope of this work, it was not possible to test the method framework in case studies. That is why it was not possible to lower the abstraction level or to construct additional layers between the elements. This is a topic that remains for further development.

Two of the interviewees pointed out that the method framework is more suitable for slow changes in an organization. There are several issues to be considered when developing an EA information security design principle with the model. When implementing rapid changes, the means are more agile. In the context of rapid organizational changes, it is not possible to consider all the issues needed, because implementation is conducted more in a trial and error manner. To be able to evaluate the suitability of the method framework for two speed IT, case studies are needed.

There were also some suggestions for improvement related to contents. It was suggested that the risk assessment should also include the risk analysis. Even though the model does not take a stand for the ways of conducting the risk assessment, risk analysis is crucial phase when resolving the possible impacts of a risk. That is why risk analysis was included in the method framework.

Second content related issue was the naming of the process. The process has also a deployment aspect along with the development. That is why deployment was included in the naming.

Some modifications regarding the relations of concepts were also suggested. First, both Objectives and Constraints should define Requirements. To modify the model to be more aligned with ArchiMate specification, the term Objective was change to Goal and the relation between Goals and Requirements were changed as suggested.

Risk assessment needs the knowledge of possible threats. That is why a relation between Threats and Risk assessment process was added.

## 8.2 The Method Framework

The final version of the method framework was designed based on the evaluation results presented above. The final versions of the method framework of EA information security design principle development is displayed in the FIGURE 13 and FIGURE 14.

The implementation of the method framework starts with the left side of the figure. An organization might have some concerns arising from changes in the organization itself, in economic sector, in legislation or in technology. Identified changes needs to be analysed trough a risk assessment and risk analysis process. The model does not take a stance on the process itself, because the means and desired goals of the risk assessment and analysis might be organization specific.

The concerns might cause threats that are identified through the risk assessment and analysis process. The identification of a threat does not automatically lead to a need to create EA information security design principles. It is possible that the organization already has functional principles with which the needed changes for the to-be state of the organization can be conducted. It is also possible that the threat does not lead to a need to modify the to-be state of the organization. However, if the threat might have a negative influence on the goals of the organization, and it is assessed that the risk needs to be managed, the risk assessment and analysis process triggers a need to design a to-be state for the organization. That triggers a process of EA security principle development and deployment.

EA security principle development and deployment process starts with an evaluation. The business and IT objectives of the organization needs to be identified along with the business and IT constraints. Both objectives and constraints specify some of the requirement the principle must meet. Even though the requirements can be treated as a specification of the constraints, the requirements need also be derived from the organizational goals. There might also be requirements that are not constraints, even though the requirements can also set conditions for the principle. The requirements can come from legislation, regulations or standards. Also, there might be some requirements that the business and the field of the business sets.

Second subprocess in the EA security principle development and deployment is a construction. Based on the requirements, an EA information security design principle or principles are derived. It is noteworthy that all the subprocesses of the EA security principle development and deployment process needs to be conducted with several stakeholders. The stakeholders needed are presented in the chapter 6.3.

The next two steps are the implementation and compliance of the principle. The implementation and compliance also need to be monitored. That means that to find out if the principle designed for the purpose is right and functional, there needs to be some means of monitoring. The method does not take a stance on monitoring methods. It is however recognized, that this phase might be the most challenging one to conduct. It is difficult to find proper means to monitor the efficiency and suitability of a principle for the purpose. To find out, if there might be some general indicators or if the indicators should be designed organization specific, more research is needed.

The process of EA security principle development and deployment is done iteratively. This means that the results of the monitoring can lead back to the evaluation of the requirements but also back to construction phase where the principle can be modified to meet the requirements better.

In an ideal situation, the risk assessment and analysis process and the EA security principle development and deployment process are both conducted continually in the organization.

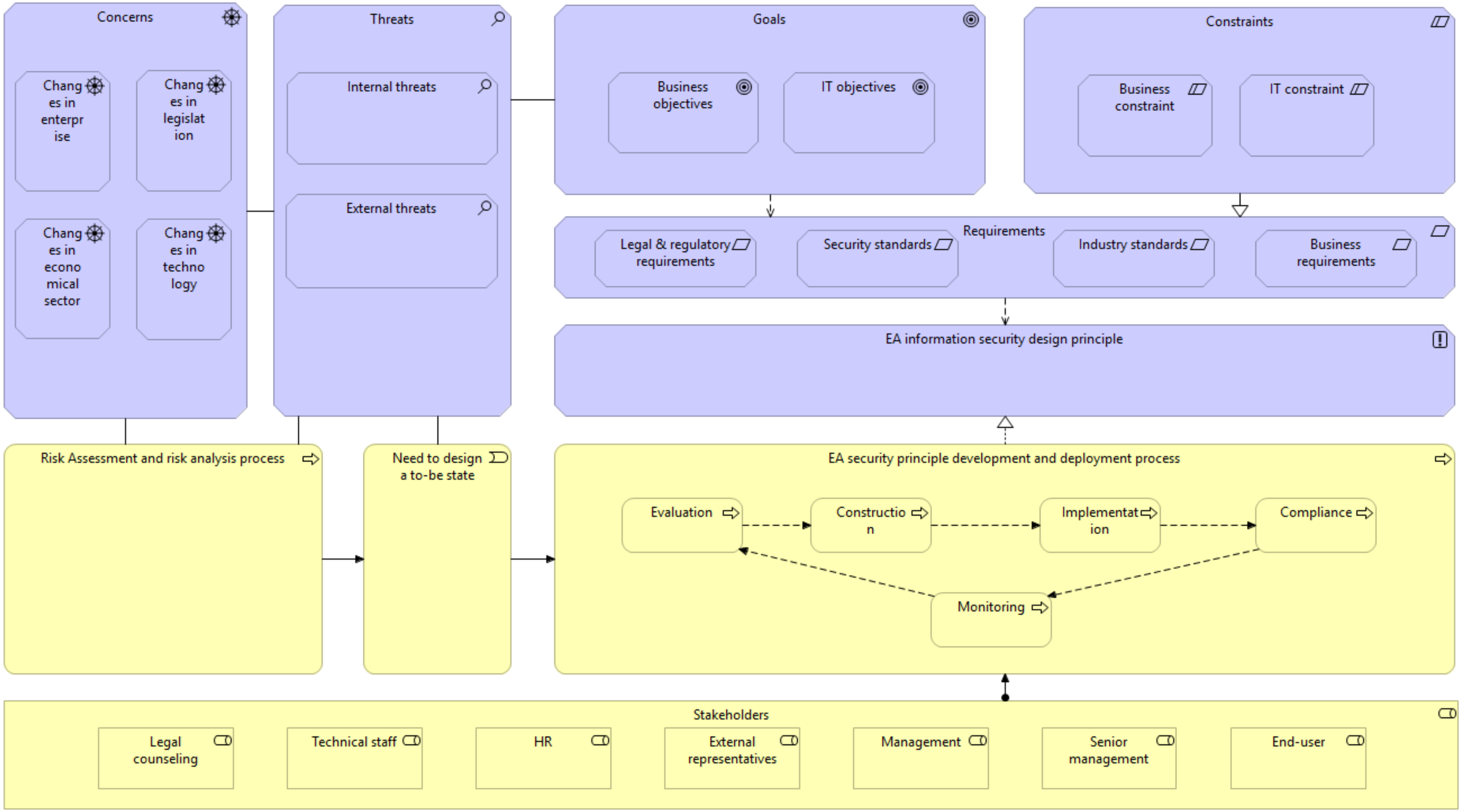


FIGURE 13 The ArchiMate version of the Method Framework of EA Information Security Design Principle Development

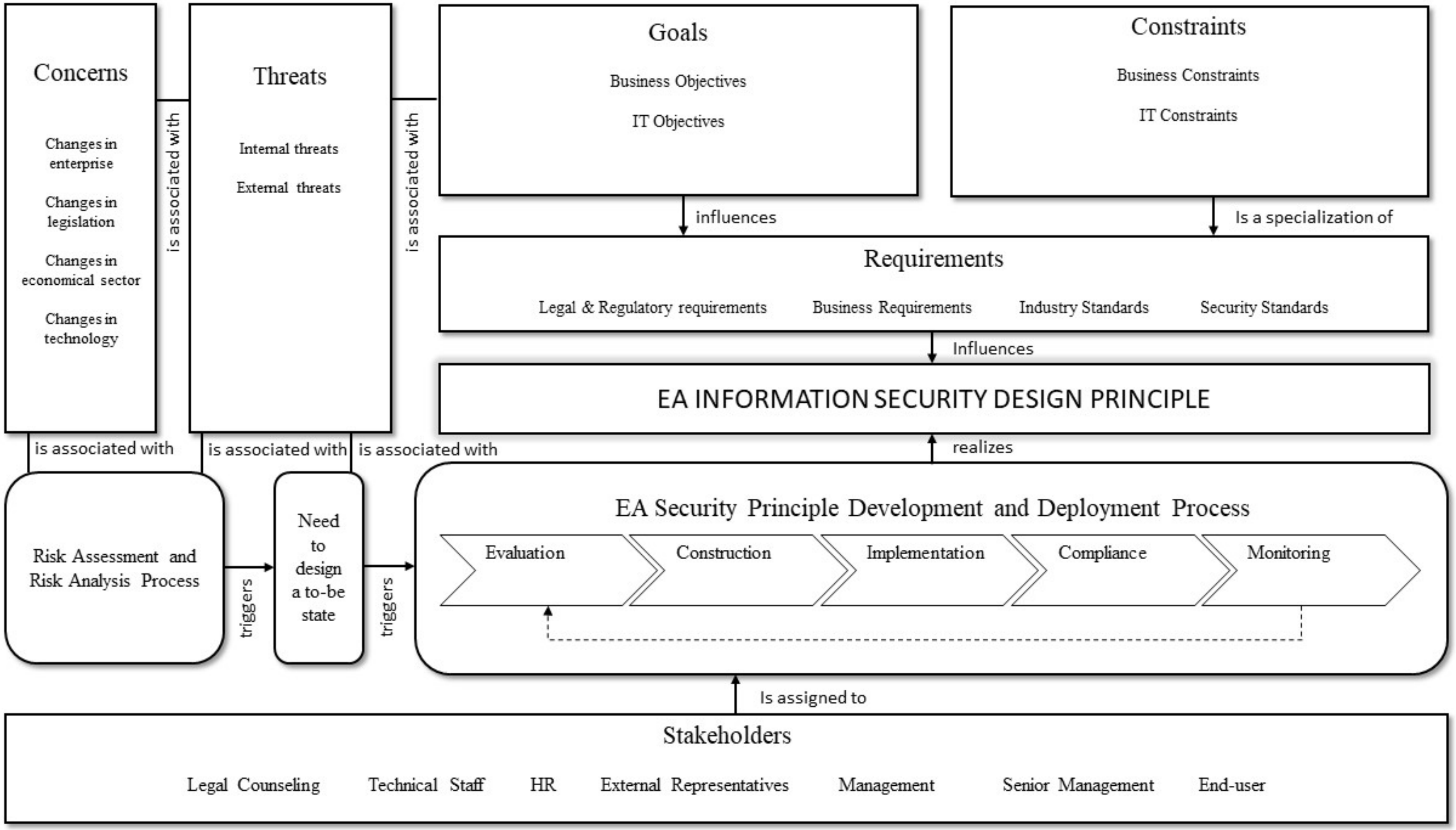


FIGURE 14 The Method Framework of EA Information Security Design Principle Development

# 9 LIMITATIONS AND FURTHER RESEARCH

One of the limitations of this study is the lack of testing the method framework in real life situations. The evaluation of the method framework was conducted with interviews, but the suitability was not tested in practice. The evaluation and further development of the method framework needs case studies, where the method framework can be evaluated in real life situations. As it is, the method framework is very generic because it is supposed to cover the context of different kinds of organizations. As was pointed out in the interviews, there might be some factors common with different organizations which have not been taken into account in the method framework. For example, successful implementation demands communication and the support of the upper management in every organization.

To determine the objectives of the solution, a pre-gathered interview material was used. Even though the material covered issues regarding information security in EA, it was not the focus of the material. That is why some of the interviewees answered the information security related questions quite superficially. Even though the interviews varied regarding the handling of the information security issues, all the themes that were found came forth in multiple interviews.

To evaluate the method framework, expert interviews were conducted. Even though most of the interviewees had expertise in both the information security and the EA fields, some of the interviewees had expertise only in either one field and the knowledge of the other field was thin. All the interviewees were Finnish and working currently in Finland, which can also bias the results.

In the future, the method framework needs to be tested with case studies. In literature, the quality criteria of EA principles are usually treated from the point of view of a full set of principles. This means that the completeness of the set is an important criterion for the quality (Marosin, Van Zee & Ghanavati, 2016). To be able to estimate if the EA information security design principle defined is aligned with other EA principles used in a given case, it is possible to use the requirements defined by Marosin et al. (2016). Marosin et al. (2016) present a set of five requirements for a good set of EA principles:

1. **Understandable**

   Each principle should be unambiguous, robust and specific. That means that they should be precise enough to be understood easily to guide a consistent decision making also in complex and controversial situations.
2. **Complete**

   The authors state that the completeness refers to two aspects: if the principles are relevant to the organization and if all the necessary principles are defined.
3. **Consistent**

   Principles should be aligned with each other so that following of a principle should not conflict the goal of another principle.
4. **Measurable**

   There should be means to measure if EA principles are followed and if they have an impact on the goals of the organization.
5. **Stable**

   Even that principles should be stable, they also should have methodology of changing the set of principles if the strategy or goals of the organization changes, principles are conflicting with one another or principles are constantly violated. (Marosin et al., 2016.)

To be able to estimate the functionality of the method framework, a set of principles needs to be defined with the method framework and estimated as a whole set aligned with other EA principles of each organization chosen for the case studies.

Another topic for future research is to study how operational the method framework presented is with different EA methods. Because ArchiMate is widely used with different EA methods, it is presumable that the method framework can also interact with different EA methods.

# 10 CONCLUSIONS

Objective of this study was to create a method framework that integrates the EA and the information security. The assumption, that the development of the method framework should start from the principle level, was supported with the expert interviews.

The starting point of the work was to combine the metamodels of the EA design principle development and the metamodels of the information security principle development. Design Science Research Methodology was found to be the most suitable mean for the purpose and Design Science Research Process was conducted in the study. Problem identification, Motivation and Objectives for the method framework came from interviews originally gathered for the VARKIT2 research (for further information, see Chapter 4). Main findings were, that information security should be included in every aspect of the EA work, including the EA principles level. EA was seen as an effective way to dismantle silo mentality in the information security field and to deal with the legislative demands affecting the information security work. It was also stated that risk management should not be only a responsibility of the information security, but also be included in the different EA methods. Literature sources showed similar results.

Even though the metamodels for the EA design principal development had a high abstraction level and gave only a little guide for the method framework design, they were in line and combinable with the information security principle development metamodels. All the elements in the metamodels were also describable in the ArchiMate language.

Development of the method framework was conducted in two iterations. Main critique considered the adaptability. The abstraction level was seen rather high, so it was somewhat difficult for some of the experts interviewed to evaluate the suitability of the method framework. Because the method framework needs to be applicable in different organizations, it cannot be too detailed. That is why it needs some further evaluation in real life situations. It is also possible that the method framework could be evaluated in to a more practical method or model.

The principle approach was seen right for integrating the information security in to the EA and the model itself needed only some minor modifications. In the discussions with the experts, one of the significant statements were related to the presentation of the method framework. To make it more communicative, the model was represented in ArchiMate symbols, but also in a more communicative way. The communication aspect also divided the interviewees opinions. Some were stating that the most important purpose of the method framework is to be a mean of making different aspects visible for the stakeholders involved. Some were more interested to estimate the suitability of the model in different EA methods. The latter aspect needs more research in the future.

Based on the expert interviews and literature sources, the need for a more seamless integration of the information security and the EA work was recognised. Because the current efforts to combine those two are seen difficult and laborious, principle level approach could be a reckoned starting point, because instead of several different guidelines and instructions, the principle level offers more holistic approach.

# REFERENCES

Aier, S., Fischer, C. & Winter, R. (2011). Construction and Evaluation of a Meta-Model for Enterprise Architecture Design Principles. *Proceedings of the 10th International Conference on Wirtschaftsinformatik WI 2.011. Volume 2. 16-18 February 2011* , (November 2015), 637–644. Retrieved from www.wi2011.ch

Armour, F. J., Kaisler, S. H. & Liu, S. Y. (1999). A big picture look at Enterprise Architectures. *IEEE IT Professional*, *1*(1), 35–42. https://doi.org/10.1109/6294.774792

Band, I., Engelsman, W., Feltus, C., Paredes, S. G., Hietala, J., Jonkers, H. & Massart, S. (2014). Modeling Enterprise Risk Management and Security with the ArchiMate Language. *Open Group*, 40.

Band, I., Engelsman, W., Feltus, C., Paredes, S. G., Hietala, J., Jonkers, H., Koning, P. & Massart, S. (2017). How to Model Enterprise Risk Management and Security with the ArchiMate Language. *Open Group*.

Barateiro, J., Antunes, G. & Borbinha, J. (2012). Manage risks through the Enterprise Architecture. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3297–3306. https://doi.org/10.1109/HICSS.2012.419

Baskerville, R. & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337–346. https://doi.org/10.1108/09576050210447019

Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal*. https://doi.org/10.1080/19393555.2011.629341

Charmaz, K. (1996). The Search for Meanings- Grounded Theory. *Rethinking Methods in Psychology*, 27–49. https://doi.org/10.1016/B978-0-08-044894-7.01581-5

Cram, W. A., Proudfoot, J. G. & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Dang, D. D. & Pekkola, S. (2017). Systematic Literature Review on Enterprise Architecture in the Public Sector. *Electronic Journal of e-Government*, *15*(2).

Ertaul, L. & Sudarsanam, R. (2005). Security Planning Using Zachman Framework for Enterprises. *Proceedings of EURO mGOV*, 153–162. https://doi.org/10.1.1.217.8967

Fischer, C., Winter, R. & Aier, S. (2010). What Is an Enterprise Architecture Principle? *Computer and Information Science 2010*, (Ieee 2000), 193–205. https://doi.org/10.1007/978-3-642-15405-8_16

Flowerday, S. V. & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers and Security*, *61*, 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Goel, S. & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, *19*(4), 281–295. https://doi.org/10.1016/j.jsis.2010.10.002

Grandry, E., Feltus, C. & Dubois, E. (2013). Conceptual Integration of Enterprise Architecture Management and Security Risk Management. In *2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops*. https://doi.org/10.1109/EDOCW.2013.19

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642.

Hevner, A., March, S., Park, J. & Ram, S. (2004). Design Science Research in Information Systems. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hoogervorst, J. (2004). Enterprise Architecture: Enabling Integration, Agility and Change. *International Journal of Cooperative Information Systems*, *13*(3), 213–233. https://doi.org/10.1142/S021884300400095X

IEEE-SA Standards Board. (2000). IEEE Recommended Practice for Architectural Description of Software-Intensive Systems. *IEEE Std*, *1471–2000*, 1–23. https://doi.org/10.1109/IEEESTD.2000.91944

Innerhofer - Oberperfler, F. & Breu, R. (2006). Using an Enterprise Architecture for It Risk Management. *ISSA*.

Jonkers, H. & Quartel, D. (2016). Enterprise Architecture-Based Risk and Security Modelling and Analysis, *9987*. https://doi.org/10.1007/978-3-319-46263-9

Josey, A. (2018). An Introduction to the TOGAF® Standard, Version 9.2.

Kaisler, S. H., Armour, F. & Valivullah, M. (2005). Enterprise Architecting: Critical Problems. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, *0*(C), 224b–224b. https://doi.org/10.1109/HICSS.2005.241

Kaisler, S. H. & Frank Armour, Ds. (2017). 15 Years of Enterprise Architecting at HICSS: Revisiting the Critical Problems. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4807–4816. Retrieved from http://scholarspace.manoa.hawaii.edu/bitstream/10125/41747/1/paper 0598.pdf

Knapp, K. J., Franklin Morris, R., Marshall, T. E. & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers and Security*, *28*(7), 493–508. https://doi.org/10.1016/j.cose.2009.07.001

Lemmetti, J. & Pekkola, S. (2012, September). Understanding enterprise architecture: perceptions by the finnish public sector. In *International Conference on Electronic Government* (pp. 162-173). Springer, Berlin, Heidelberg.

Lemmetti, J. and Pekkola, S., 2014. Enterprise architecture in public ICT procurement in Finland. Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP WG 8, pp. 227-236.

Lindström, Å. (2006). On the syntax and semantics of architectural principles. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *8*(C), 1–48. https://doi.org/10.1109/HICSS.2006.367

March, S. T. & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Marosin, D., Van Zee, M. & Ghanavati, S. (2016). Formalizing and modeling enterprise architecture (EA) principles with goal-oriented requirements language (GRL). *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9694*, 205–220. https://doi.org/10.1007/978-3-319-39696-5_13

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E. & Wieringa, R. (2018). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*. https://doi.org/10.1007/s10270-018-0661-x

Mayer, N. & Feltus, C. (2017). Evaluation of the risk and security overlay of archimate to model information system security risks. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, *2017–Octob*, 106–116. https://doi.org/10.1109/EDOCW.2017.30

Maynard, S. B., Ruighaver, A. B. & Ahmad, A. (2011). Stakeholders in security policy development. *Proceedings of the 9th Australian Information Security Management Conference*. https://doi.org/10.4225/75/57b546fecd8c6

Mitnick, K. D., Simon, W. L., Vartanian, F. R., Jaffe, S., Leventhal, C. & Mitnick, A. (2011). Controlling the Human Element of Security.

Niemi, E.I. and Pekkola, S., 2016. Enterprise architecture benefit realization: Review of the models and a case study of a public organisation. SIGMIS Database, 47(3), pp. 55–80.

Nightingale, D. & Rhodes, D. (2004). Enterprise systems architecting: Emerging art and science within engineering systems. *MIT Engineering Systems Symposium*, (March), 1–12. Retrieved from http://seari.mit.edu/documents/readings/ESD-Symposium-Enterprise-Systems-Architecting.pdf

Ostrowski, Ł., Helfert, M. & Hossain, F. (2011). A Conceptual Framework for Design Science Research. *10th International Conference Business Informatics Research, Riga; Lecture Notes in Business Information Processing Vol. 90*, 345–354. https://doi.org/10.1007/978-3-642-24511-4_27

Patton, M. (1990). Qualitative Evaluation and Research Methods. *Qualitative Evaluation and Research Methods*, 169–186. https://doi.org/10.1002/nur.4770140111

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Penttinen, K. (2018). The Long and Winding Road of Enterprise Architecture Implementation in the Finnish Public Sector. University of Jyväskylä: Jyväskylä Studies in Computing.

Penttinen, K. and Isomäki, H., 2010. Stakeholders' Views on Government Enterprise Architecture: Strategic Goals and New

Public Services. In Normann Andersen, K., Francesconi, E., Grönlund, Å. and van Engers, T., Eds., Electronic

Government and the Information Systems Perspective, Proceedings of the EGOVIS2010 Conference.

Richardson, G. L., Jackson, B. M. & Dickson, G. W. (1990). A Principles-Based Enterprise Architecture: Lessons from Texaco and Star Enterprise. *MIS Quarterly*, *14*(4), 385–403. https://doi.org/10.2307/249787

Seppänen, V., Penttinen, K. & Pulkkinen, M. (2018). Key Issues in Enterprise Architecture Adoption in the Public Sector. Electronic journal of e-government, 16(1).

Shedden, P., Scheepers, R., Smith, W. & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine*, *41*(2), 152–166. https://doi.org/10.1108/03055721111134790

Stelzer, D. (2009). Enterprise architecture principles: literature review and research directions. *Proceedings of the 2009 International Conference on Service-Oriented Computing*, 12–21. https://doi.org/10.1007/978-3-642-16132-2_2

The National Audit Office of Finland. (2017). Steering of the operational reliability of electronic services.

The Open Group. (2011a). The TOGAF® Standard, Version 9.1.

The Open Group. (2011b). TOGAF ® and SABSA ® Integration, (October), 1–58. Retrieved from https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12449

The Open Group. (2016). Open Group Guide Integrating Risk and Security within a TOGAF ® Enterprise Architecture. *Security Forum (a Forum of The Open Institute Group)*. Retrieved from https://www.hva.nl/binaries/content/assets/serviceplein-a-z-lemmas/media-creatie-en-informatie/hbo-ict/competenties/hbo-competenties-ict-opleidingen_7september2015.pdf

The Open Group. (2017). ArchiMate® 3.0.1 Specification.

Tolvanen, J. P. (1998). *Incremental method engineering with modeling tools : theoretical principles and empirical evidence*. Retrieved from http://everware-cbdi.com/private/downloads/_uYGGxiMGoBpSP4jZJqSrg/An Update to the SOA Adoption Roadmap Framework.pdf

Valtiovarainministeriö (2017). Julkisen hallinnon kokonaisarkkitehtuuri. Julkisen hallinnon arkkitehtuuriperiaatteet. Määrittely 1.91. https://wiki.julkict.fi/julkict/juhta/juhta-tyoryhmat-2016/jhka-tyoryhma/jhka-2.0/jhka-2-0-8-periaatteet/

Venable, J. (2006). A framework for design science research activities A Framework for Design Science Research Activities John Venable School of Information Systems Curtin University of Technology Abstract :, (January 2006).

Venable, J. R., Pries-heje, J. & Baskerville, R. (2017). Choosing a Design Science Research Methodology. *Australia Choosing a Design Science Research Methodology Keywords Design Science Research (DSR), Design Science Research Methodology*, 1–11. Retrieved from https://www.acis2017.org/wp-content/uploads/2017/11/ACIS2017_paper_255_FULL.pdf

Von Solms, B. & von Solms, R. (2018). Cyber security and information security – what goes where? *Information and Computer Security*, 00–00. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*. https://doi.org/10.1016/j.cose.2013.04.004

Winter, R. & Aier, S. (2011). How are Enterprise Architecture Design Principles Used? *2011 IEEE 15th International Enterprise Distributed Object Computing Conference Workshops*, 314–321. https://doi.org/10.1109/EDOCW.2011.27

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal*. https://doi.org/10.1147/sj.263.0276