Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 117, Issue 20, September/October 2019, Pages 57–71
https://doi.org/10.7250/csimq.2019-20.03

Method Framework for Developing Enterprise Architecture Security Principles

Sara Larno, Ville Seppänen* and Jarkko Nurmi

Faculty of Information Technology, University of Jyvaskyla, Mattilanniemi 2, Jyväskylä, FI-40014, Finland

sara.larno@gmail.com, ville.r.seppanen@jyu.fi, jarsamnu@student.jyu.fi

Abstract. Organizations need to consider many facets of information security in their daily operations – among others, the rapidly increasing use of IT, emerging technologies and digitalization of organizations' core resources provoke new threats that can be difficult to anticipate. It has been argued that the security and privacy considerations should be embedded in all the areas of organizational activities instead of only relying technical security mechanisms provided by the underlying systems and software. Enterprise Architecture Management (EAM) offers a holistic approach for managing different dimensions of an organization, and can be conceived as a coherent and consistent set of principles that guide how the enterprise must be designed. This article contributes with a method framework for integrating information security with EAM, aimed at providing support for the decision-making related to formulating context-aware EA security principles. The presented method framework is a result of a constructive research based on both the theoretical body of knowledge and the empirical evidence, obtained by interviewing 35 Finnish EA and information security practitioners.

Keywords: Enterprise Architecture Management, Enterprise Architecture Principle, Information Security, Information Security Policy, Method Framework, Constructive Research.

1 Introduction

Organizations constantly face new challenges in the area of information security. Digital transformation, networked business models, continuously evolving organizations, emerging technologies, increasing complexity of information systems and technology landscapes, regulatory pressures and changes in legislation, and several other factors necessitate that organizations must constantly keep their eye on the security requirements and redefine them as needed. As an example, since May 2018 the enterprises operating in Europe have been obligated

* Corresponding author

Reference: S. Larno, V. Seppänen and J. Nurmi, "Method Framework for Developing Enterprise Architecture Security Principles," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 20, pp. 57–71, 2019. Available: https://doi.org/10.7250/csimq.2019-20.03

Additional information. Author's ORCID iD: V. Seppänen – https://orcid.org/0000-0003-3843-4843. PII S225599221900117X. Received: 30 May 2019. Accepted: 23 October 2019. Available online: 31 October 2019.

to comply with the General Data Protection Regulation (GDPR); and failing to guarantee organizational security and privacy of their customers' personal data may lead to substantial fines. It has been argued that nowadays the security and privacy considerations should be embedded in all the areas of organizational activities instead of only relying on technical security mechanisms that underlying systems and software provide [1], [2].

The enterprise architecture (EA) management (EAM) has been seen as a viable approach for integrating different layers of information security and aligning them with the context of continuously changing business requirements. (e.g. [3]). As stated by The Open Group [4, p.1] "for too long, information security has been considered a separate discipline, isolated from the business processes and Enterprise Architecture". Although some research on security and EA exist (for instance, enterprise privacy architecture (EPA), enterprise security architecture (ESA), enterprise information security architecture (EISA) and Sherwood Applied Business Security Architecture (SABSA)), these approaches propose additional architectures to reinforce the existing EA method [3]. As discussed later in this article, the information security policy is divided into three categories of abstraction encompassing the whole organization [5], thus necessitating the security perspectives to be immersed into EA itself, instead of being additional architectural viewpoints or extensions. As argued in [25], the current approaches often focus solely on information systems and technology components of the architecture, and as such do not offer a requisite holistic approach to integrate the information security with the practices of EAM. Second, prior research is focused on discussing the risk management aspects on information security. While, for instance, Enterprise Architecture-Based Risk and Security Modelling and Analysis (ERSM) suggests security principles, no guidance for the development of the principles is given.

According to [6], the entire EA can be conceived as a coherent and consistent set of principles that guide how the enterprise must be designed, making EA principles a viable instrument of achieving organizational security. The objective of this study is to develop an abstract design knowledge artefact in the form of a method framework for integrating information security principle development with the EAM. As a practical contribution, the article provides support for decision-making related to formulating context-aware EA security principles, while a theoretical contribution can be found from the coverage of two distinct yet interrelated streams of research: information security and EA. The presented method framework is the result of the constructive research based on both the theoretical body of knowledge and the empirical evidence, which was obtained by interviewing 35 Finnish EA and information security practitioners.

The remainder of this article is organized as follows. In the next section we outline the theoretical foundation for this study by discussing its core concepts, i.e. the enterprise architecture principles and security policies, and their possible relation to each other. The third section describes our constructive research process phase by phase, and then the fourth section presents the results of the constructive work. The fifth section provides a discussion on the results. Finally, the sixth section concludes the paper, addresses limitations of the study, and suggests topics for further research.

2 Theoretical Background

This section discusses the key concepts of the research domain and establishes the theoretical foundations for the constructive part of the study. The first section addresses the enterprise architecture and, more specifically, the enterprise architecture principles, and the second covers the concept of information security policy. While the clear distinction between the terms principle and policy is not always drawn (cf., [7]), in the following we characterize the former as a rule to be followed and the latter as collection of guidelines to be adopted. By discussing these concepts, we aim to address the need for and the current lack of a holistic approach for integrating aspects of information security into the EAM.

2.1 Enterprise Architecture Principles

The EAM offers a holistic approach for managing different dimensions of an organization, such as its goals and objectives, business activities, software applications, data and information, and technology infrastructures. It fosters the use of common language and supports the co-operation between stakeholder groups [8]. EAM is widely used in strategy formation, planning, and implementation and in aligning business capabilities with the supporting IT resources [9].

To structure and guide the EAM-related activities, organizations use different methodologies, which have been developed both in the academia and industry. The origins of the modern EA can be traced to the Business Systems Planning methodology in the 1960s [10]. However, the term "enterprise architecture" and the related terminology were coined later in the early publications regarding the PRISM architecture framework (cf., [11]) and the Zachman Framework™ [12]. Currently, The Open Group Architecture Framework (TOGAF®), introduced in 1995, is the most widely adopted EA methodology in the industry [13]. However, most of the organizations have taken a "hybrid framework approach". [14] argues that no single methodology meets all requirements or addresses all the needs of a particular organization [13]. In a hybrid approach, aspects, ideas and approach are combined from a multiple different methodologies and frameworks.

There are some characteristics that are common to the majority of EAM methodologies. These include the separation of different viewpoints (such as business-related elements and technology-related elements) when an organization's architectural structures are being designed to constitute an aligned whole. Second, architectural planning and development is advised to consider the current state of the architectural structures in relation to the desired target state that would better serve the implementation of business objectives. By analyzing gaps between the current and desired structures, it is possible to identify and prioritize the relevant areas for development. Third, the EA frameworks, which can be considered as a form of enterprise ontology (cf., [15], [16], [17]), provide different viewpoints and different levels of abstraction (such as contextual, conceptual, logical and physical) for different stakeholders and their distinctive needs. For instance, a CIO might be interested in finding outdated software applications using the overall view provided by the application portfolio model, while a software developer designing the best-fitted integration approach might be interested in studying the APIs supported by the current information systems architecture. The design of actual implementable architectural structures is guided by the strategy-level considerations. For instance, along with the business architecture, information systems architecture, and technology architecture, the TOGAF® content metamodel separates the architecture vision derived from the business and technology strategies, the architecture requirements and constraints, and the architecture principles, which formulate the general underlying rules and guidelines for the architecture development.

As the principles manifest general rules and guidelines to support an organization fulfilling its mission, defining the architecture principles is recommended as the initiating activity of EAM [18]; whereas principles constitute a foundation of thinking about the systems design [19] and the requirements, and, on the other hand, state the functional and constructional properties for a system to have [20]. Therefore, the principles can be seen as boundary conditions from which the implementable requirements are derived.

The EA principles can either serve as the designing principles that are used to describe the design of actual system artefacts or the regulative principles to convey a prescriptive notion limiting the design options allowed in a system design [21]. [20] characterizes the EA principles being the latter. It is argued that the EA principles are a specific form normative principles that "guide/direct the enterprise normatively restricting design freedom" [20, p. 11]. Normative principles are based on artifacts such as strategy, the existing environment, and external developments [20]. The EA principles pursue the organization-wide consensus in the development, maintenance, and use of EA as well as in guiding its implementation as operational activities and supporting assets. As such the principles bridge the strategy and operations. In

practice, the EA principles are widely formulated in organizations and used, for instance, for reviewing development initiatives and projects. Therefore, the documentation and communication of EA principles is essential. The documentation should include, as a profound element, a clear definition of a principle's structure and the relations it has with its environment [22]. Furthermore, the documentation should address the principle's motivating rationale, concrete implications, and measures with which its fulfillment is evaluated [23], [24].

2.2 Information Security Policy

Organizations need to consider many facets of information security in their daily operations. The rapidly increasing use of IT, emerging technologies and digitalization of organizations' core resources provoke new threats that can be difficult to anticipate [25]. Attacks that damage or modify data can affect the critical infrastructure without any awareness of its owner. It is noteworthy that at the same time as new security threats have appeared alongside emerging technologies, an increasing number of threats are located inside the organization. Many of these threats are caused by unintentional, careless or negligent behavior [26], [27], [28]. Therefore, a majority of the literature on information security focuses on the user's perspective and how the users of information and technology resources can by their actions prevent, detect and respond to security threats [29].

Information security also encompasses data sources that are not in digital formats. Information that is based on physical documents or employees' knowledge can as well be a target to security threats [30]. Individual knowledge can be a key competitive advantage for an organization and therefore needs to be protected. Information security vulnerabilities contain a significant risk, not only to the operations of an organization, but also from the point of view of the organization's reputation. To this end, several organizations have been increasingly focusing on developing safety-related policies and aligning them with non-organizational regulations.

The number of studies on the implementation and efficiency of information security has significantly increased in the 21st century and the information security policy development is an area of growing scholarly interest. Generally, the concept of the information security policy is divided into the three categories of abstraction. At the lowest level of abstraction, information security is looked at from a technical point of view [5]. At this level, the key concern is the security architecture of technical systems, usually focusing on standards and procedures for the systems configuration or maintenance. At the next level of abstraction, information security is viewed from the user's point of view [5]. Here, certain areas of technology, such as the use of internet services, are addressed. These policies may include instructions and procedures that employees must observe in their daily interactions with the information and technology resources. The majority of extant research literature is examining the security policies through an individual and operational abstraction level [29]. At the highest level of abstraction, the information security is approached from the senior management point of view [5]. At this level, instead of the actual operative principles, the focus is on the strategic direction of the organization and the extent and nature of security objectives. These guide the development, implementation and management of the security programs and assign responsibilities to the various security areas at the most abstract, philosophical level [29].

To gain a needed broader perspective on the problem area, the topic of security has been approached from the perspectives of policy compliance and information security culture [29]. However, [31] argue that the extant literature on information security policies focuses on describing the structures and content, but usually does not describe a detailed development process. The professionals involved in the information security policy development are provided with little knowledge about the processes they should follow. They often need to rely on guidelines which are not specifically designed for their organizations and thus fail to recognize and answer to their specific threats and requirements [5], [31].

For constructing the information security policy, [5] argues for three matters to be considered. 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 a 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 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 the change, but also capable of achieving an appropriate level of information security. This kind of agile aspect is essential as organizational change can also help to 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.

The second matter is political simplicity. [5] notes that inflexible policies induce secret and poorly considered non-compliance. Therefore, the process of policy construction must be transparent, aware of its context, and involve the stakeholders at the different levels of an organization. The policy-related decisions need to be well-reasoned and their implications explicit. Thirdly, an information security policy must implement the existing criteria that can be obtained, for instance, 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.

Cyber security risks are socio-technical in nature as they include not only technical vulnerabilities but often also include factors related to behavior of human actors [28]. Consequently, several researchers have phrased the potential of the EAM to serve as an encompassing instrument for approaching information security related questions. For instance, [32] notes that the EAM provides a mean to mitigate the limiting siloed thinking of traditional risk management processes as it gives a better understanding on how an asset and its value can be affect by a manifestation of a risk. Similarly, [2] argues that the EAM is a promising approach to deal with the increasing complexity of organizations, technologies and the related security threats. Most of the current efforts, however, have focused only on individual areas on the domain of EAM, such as information systems risk management (e.g. [2], [33], [34]). Therefore, as argued in [35], the holistic approach to the security in EA is still lacking.

3 The Constructive Research Approach

As stated previously, the objective of this study is to develop an abstract design knowledge artefact. Design knowledge, produced by design research, can be separated into two outcomes, namely, abstract and situational design knowledge. Abstract design knowledge comes from meta-design, for instance, literature review, modelling and engagement scholarship [36] and produces abstract concepts, generic models, guidelines for design practices and systems abstractions with key properties [36]. 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. Design science evaluation has two forms: artificial and naturalistic evaluation [46] of which artificial evaluation was used in this study. In design science research, there are two evaluation related phases, evaluation and demonstration. 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, and the artefact was evaluated based on the views of the interviewees. The method framework was modified the first time after four interviews, and the second time after all the nine interviews were conducted.

In the field of method engineering, it is often argued that no method is suitable as such and some situational adaptation is always needed. The method adaptation refers to the activities of

enhancement, extension or restriction to make a method suitable for a specific domain, an organization, or a project [14], [37], [38]. Adaptability of the EA methods is particularly important due to the considerable heterogeneity of organizations and their business environments [39], [40], [41], [42]. In comparison to a method, a method framework is purposefully a more abstract methodological element that supports the definition of methods [43]. The method framework can be considered as a generalization of a method, which is then adjusted and specified to the context of a certain organization.

This section describes step-by-step the constructive research process that adopts ideas from several notable works on the design science research (e.g. [44], [45], [46], [47]). Also, the goals and requirements regarding the method framework's content and expedience are presented. Figure 1 summarizes the phases of the research process that was followed while constructing the Method Framework for Enterprise Architecture Security Principles (MF4EASP).

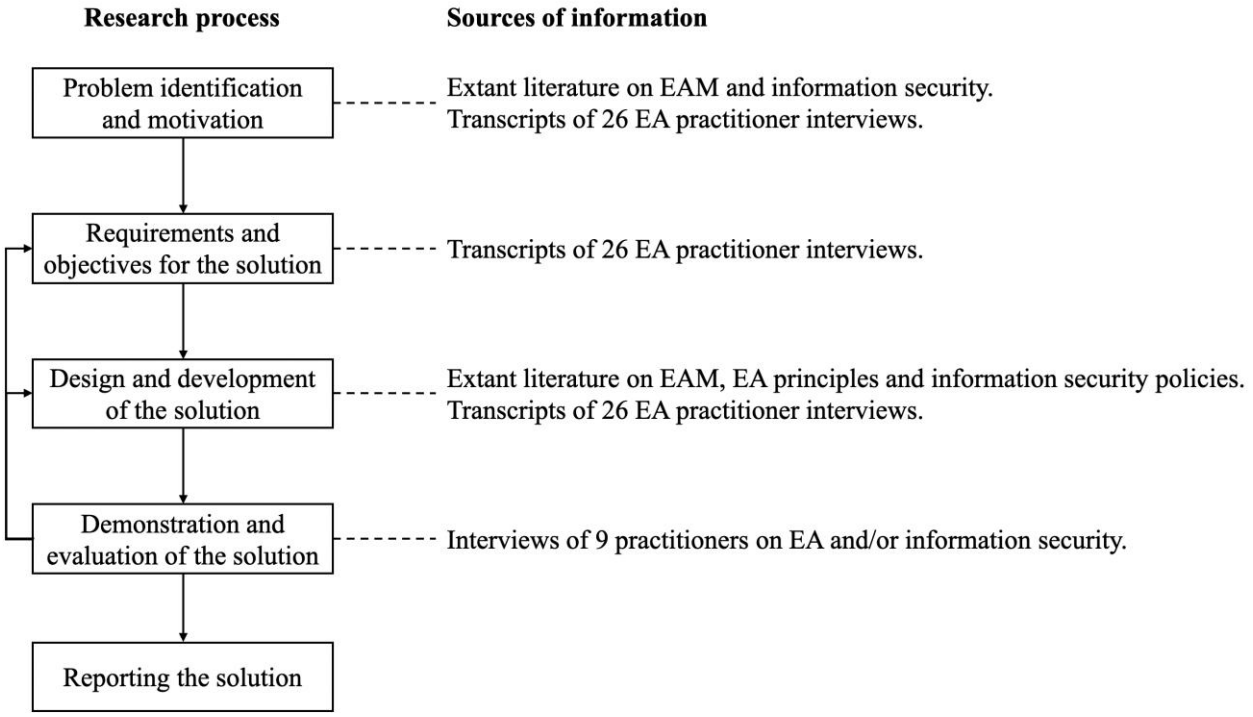

Figure 1. The phases of the research process and the accompanying sources of information

3.1 Problem Identification and Motivation

The problem, i.e. the need for and the current lack of a holistic approach for integrating aspects of information security into EAM, has been raised in recent studies. For instance, a study [35] argues that the integration of security and risk related concerns into the holistic approaches of EAM are currently at an inadequate level. Consequently, recent efforts have focused on information systems risk management (e.g. [2], [7], [35], [48]). However, in a review of 15 years of academic EA endeavors, a study [1] notes that although some progress has been made, EA has not yet reached the state of being a viable tool for addressing emerging security challenges and new threats to organizations' complex information systems. For instance, although EAM is mandated by legislation in the Finnish public sector, the National Audit Office of Finland, in their 2017 report, discovered several problems in the area of information security. Their report states that EA descriptions would serve as a valuable tool for evaluating the criticality of electronic services but EAM is not properly integrated with the operational requirements and practices. It was also found that the criticality of the ICT systems is not regularly checked,

although the frequent changes occurring in the operating environment would absolutely need it. Finally, the report states that the information security is commonly instituted as the responsibility of the IT units, even though they may not be aware of all the necessary business-related concerns, and thereby the holistic view to the information security remains lacking.

3.2 Requirements and Objectives

We analyzed the rich qualitative data obtained by interviewing 26 seasoned experts on EA, who contributed to the problem identification and to capturing the requirements and objectives for the MF4EASP. These informants serve in different positions in both private IT companies and public sector and their experience in EA-related activities range from 3 to 40 years with the average of 15 years. The interviews addressed the informants' views of the past, present and future practices of EAM. The data were screened for the information relevant to the objectives of this study. The details of the data collection can be found in [48]. The identified generic requirements for the MF4EASP are presented in Table 1. These are accompanied with the representative examples of citations from the interview transcripts. The excerpts are translated from Finnish to English.

Table 1. The guiding requirements for the development of MF4EASP

Requirement	Informants	Example from an interview
1) Information security should be included in every aspect of EAM.	1, 3, 5, 9, 10, 13, 14, 19, 22	*"Information security must be taken into account in all the architectural solutions through all the* [architecture] *layers."*
2) Information security should be included in EA design principles.	1, 12	*"Security cannot be just a glued-on concern. It must be a design principle."*
3) Risk management should be an integral part of EAM.	1, 2, 5, 20	*"Yes, we have been focusing our attention to that* [the EA method] *could guide the information security and risk management."*
4) Information security management practices should be adaptable to the purpose of the organization.	5, 8, 15, 23, 25	*"*[Planning of the information security] *should be purpose-driven. I mean, what are the needs of the business and operational functions. And what are the related risks. Then you can conclude what kind of information protection or security you really need. That way, you don't always categorically need to take the hardest road."*
5) Silo-mentality must be dismantled.	2, 6, 7, 19, 21	*"It is also often the case here that there are silos among experts. The interaction and co-operation are needed. And in a way, of course, the EAM is a pretty good tool for facilitating that conversation."*
6) A means to deal with legislative demands and regulatory pressures should be provided.	3, 5, 11,16, 17, 19, 26	*"*[Regulative laws] *are very extensive* [and] *they pose large and complex requirements. EAM is an appropriate tool for dealing with them."*
8) Information security practices must be able to respond to changes taking place in the operating environments.	13, 17, 18, 20, 24, 26	*"I think that the number of cloud-based solutions and hybrid solutions, where some of the information is stored locally and some of it in the cloud,* [will continue to increase]. *You need to be able to continuously change the way you do your work."*

3.3 Design and Development

The overall structure for the artefact presented in this paper draws from the previous works on the design of EA principles and information security policies. A number of academic contributions on the EA principle development can also be found (e.g. [6], [23], [24]), although their applicability is somewhat limited due to their generality and purposefully wide scope. Based on the literature review [49], the consolidated metamodel of EA principles has been presented [22]. By itemizing the elements of a principle, this metamodel differentiates the core definition of the EA principle, including its statement, rationale, implications, key actions, and related measures, and also provides an extended definition that considers the principle's impact on its environment. We used the work presented in [22] for defining the key components and the areas of concern for MF4EASP.

Next, for the structure of EA security principle development process, we adapted the process of the policy development framework [31] and the relevant components presented in the Comprehensive Information Security Policy Process Model [50]. Finally, we strived to balance the requirements found in our empirical data with the requirements of suppleness, political simplicity and criterion-orientation as discussed in relation to information security meta-policy in [5].

The MF4EASP was constructed using the ArchiMate® 3.0.1 specification. The ArchiMate® modeling language is an Open Group standard, which provides a TOGAF® compliant modeling notation that covers all the EA domains. It is widely used in both public and private organizations around the world and is supported by the majority of EA modeling tools. As a semi-formal modeling language, it provides a coherent and visually uniform representation for EA artefacts covering different components of an architecture and their dependencies. As such it aims at enabling communication among stakeholders, and guides complicated change processes on architectural structures.

3.4 Demonstration and Evaluation

Nine expert practitioners took part in evaluating the tentative versions of MF4EASP. The evaluators were selected using the criterion sampling (c.f., [48]) so that the informants could provide profound and well-reasoned insights to support the further development of the construct. Four of the evaluators have their expertise both in the fields of EA and information security, three in the information security, and two in the EA. Their occupational positions included Chief Information Officer, Chief Digital Officer, Enterprise Architect, Specialist, Researcher, and different managerial positions. The evaluators' professional experience in the field of their expertise ranged from 2 to 30 years with the average of 14 years.

The evaluation of the method framework was conducted by presenting the MF4EASP to the evaluator who was then asked to give feedback, criticism and constructive ideas regarding various aspects. Each evaluator was met individually by the first author, to ensure that their views and opinions would not affect the other evaluators. The aspects of evaluation were based in the method engineering knowledge and adhered to shell model presented in [52]. Table 2 presents the themes covered during the evaluation and the questions they were addressed with. Overall, the evaluation was targeted to the correctness, completeness and applicability of the MF4EASP.

The evaluation was conducted for the two versions of MF4EASP in the two rounds. Some changes were implemented to the first version of construct according to the feedback given by the first four evaluators. These included, for instance, a possibility for both objectives and constraints to define requirements for design principles, the acknowledgement of possible stakeholder-induced risks, and that the process needs to, in addition to security principle development, consider their implementation in an organization.

Table 2. The artefact evaluation themes and the related questions

	Assumptions and/or Implications	Derived Evaluation Questions
Values and Assumptions	- EAM is a beneficial approach to information security issues. - EA principles and information security policies share similar approaches, goals and levels of abstraction and can be used in union to develop an information security principle.	- Are the assumptions correct? - Are the assumptions relevant? - Are there any other assumptions to be considered?
Development Objectives and Decisions	- The objective is to develop a method for EA information security design principle development.	- Is it possible to develop an efficient EA information security design principle with the MF4EASP? - Are the presented development decisions correct? - Are the presented development decisions coherent?
Participation and Roles	- The participating roles include management; legal counseling; HR; IT staff; end-users; external representatives.	- Is there a stakeholder role missing or excessive?
Process	- The process combines the aspects of EA principle development and security principle development.	- Do the sub-processes represent suitable content for the development process? - Are the sub-processes orderly arranged? - Is there a sub-process missing or excessive?
Notation	- The method framework is represented using the industry standard ArchiMate® modeling notation.	- Are the notational constructs understandably and correctly related to the concepts used (for instance, fidelity, completeness, only one construct used per concept)? - Is the modeled representation of MF4EASP understandable? - Are the concepts meaningful, relevant and sufficient?
Conceptual Structure	- The conceptual structure is based on and extends the ArchiMate® metamodel and previous information security policy development frameworks.	- Are the relationships between concepts meaningful, relevant and sufficient? - Is there a concept missing or excessive? - Is the level of detail adequate for the MF4EASP to be used in different organizations?

On the next round, both the original and the altered versions of the construct were presented to the five evaluators. Overall, the review feedback resulted in some corrections, alterations and adjustments to the method framework. The comments addressed details of the graphical representation (i.e. the ArchiMate® notation and its use), a need to alter the types of relationships or to add new relationships between concepts, missing sources of security threats, alleged challenges related to the implementation of the suggested development process, and concerns regarding the monitoring an organization's compliance to the principles. The last two, while absolutely critical and present important topics for the future research, go beyond the scope of this study. Therefore, we purposefully omitted the details of the context-specific process implementation and the enforcement of principle adherence. Some of the comments, although each of them were thoroughly contemplated during the evaluation and redesign of the method framework, were omitted because did not clearly meet the objectives of MF4EASP. The evaluator comments are summarized in Table 3.

Table 3 Evaluation comments requesting for alteration

Area of Evaluation	Evaluator comments requesting for alteration
Values and Assumptions	- None.
Development Objectives and Assumptions	- The high level of abstraction makes it difficult to implement an efficient method.
Participation and Roles	- Senior level management roles need to be added as stakeholders. - Stakeholder groups should cover also 'leadership roles' as it is different from the managerial roles. - It should be possible to acknowledge stakeholders as potential security threats.
Process	- The process could be difficult to implement. - There is a risk that information security ends up guiding business activities. - The principles are not a sufficient mean to guide an organization. More specific guidelines and instructions are needed. - More specific guidelines are needed for practical implementation. - It can be difficult to recognize the needed factors in an organization. - The use of Balanced Score Card and SWOT analysis could provide additional support while implementing the process. - The method is better suited for implementing slow changes and improvements.
Notation	- The use of some ArchiMate® elements does not adhere to the language specification. - The method framework is difficult to understand without written explanation. - The ArchiMate®-based representation is not well-suited for supporting the communication between different stakeholders.
Conceptual Structure	- The concepts should be specified in more detail. - The level of abstraction is high, which makes it impossible to identify the expected elements from an organizational context. - The level of detail does not cover "two-speed IT" and is more suitable for slow changes. - Two-speed IT should be considered. - The method framework claims that the risk assessment could be done without the knowledge about possible threats. - The legislation is not only a requirement. It can also be a constraint. - The risk assessment alone is not sufficient. It must be preceded by risk analysis.

4 MF4EASP – The Method Framework for Developing Enterprise Architecture Security Principles

The design of the MF4EASP method framework, as presented in Figure 2, was based on the literature on EA principles and information security policy construction as well as interviews of 26 seasoned EA practitioners and 9 experts on EA and/or information security. In the following, the components of MF4EASP are structured to adhere to the layers of SABSA[†] business driven enterprise security architecture framework, due to its commonly acknowledged position. The SABSA compliant layers included in the MF4EASP are the contextual, conceptual, logical, physical and component layer. SABSA suggests these layers for the management of delivery of security solutions throughout their entire lifecycle. The contextual architecture layer's (i.e. business view) main function is to identify and extract security requirements from the business environment. The risk assessment is conducted based on these requirements [53]. The conceptual

[†] https://sabsa.org/

architecture layer (i.e. architect's view) generalizes the business concerns and considerations into policies and procedures. The logical architecture layer (i.e. designer's view) defines detailed security controls and management objectives to, for instance, access control and monitoring operations. This layer transforms the abstract business requirements to applicable security specifications [53]. Finally, the physical architecture layer (i.e. constructor's view) and the component architecture layer (i.e. technician's view) are the fields of operations managers and systems developers, respectively, who implement the security mechanisms according to the above layers. When using the MF4EASP, enterprise architects are to operate on the areas related to the conceptual and logical layers. They define the EA security principles, carefully align them with the organization's EA, and bridge the domains of the business requirements and the related security implementations.

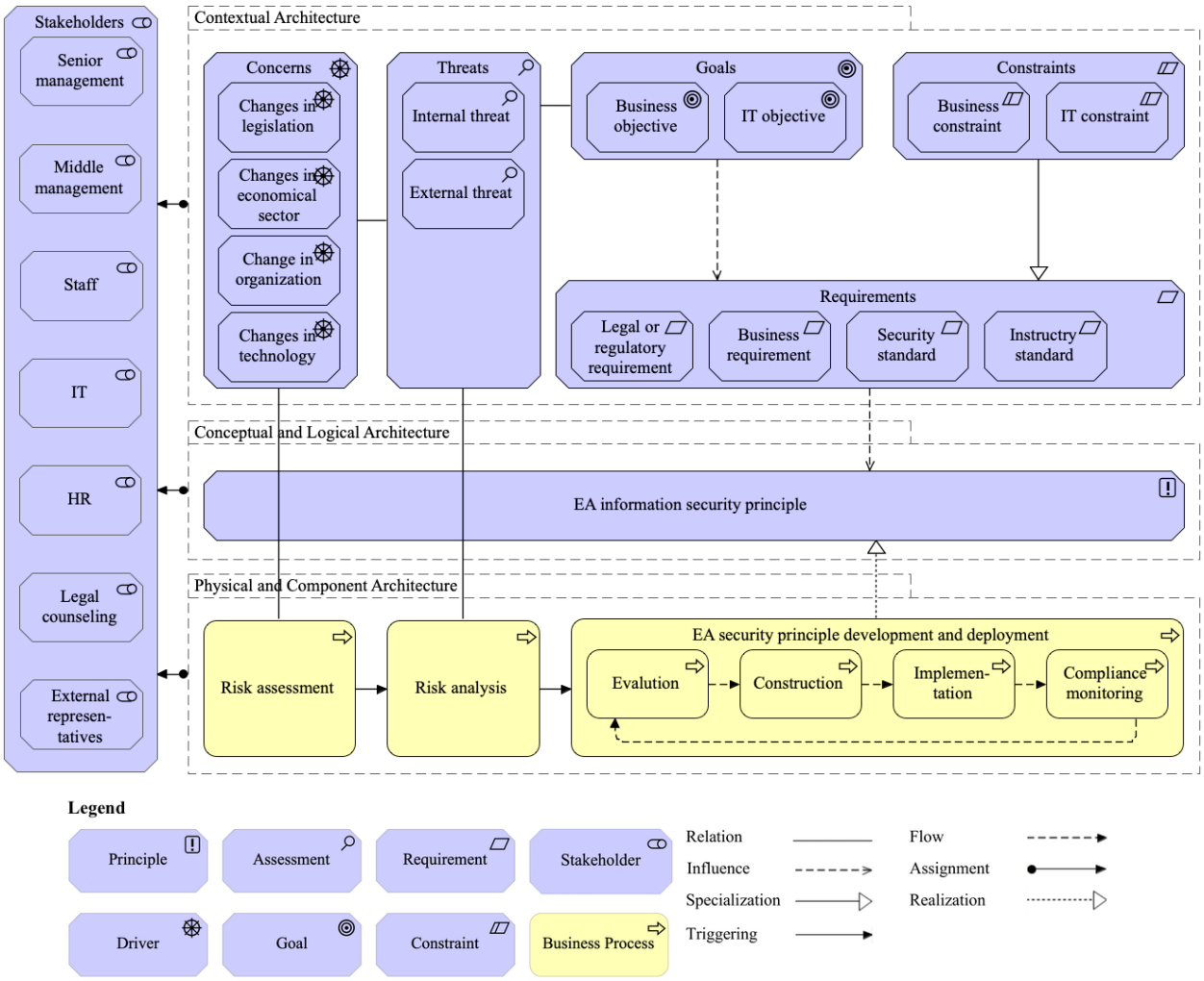

Figure 2 The MF4EASP method framework

The implementation of the MF4EASP starts from the upper left-hand side corner (Figure 2). An organization might have concerns arising from minor or major changes in the organization itself, its economic sector or business domain, legislation, or technology. Then, the identified changes are channeled through the processes of risk analysis and risk assessment, whose detailed implementation should be fitted for each particular organization and its branch of industry. The risk analysis and assessment may state a concern being a potential security threat. An identified threat does not necessarily trigger a need to establish a new EA security principle. It is well possible that the organization already has functional principles to handle these emergent changes. However, if the threat is considered to potentially have a negative impact on the goals of the

organization, and it is assessed that the related risks need to be mitigated, the outcome of the risk assessment process will initiate the EA security principle development and deployment process.

The process starts with the evaluation of the situation at hand. The relevant stakeholders revise the business and IT objectives and evaluate the constraints they set. The objectives and constraints specify the requirements that the principle must meet. Even though the requirements can be treated as the specified types of the constraints, requirements analysis must also consider the needs derived from the organizational goals. It is also possible that there are non-constraining requirements, which still set conditions for the principle. The principle construction should acknowledge all the stakeholders to whom the principle will have an effect on.

The next sub-process covers the principle's implementation to the related structures of an organization's EA. A principle may have an impact on an entire organization, its certain business unit, an expected professional behavior, a work practice, an information system, technology, etc. Once a principle has been implemented, the compliance monitoring will commence, focusing on the appropriate indicators and utilizing the means best suited for the purpose. If the monitoring of the adherence to the principle reveals either that the principle as such does not reflect the actual business concerns to the appropriate expedient or the organization, for this or some other reason, fails to comply with the requirements it posits, the process returns to the evaluation phase. The re-evaluation of the already implemented principle may either lead to strengthening its rationale or enforcement practices, to the principle's readjustment, or even its dismissal.

An organization can integrate its information security policy with the practices of EAM by following the principles constructed and implemented using the MF4EASP. All the layers of EA should be compliant to the principles, as discussed in Section 2.1. For instance, a generic security principle stating that the data related to the personal information must be treated securely and confidentially, would extend over professionally conducted work practices, the information systems supporting these practices as well as the technology layer, such as the data storages, upon which the systems' data management processes are executed. The EA security principles constructed using the MF4EASP can be, and should be, used as both the design principles and the regulative principles, and, on the other hand, are applicable on all the target areas of information security policies.

5 Discussion

Although the presented method framework was carefully evaluated by several professionals of the fields of information security and enterprise architecture, its actual capability to serve in real life situations still remains to be seen. This will require further studies on the implementations of MF4EASP. The evaluators also pointed to some concerns regarding the suggested method framework that we did not see feasible to include at this stage, or that were outright impossible to implement, as they would have necessitated the formulation of universally normative guidelines. For instance, some of the evaluators were skeptical about the practical implementation capability of the EA security principle development and deployment process. Likewise, another evaluator uttered that more specific guidelines would be required for this purpose. However, as we presented a generic and context-independent method framework, we purposefully did not want to formulate organization-specific guidelines. The principle implementation undeniably affects the organizational culture and its embedded mechanisms, which are not only the targets of change but also the effectors in this process. These fine-grained details are impossible to address within the scope of this study.

Another evaluator also expressed a concern regarding that the MF4EASP would lead to a situation where the security principles end up guiding business activities and thus limit possibilities for innovation and experimentation, which can be highly important for nurturing new business opportunities. In a similar manner, two evaluators addressed concerns related to the 'two-speed IT', which is argued being an enabling requisite for digital innovation. On this regard, we want to re-emphasize that the contextual architecture (i.e. business view) is the

driving viewpoint for the security principle development. It is not the purpose of the MF4EASP that it should limit the organization's capability to innovate and experiment for the sake of information security adherence. However, these experimentations, naturally, need to be in line with the business goals and constraints, and should they be decided to be released into the production environment, they need to comply with the organization's security policy guided by the business objectives.

6 Conclusions and Future Work

The objective of this study was to develop an abstract design knowledge artefact in the form of a method framework for integrating information security principle development with EAM. The presented method framework is a result of constructive research based on both the theoretical body of knowledge and the empirical evidence, which was obtained by interviewing 35 Finnish EA and information security practitioners. The empirical data served the major role in constructing the results of this study. All our informants are based in Finland and therefore mostly reflect the local standpoints and the European standards and regulations to the information security. A theoretical contribution can be found from the coverage of two distinct yet interrelated streams of research: information security and EA. Therefore, the results presented in this paper contribute to the currently lacking theoretical body of knowledge on EAM-driven information security management practices and their practical implications should be generally applicable. While the proposed method framework still needs to be tested with actual use cases, the current results provide actionable guidelines for the organizations struggling with the challenges related to the information security in the constantly changing business environments.

References

[1] S. Kaisler and F. Armour, "15 Years of Enterprise Architecting at HICSS : Revisiting the Critical Problems," *Proc. of the 50th Hawaii International Conference on System Sciences*, 2017, pp. 4807–4816. Available: https://doi.org/10.24251/HICSS.2017.585

[2] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management," *Softw. & Syst. Model.*, vol. 18, no. 3, pp. 2285–2312, 2018. Available: https://doi.org/10.1007/s10270-018-0661-x

[3] F. Burmeister, P. Drews, and I. Schirmer, "A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation," *Proc. of the 52nd Hawaii International Conference on System Sciences*, pp. 6052–6061, 2019. Available: https://doi.org/10.24251/HICSS.2019.729

[4] The Open Group, "Integrating Risk and Security within a TOGAF ® Enterprise Architecture," *Secur. Forum (a Forum Open Inst. Group)*, 2016. [Online]. Available: https://publications.opengroup.org/g152

[5] R. Baskerville and M. Siponen, "An information security meta- policy for emergent organizations," *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 337–346, 2002. Available: https://doi.org/10.1108/09576050210447019

[6] J. Hoogervorst, "Enterprise Architecture: Enabling integration, Agility and Change," *Int. J. Coop. Inf. Syst.*, vol. 13, no. 3, pp. 213–233, 2004. Available: https://doi.org/10.1142/S021884300400095X

[7] N. Mayer and C. Feltus, "Evaluation of the risk and security overlay of archimate to model information system security risks," *Proc. of the IEEE 21st Int. Enterp. Distrib. Object Comput. Work. EDOCW*, pp. 106–116, 2017. Available: https://doi.org/10.1109/EDOCW.2017.30

[8] S. Aier, C. Riege, and R. Winter, "Classification of Enterprise Architecture Scenarios," *Enterp. Model. Inf. Syst. Archit.*, vol. 3, no. 1, pp. 14–23, 2008. Available: https://doi.org/10.18417/emisa.3.1.2

[9] F. Rahimi, J. Gøtze, and C. Møller, "Enterprise architecture management: Toward a taxonomy of applications," *Commun. Assoc. Inf. Syst.*, vol. 40, no. 1, pp. 120–166, 2017. Available: https://doi.org/10.17705/1CAIS.04007

[10] S. Kotusev, "Enterprise Architecture: What Did We Study?" *Int. J. Coop. Inf. Syst.*, vol. 26, no. 4, 2017. Available: https://doi.org/10.1142/S0218843017300029

[11] H. A. Proper and M. M. Lankhorst, “Enterprise Architecture: Towards essential sensemaking,” *Enterp. Model. Inf. Syst. Archit.*, vol. 9, no. 1, pp. 5–21, 2014. Available: https://doi.org/10.1007/s40786-014-0002-7

[12] J. F. F. Sowa and J. A. Zachman, “Extending and Formalizing the Framework for Information Systems Architecture,” *IBM Syst. J.*, vol. 31, no. 3, pp. 590–616, 1992. Available: https://doi.org/10.1147/sj.313.0590

[13] B. H. Cameron and E. Mcmillan, “Analyzing the Current Trends in Enterprise Architecture Frameworks,” *J. Enterp. Archit.*, vol. 3, no. 2, pp. 18–27, 2013.

[14] S. Leist and G. Zellner, “Evaluation of current architecture frameworks,” *Proc. of the 2006 ACM symposium on Applied computing*, pp. 1546–1553, 2006. Available: https://doi.org/10.1145/1141277.1141635

[15] J. L. G. Dietz and J. A. P. Hoogervorst, “Enterprise ontology in enterprise engineering,” *Proc. of the 2008 ACM Symp. Appl. Comput. SAC 08*, vol. 28, pp. 572–579, 2008. Available: https://doi.org/10.1145/1363686.1363824

[16] L. A. Kappelman and J. A. Zachman, “The Enterprise and Its Architecture: Ontology & Challenges,” *J. of Computer Information Systems*, vol. 53, no. 4, pp. 87–95, 2015. Available: https://doi.org/10.1080/08874417.2013.11645654

[17] J. Lapalme, A. Gerber, A. Van Der Merwe, J. Zachman, M. De Vries, and K. Hinkelmann, “Exploring the future of enterprise architecture: A Zachman perspective,” *Comput. Ind.*, vol. 79, pp. 103–113, 2016. Available: https://doi.org/10.1016/j.compind.2015.06.010

[18] J. A. P. Hoogervorst, “Enterprise Architecture in Enterprise Engineering,” *Enterp. Model. Inf. Syst. Archit.*, vol. 3, no. 1, pp. 1–12, 2008. Available: https://doi.org/10.18417/emisa.3.1.1

[19] C. C. Wood, “Principles of secure information systems design,” *Comput. Secur.*, vol. 9, no. 1, pp. 13–24, 1990. Available: https://doi.org/10.1016/0167-4048(90)90150-R

[20] H. A. Proper and D. Greefhorst, “Principles in an Enterprise Architecture Context,” *J. Enterp. Archit.*, vol. 7, no. 1, pp. 8–16, 2011. Available: https://doi.org/10.1007/978-3-642-20279-7_2

[21] P. Van Bommel, P. G. Buitenhuis, S. J. B. A. Hoppenbrouwers, and H. A. Proper, “Architecture principles: A regulative perspective on enterprise architecture,” *Enterp. Model. Inf. Syst. Archit.*, vol. 3, no. 1, pp. 1–15, 2008.

[22] S. Aier, C. Fischer, and R. Winter, “Construction and Evaluation of a Meta-Model for Enterprise Architecture Design Principles,” *10 Int. Tagung Wirtschaftsinformatik*, no. February, pp. 637–644, 2011.

[23] G. L. Richardson, B. M. Jackson, and G. W. Dickson, “A Principles-Based Enterprise Architecture: Lessons from Texaco and Star Enterprise,” *MIS Q.*, vol. 14, no. 4, pp. 385–403, 1990. Available: https://doi.org/10.2307/249787

[24] Å. Lindström, “On the Syntax and Semantics of Architectural Principles,” in *Proc. of the 39th Hawaii International Conference on System Sciences*, 2006, pp. 1–10. Available: https://doi.org/10.1109/HICSS.2006.367

[25] G. D. Moody, M. Siponen, and S. Pahnila, “Toward a Unified Model of Information Security Policy Compliance,” *MIS Q.*, vol. 42, no. 1, pp. 285–311, 2018. Available: https://doi.org/10.25300/MISQ/2018/13853

[26] M. Warkentin and R. Willison, “Behavioral and policy issues in information systems security: the insider threat,” *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 101–105, 2009. Available: https://doi.org/10.1057/ejis.2009.12

[27] M. Siponen, S. Pahnila, and M. A. Mahmood, “Compliance with Information Security Policies : An Empirical Investigation,” *IEEE Comput. Soc.*, vol. 43, no. 2, pp. 64–71, 2010. Available: https://doi.org/10.1109/MC.2010.35

[28] T. R. McEvoy and S. J. Kowalski, “Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach,” *Complex Syst. Informatics Model. Q.*, no. 18, pp. 47–64, 2019. Available: https://doi.org/10.7250/csimq.2019-18.03

[29] W. A. Cram, J. G. Proudfoot, and J. D’Arcy, “Organizational information security policies: A review and research framework,” *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 605–641, 2017. Available: https://doi.org/10.1057/s41303-017-0059-9

[30] B. von Solms and R. von Solms, “Cybersecurity and information security – what goes where?” *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, 2018. Available: https://doi.org/10.1108/ICS-04-2017-0025

[31] S. V. Flowerday and T. Tuyikeze, “Information security policy development and implementation: The what, how and who,” *Comput. & Secur.*, vol. 61, pp. 169–183, 2016. Available: https://doi.org/10.1016/j.cose.2016.06.002

[32] J. Barateiro, G. Antunes, and J. Borbinha, “Manage risks through the Enterprise Architecture,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 3297–3306, 2012. Available: https://doi.org/10.1109/HICSS.2012.419

[33] F. Innerhofer-Oberperfler and R. Breu, “Using an Enterprise Architecture for IT Risk Management,” *Proc. of the ISSA 2006 from Insight to Foresight Conference*, 2006.

[34] J. S. Burkett, “Business Security Architecture: Weaving Information Security into Your Organization’s Enterprise Architecture through SABSA®,” *Inf. Secur. J.*, vol. 21, no. 1, pp. 47–54, 2012. Available: https://doi.org/10.1080/19393555.2011.629341

[35] H. Jonkers and D. Quartel, “Graphical Models for Security,” *Third International Workshop, GraMSec 2016*, vol. 9987, pp. 94–101, 2016. Available: https://doi.org/10.1007/978-3-319-46263-9_6

[36] Ł. Ostrowski, M. Helfert and F. Hossain, “A conceptual framework for design science research,” *Proc. of the International Conference on Business Informatics Research*, Springer, LNBIP, vol. 90, pp. 345–354, 2011. Available: https://doi.org/10.1007/978-3-642-24511-4_27

[37] J. Ralyte *et al.*, “Towards a Generic Model for Situational Method Engineering To cite this version : Towards a Generic Model for Situational Method,” *Proc. of the Int. Conf. Adv. Inf. Syst. Eng.*, Springer, LNCS, vol. 2681, pp. 95–110, 2012. Available: https://doi.org/10.1007/3-540-45017-3_9

[38] M. Leppänen, *An Ontological Framework and a Methodical Skeleton for Method Engineering: A Contextual Approach*. Jyväskylä Studies in Computing 52, 2005.

[39] M. Leppänen, K. Valtonen, and M. Pulkkinen, “Towards a Contingency Framework for Engineering an Enterprise Architecture Planning Method,” *Proc. of 30th Information Systems Research Seminar in Scandinavia*, 2007.

[40] C. Riege and S. Aier, “A Contingency Approach to Enterprise Architecture Method Engineering,” *International Conference on Service-Oriented Computing*, Springer, LNCS, vol. 5472, pp. 388–399, 2008. Available: https://doi.org/10.1007/978-3-642-01247-1_39

[41] K. Valtonen, V. Seppänen, and M. Leppänen, “Government enterprise architecture grid adaptation in Finland,” *Proc. of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*, 2009. Available: https://doi.org/10.1109/hicss.2009.232

[42] S. Buckl, “Developing organization-specific enterprise architecture management functions using a method base,” Ph.D. dissertation, Technische Universität München, Lehrstuhl für Informatik XIX, 2011.

[43] C. Salviano, A. Zoucas, J. Silva, Â. Alves, C. G. von Wangeheim, and M. Thiry, “A Method Framework for Engineering Process Capability Models,” *16th Eur. Syst. Softw. Process Improv. Innov. Ind. EuroSPI 2009.*, vol. 1, pp. 25–36, 2009.

[44] S. T. March and G. F. Smith, “Design and natural science research on information technology,” *Decis. Support Syst.*, vol. 15, no. 4, pp. 251–266, 1995. Available: https://doi.org/10.1016/0167-9236(94)00041-2

[45] A. R. Hevner, S. T.March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004. Available: https://doi.org/10.2307/25148625

[46] J. Venable, “The role of theory and theorising in Design Science research,” *Proc. DESRIST*, pp. 24–35, 2006.

[47] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007. Available: https://doi.org/10.2753/MIS0742-1222240302

[48] M. Q. Patton, *Qualitative evaluation and research methods*. Thousand Oaks, CA, US: Sage Publications, Inc., 1990.

[49] K. Penttinen, “The Long and Winding Road of Enterprise Architecture Implementation in the Finnish Public Sector,” Ph.D. dissertation, Faculty of Information Technology, University of Jyväskylä, Finland, 2018.

[50] D. Stelzer, “Enterprise architecture principles: Literature review and research directions,” *Service-Oriented Computing. ICSOC/ServiceWave 2009 Workshops*, Springer, LNCS, vol. 6275, pp. 12–21, 2010. Available: https://doi.org/10.1007/978-3-642-16132-2_2

[51] K. J. Knapp, R. F. Morris, T. E. Marshall, and T. A. Byrd, “Information security policy: An organizational-level process model,” *Comput. & Secur.*, vol. 28, no. 7, pp. 493–508, 2009. Available: https://doi.org/10.1016/j.cose.2009.07.001

[52] J.-P. Tolvanen, “Incremental Method Engineering with Modeling Tools: Theoretical Principles and Empirical Evidence,” Ph.D. dissertation, University of Jyväskylä, Finland, 1998.

[53] C. Magnusson and S. C. Chou, “Risk and compliance management framework for outsourced global software development,” *Proc. of the 5th Int. Conf. Glob. Softw. Eng. ICGSE 2010*, pp. 228–233, 2010. Available: https://doi.org/10.1109/ICGSE.2010.34