Mika Kokkonen

TOWARDS AN OPTIMAL SELF-ASSESSMENT TOOL FOR INFORMATION SECURITY INVESTMENT DECISION-MAKING

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2017

ABSTRACT

Kokkonen, Mika
Towards an optimal self-assessment tool for information security investment decision-making
Jyväskylä: University of Jyväskylä, 2017, 71p.
Information systems, Master's Thesis
Supervisor: Soliman, Wael

Previous research has focused mainly on economic models that aim to help organizations to identify *how much* to invest in information security. These models aimed for benefit maximization and focused on certain parts of information security investment process. Thus, the classical theories and models are problematic in information security investment decision-making, and more holistic approach should be taken in information security investments.

Information security field lacks research on information security self-assessment tools in information security investment decision-making. This research attempted to fill this gap by studying the existing literature and creating a conceptual information security tool model through design science research process. Preliminary conceptual tool model was developed based on literature study, after which empirical case study demonstrated the tool in working life, and refinement was conducted based on the case study findings. The results of the case study were in line with recent research and helped in the validation of the tool concept.

Overall, this master thesis contributed to information security research by providing a blueprint for an information security self-assessment tool that would help organization to better identify *to what* information security area(s) to invest. The empirically-grounded model can help organizations and tool developers to understand what kind of tools are needed in information security investments.

Keywords: self-assessment, tool, information security, investment, decision making

TIIVISTELMÄ

Kokkonen, Mika
Towards an optimal self-assessment tool for information security investment decision-making
Jyväskylä: Jyväskylän yliopisto, 2017, 71 s.
Tietojärjestelmätiede, pro gradu-tutkielma
Ohjaaja: Soliman, Wael

Aikaisempi tutkimus keskittyi pääasiallisesti taloudellisiin malleihin, joiden tarkoituksena oli auttaa organisaatioita tunnistamaan *kuinka paljon* heidän tulisi sijoittaa tietoturvallisuuteen. Nämä mallit pyrkivät tuottojen maksimointiin ja keskittyivät tietoturvainvestointiprosessin tiettyihin osiin. Tästä johtuen, klassiset teoriat ja mallit ovat ongelmallisia tietoturvainvestointien päätösten teossa, jonka myötä tulisi omaksua kokonaisvaltaisempi lähestyminen tietoturvainvestointeihin.

Tietoturvallisuuden tutkimuskentältä puuttuu tutkimusta tietoturvallisuuden itsearviointityökalujen käytöstä tietoturvainvestointien päätöksenteossa. Tämä tutkimus pyrki täyttämään tämän aukon tutkimalla olemassa olevaa kirjallisuutta ja luomalla käsitteellisen tietoturvatyökalun mallin suunnittelutieteen prosessin kautta. Alustava malli luotiin olemassa olevaan kirjallisuuteen perustuen, jonka jälkeen empiirinen tapaustutkimus havainnollisti työkalua työelämän edustajille, ja työkalun kehittämistä tehtiin tapaustutkimuksen tulosten pohjalta. Tapaustutkimuksen tulokset olivat linjassa viimeisimpien tutkimusten kanssa ja ne auttoivat vahvistamaan käsitteellistä työkalumallia.

Kaiken kaikkiaan, tämä pro gradu-tutkielma myötävaikutti tietoturvallisuuden tutkimuskenttään luomalla käsitteellisen tietoturvallisuuden itsearviointityökalun mallin, joka auttaisi organisaatioita paremmin tunnistamaan *mihin* tietoturvallisuuden alueisiin heidän tulisi investoida. Empiirisesti perusteltu malli voi auttaa organisaatioita ja työkalujen kehittäjiä ymmärtämään minkälaisia työkaluja tarvitaan tietoturvallisuuden investoinneissa.

Asiasanat: itsearviointi, työkalut, tietoturva, investointi, päätöksenteko

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Organizations of all sizes are investing in information security (hereafter InfoSec) to reduce the likelihood and impact of major damages caused by InfoSec incidents. Earlier in InfoSec investment research, scholars have argued that there exists an optimal level of InfoSec investment for each organization. Investing less than the optimal level will result in unacceptable InfoSec risks, and investments exceeding the optimal level do not necessarily bring justifiable investment results. (e.g. Huang, Hu & Behara, 2008, 1-2.)

Until recently, many organizations made InfoSec investment decision based mainly on industry best practices, but not fully understanding their specific InfoSec risk situation. Lacking articulation of how the InfoSec risks integrate to organizational risks and because of the uncertain nature of InfoSec, many organizations experienced under-funding on InfoSec (Moore, Dynes & Chang, 2016, 1; Beebe, Young & Chang, 2014, 135). Also, the characteristic problem in InfoSec investments is the intangible nature of the benefits (Shao, 2015, 37.)

One major driver for InfoSec investments used to be lists of controls from InfoSec frameworks and investments were made to "check the box" to allocate investments. The shortcoming of this is that organizations do not critically think about their specific risk environment, but only achieves compliance against selected control framework. However, even the tools are more mature nowadays, decision-makers may not be using them effectively, but still use them to "get a check to boxes", and do not make effort to understand their organization's realities. (Moore et al., 2015, 14.)

The InfoSec self-assessment tools vary from supplier to another and some InfoSec professionals create their own custom tools based on common InfoSec frameworks (Moore et al, 2015). This indicates that the organizations developing their own InfoSec frameworks are more likely to have better understanding of their InfoSec environment (Moore et al, 2015). Therefore, tools that can be modified to organizational needs would add more value to their InfoSec (investment) management and decision-making.

Tools, whatever the implementation, are and will be a good addition to InfoSec professionals' toolkit as e.g. compliance is easier to confirm with the documented information provided by or within the tools. Compliance is also one of the main drivers of InfoSec investments (Shao, 2015; Moore et al., 2015), and, for example, upcoming EU General Data Protection Regulation (GDPR) (Eurlex, 2016) requires organizations that handle personal data to confirm that they have implemented adequate InfoSec controls to protect the information, thus confirming the compliance is needed. However, not all InfoSec professionals see compliance as the main driver (Moore et al., 2015, 8). Therefore, based on the previous information, the need for InfoSec self-assessment tool research in the InfoSec investment decision-making process was identified.

This research attempts to develop a blueprint for an InfoSec self-assessment tool (hereafter blueprint), which would help organizations, and others, to identify what they should include and how these tools can be effectively used as a support in InfoSec investment decision-making process. Unlike the previous, classical economic models that are mostly mathematical calculations of *how much* to optimally invest in InfoSec, this research aims to create a blueprint that consists of needed features in an InfoSec tool that helps organizations to identify *to what* InfoSec area(s) to invest. As there is not much, but only some (e.g. Swanson, 2001; Bodin, Gordon & Loeb, 2005), extant theoretical literature about InfoSec tool usage in investment decision making *to what* to invest, author attempts to build a new InfoSec self-assessment tool blueprint through qualitative research, using design science research method (DSRM) and case study.

The research is carried out as a DSR, which is suitable for IT artefact development and to find solutions to understand research problem, or business need. Author attempted to create a more flexible, non-mathematical blueprint for organizations to better understand their specific InfoSec environment, and make more justified and proactive InfoSec investment decisions, as well as monitor the InfoSec environment more systematically.

The first contribution of this research is the preliminary blueprint that covers the most salient functionalities required from an InfoSec self-assessment tool, based on the examined literature. The preliminary blueprint (v1.0) was evaluated in case studies that included working life, i.e. organizations from manufacturing industry. Case studies brought valuable working life perspective to the blueprint development, and most importantly the interview results were in line with the recent studies. The interviewed organizations concurred that financial metrics are not suitable, or at least hard to use, for InfoSec investments, which confirms e.g. Shao (2015) and Moore et al. (2015) findings. The interview results also confirm that the organizations developing their own InfoSec frameworks are more likely to have better understanding of their InfoSec risks, and better answer to question "where our security begins and ends".

Based on the case studies, the refined blueprint (v2.0) emerged as the second contribution. The objective was to create as exhaustive InfoSec tool blueprint as possible, which covers organizational factors helping the InfoSec investment

decision-making. With the help of the new blueprint, organizational InfoSec investment decision-makers and tool developers can see what is needed from an InfoSec tool, reasoned with theoretical and empirical base.

This rest of the research is organized as follows: the rest of this chapter describes the research problem, motivation and goals, and central concepts. The second chapter analyses the InfoSec investment literature of the previous and the most recent research. Thereafter, chapter three describes the research design that was used. The fourth chapter describes the development and refinement of the InfoSec self-assessment tool blueprint through design science process. Chapter 5 presents contributions, implications and limitations of the research along with the potential future research. Chapter 6 concludes the research and its findings.

1.1 Research problem

Previous literature (see chapter 2) covers InfoSec investment mostly from mathematical, optimal investment point of view of" how much" to invest to InfoSec area(s), and not directly "to what" to invest. Also, the latest research (see chapter 2) argues that nowadays the classical models are not suitable solutions to cover the needs of organizations regarding InfoSec investment decision-making. Therefore, the problem investigated in this research is the lack of effective usage of InfoSec self-assessment tools in InfoSec investment decision-making to identify "to what" to invest. This leads to the following main research question:" What should an optimal InfoSec self-assessment tool include to assist InfoSec investment decision-making?"

1.2 Motivation and objectives

The impetus for this research came from author's own experience with InfoSec self-assessment tools and from working life that needed more systematic and proactive way to assess and prioritize the InfoSec investment targets. The InfoSec self-assessment tools alone are not adequate support in InfoSec management let alone investment decision-making, however, such tools can provide valuable information in many cases of InfoSec (investment) management. Also, as Moore et al. (2015) state, only a few Chief information security officers (hereafter CISO) mentioned using numeric metrics when prioritizing investments. Thus, it is important to identify CISOs' current real needs regarding InfoSec self-assessment tools that are needed in InfoSec investment decision making.

Literature on the subject (e.g. Gordon & Loeb, 2002; Huang et al., 2008; and Cavusoglu, Raghuntahan and Yue, 2008) show that the economic theories, such as economic benefit maximization and analytical hierarchical process, do not directly align with the current InfoSec self-assessment tools, because the tools do not always contain numerical information needed in the classical mathematical

models. However, some InfoSec tools can provide some of the information needed to conduct the classical investment calculations. While the economic models evaluate *how much* to invest in InfoSec (e.g. Shao, 2015, 120), InfoSec self-assessment tools help in identifying *to what* InfoSec area(s) investments are needed.

Earlier InfoSec research has focused mostly on technological side, but along the way scholars have noted that it is not sufficient to only study InfoSec technology. To effectively assess organizational InfoSec, people, processes and technology must be considered. Many information systems projects tend to fail, and this must be considered also in InfoSec investments. It is argued that the classical InfoSec investment models are not fitting well to real-life use, and decision-makers in organizations do not use them, but develop e.g. their own InfoSec self-assessment tools based on InfoSec frameworks to support the InfoSec investment decision making (Dor & Elovici, 2016, 2; Moore et al, 2015). Thus, based on the above, author identified the need for this research and motivation to conduct this research.

The purpose of this research is to develop an InfoSec self-assessment tool blueprint that would help organizations see, what needs to be considered to effectively identify *to what* InfoSec area(s) to invest. Thus, to address the purpose, author argues that InfoSec investment decision making process needs:

1. An InfoSec self-assessment tool that would help organizations to assess their InfoSec posture and operational InfoSec environment to see, what needs to be considered to effectively identify *to what* InfoSec area(s) to invest.
2. Identification of the key features in the InfoSec self-assessment tools that are of use in InfoSec investment decision making process.

Therefore, the objective of this paper is to develop an InfoSec self-assessment tool blueprint, which could help InfoSec investment decision-makers. To address the research question, an iterative process was used. First, the preliminary InfoSec self-assessment tool blueprint was composed informed by the existing literature. Then empirical case studies were used to demonstrate and assess the preliminary blueprint. Lastly, based on the case study assessments, author refined the preliminary blueprint and developed a consensus-built and empirically grounded InfoSec self-assessment tool blueprint. The objective was to create as exhaustive blueprint as possible, so that further research can test it more empirically.

1.3 Central concepts

Central concepts in this research are InfoSec tools, investments, frameworks, and decision-making process. These concepts are described below to define them in the context of this research.

1.3.1 IT artefact

IT artefacts are created to solve identified organizational problems. These IT artefacts can be constructs, models, methods, or instantiations, as well as may include social innovations or new properties of technical, social, or informational resources. In other words, any designed object with an embedded solution to research problem. (Peffers et al., 2007, 49.)

In this research, the artefact represents a blueprint (i.e., conceptual model) for an InfoSec self-assessment tool, which aims to help InfoSec investment decision makers in InfoSec investment decisions *to what* InfoSec area(s) to invest.

1.3.2 InfoSec self-assessment tool

InfoSec self-assessment tools can be anything between Excel spreadsheet and comprehensive GRC-tools, such as RSA Archer (RSA, 2016), or other ready-made tools, such as FFIEC cyber assessment tool (FFIEC, 2016). The purpose of the InfoSec self-assessment tool is to aid organization in InfoSec investment decision-making process to identify the InfoSec area(s) *to what* to invest.

1.3.3 InfoSec Investment

InfoSec investments include reduction of InfoSec risks, balance of business needs and InfoSec requirements, compliance management, and cultural fit (Shao, 2015, 16). Investment in this research is any allocation of resources, such as money or time, to improvement of InfoSec in different areas, such as people, processes, and technology.

1.3.4 Frameworks

Frameworks, in the context of this research, are e.g. standards, frameworks, and best practices used in InfoSec domain. Those include standards, such as ISO27001 (ISO, 2013), frameworks, such as NIST cyber security framework (CSF) (NIST, 2016), and other best practices, such as ISF standard of good practice (2016).

1.3.5 Decision making process

InfoSec investment decision making process consists of several phases that vary from organization and industry to another. Dor and Elovici's (2016) conceptual model for InfoSec investment decision-making process encompasses comprehensive list of concepts, categories, and associations within qualitative model that addresses the gaps in previous research (Dor & Elovici, 2016, 10). The model consists of the following categories and concepts (table 1).

TABLE 1. The full list of categories and concepts (Dor & Elovici, 2016, 4)

Categories (decision process phases)	Concepts
1. External environments of business	A. Strategy
2. Organizational structure or behavior	B. Constraints
3. Understanding of the cyber threat landscape	C. Quality
4. Current information security posture of an organization	D. Prioritization and budgeting
5. Information security gap analysis	E. Applying information security capabilities
6. Identifying the required capabilities	F. Organizational information security education and awareness
7. Identifying relevant alternatives	G. Information security compliance
8. Analysis of alternatives	H. Information security threats
9. Selecting a portfolio of projects	I. Risk management
10. Proof of concept	J. Decision makers
11. Decision and/or execution	K. Decision variables
12. Project initiation	L. Competitive advantage
13. Project planning	M. Doctrine and/or organizational policy
14. Project execution	N. Customer expectations
	O. Implementation
	P. Start-ups

In this research, author derives InfoSec decision making process from Dor and Elovici's (2016) process model, and Fenz, Ekelhart and Neubauer's (2011) AURUM architecture. The derived InfoSec investment decision-making process consists of the following five generic stages (figure 1):

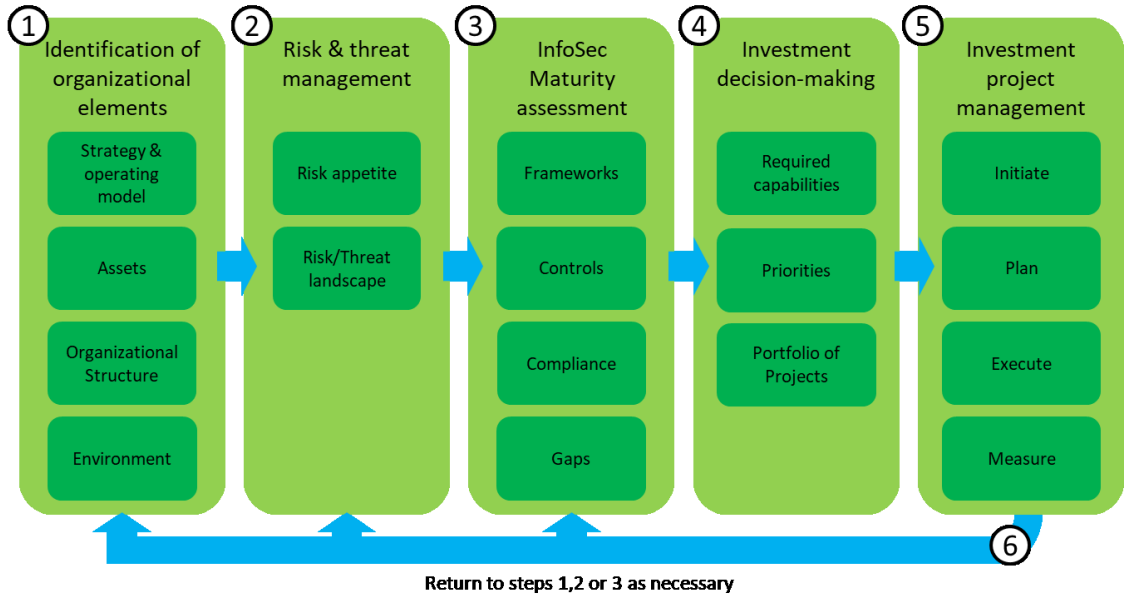

FIGURE 1. InfoSec investment decision-making process (derived from Dor & Elovici, 2016.)

2 Literature review

In this chapter, the previous studies on InfoSec investments is reviewed and covers the most common literature regarding the InfoSec investments. Existing literature was chosen from long enough time-period, from 2002 to 2015, to gain better view of the history of InfoSec investment theories and to compare the existing research to the latest research.

The literature review, which was conducted at earlier stage, is descriptive review, which is general review without strict rules. The phenomena under research can be described comprehensively and, when needed, compartmentalized to several attributes. Research questions are more casual than in systematic review or meta-analysis. (Salminen, 2011, 6.)

InfoSec investment literature information retrieval was conducted via Google, Google scholar, and university literature databases. The searches were conducted between 2016 and 2017 using search different terms, such as "information security tools in investment decision making process", and any combination of the previous separated by "AND". The examined literature is divided into categories describing their content, and to the most recent literature regarding the topic. Optimal InfoSec investment has been seen also as decision-theoretic (Shao, 2015) and the examination revealed that they are also mostly mathematical models. Table 2 provides a summary of the reviewed literature.

TABLE 2. Summary of the reviewed literature.

Study	Theory	Approach	Methodology	Key findings
Classical economic approaches				
Gordon & Loeb (2002)	Economic benefit maximization	Quantitative	Mathematical model	1.Firms should not necessarily invest to the information with highest vulnerability. 2.Optimal amount of investment never exceed 36,8%, typically much less.
Matsuura, K (2003)	None	Quantitative	Mathematical model	1.Improved the Gordon & Loeb (2002) model
Bodin et al., (2005)	Analytical hierarch process	Quantitatve	Qualitative process and mathematical model	1.AHP model to help organizations to compare e.g. proposals and determine optimal allocation of InfoSec budget.
Hausken, K. (2006)	Economic benefit maximization	Quantitative	Mathematical model	1.Further investigates Gordon & Loeb (2002) model. 2.Four marginal returns to InfoSec investment.

Huang et al. (2006)	None	Quantitative	Mathematical model	1.Organizations with small budget should allocate resources to one class of an attack (distributed or targeted).
Huang et al. (2008)	Expected utility theory	Quantitative	Mathematical model	1.Not all InfoSec risks are worth investing against. 2.Optimal level of InfoSec investment does not increase with aversion to risks. 3.Optimal InfoSec investment does not does not always go up with its effectiveness.
Cavusoglu et al. (2008)	Game theory	Quantitative	Mathematical model	1.Decision-theoretic techniques are incomplete to determine InfoSec investment levels. 2.Sequantial game (theory) results in the maximum payoff to a firm that leads and hacker follows.
Huang & Behara (2013)	None	Quantitative	Mathematical model	1.With small InfoSec budget organization should invest into one class of attack. 2.With connected and open information systems organizations should invest to defend against targeted attacks.
Gal-Or and Ghose (2005)	Game theory	Quantitative	Mathematical model	1.Information sharing is more valuable with products with higher substitutability. 2.Sharing alliances yield greater benefits, which increase with firm size.
Chai, Kim and Rao (2011)		Qualitative	Event methodology	1. InfoSec investment announcements lead to positive abnormal returns for organizations stock market price

Behavioural economic approach				
Cavusoglu et al. (2010)	None	Qualitative	Literature review on psychology and behaviourism	1.Decision makers do not possess complete information regarding InfoSec risks and alternatives to deal with the risks. 2.Decision-making process is not immune to non-economic forces that affect decisions. 3.Remove ambiguity about InfoSec risks, clarify benefits associated with investment, and foster InfoSec awareness.
Beebe et al. (2014)	Prospect theory	Qualitative	Survey on framing effects	1. InfoSec investment decision-makers are not rational. 2.Risk perception and individual level biases need to be considered in InfoSec investments.
Alternative approaches				
Shao. (2015)	Herding theory	Qualitative	Field study	1.Framework for InfoSec investments. 2.Classical frameworks (above) are problematic in InfoSec investments. 3. InfoSec investment managers should pay attention to what influences the investment decision-making.
Moore et al. (2015)	None	Qualitative	Semi-structured interviews, survey	1.Almost all CISOs use frameworks prioritize InfoSec investments. 2.Focus is on process measures, not outcome.
Dor & Elovici. (2016)	Grounded theory	Qualitative	Open-ended interviews	1.Conceptual model for InfoSec investment decision making process. 2.Holistic theory of decision phases and involved stakeholders.

2.1 Classical economic approaches

Gordon and Loeb (2002) presented an economic model with which one could calculate the optimal amount to invest in InfoSec. The model considers the vulnerability of the information and the potential loss from the vulnerability affects the optimal amount of investments to InfoSec. Their analysis indicated that maximum amount a risk-neutral firm should invest is only a fraction of the expected loss. The fraction is <37% within their two broad classes and in most cases far less than 37%. As a result, some investment in InfoSec is reasonable, but sometimes investing more to certain area of InfoSec is not always worth the cost. Their analysis also shows that investment to InfoSec in some areas does not increase with the level of the vulnerability, and thus normally, with their second-class function, investments should focus on the midrange areas. The limitation of their study is that it is a single-decision maker model that does not consider the potential attackers' strategies, i.e. they did not consider the game theoretic aspects. (Gordon & Loeb, 2002, 439-440; 453.)

However, already in 2003 Matsuura (2003) argued that Gordon and Loeb's (2002) model fails to incorporate an important variable in the model, which is InfoSec insurance (Matsuura, 2003, 6). Matsuura (2003) argued that as the loss in Gordon & Loeb's (2002) model is not a constant but a variable as InfoSec insurance reduces the losses. Matsuura (2003) also argued that as the investment is continuous in Gordon and Loeb's (2002) model, investment subjects are not treated as discrete pieces but as a whole. Matsuura (2003) then proposed improvements to Gordon and Loeb's (2002) mathematical model by adding InfoSec insurance, however goal being also optimum solution.

Bodin, Gordon and Loeb (2005) investigated analytic hierarchy process (AHP) to address the issues of how to spend InfoSec budget and how to justify the decisions to organization's financial officer. As the authors, Gordon and Loeb, have made the previously mentioned model (2002), they refer to their work and surprisingly already then (2005) state that the traditional economic approaches are severely constrained. However, the AHP process is a rating method to determine the optimal allocation of InfoSec budget, and offers a simple mathematical model to compare the e.g. proposal in the light of the AHP tree that consists of areas of goals to improve the InfoSec system, its sub-categories of confidentiality, integrity and availability, and their sub-categories. (Bodin et al., 2005, 80-81.)

Hausken (2006) evaluates Gordon and Loeb's (2002) model and makes four mathematical models of marginal returns to InfoSec investment. Hausken (2006), however, argued that his models are not capped to the level for Gordon and Loeb (2002) model. Other extension to Gordon and Loeb (2002) model have been made by e.g. Willemson (2006), Wang (2009), Tatsumi and Goto (2009), and Willemson (2010.)

Huang, Behara and Hu (2006) also proposed an economic, mathematical model, which was different from previous single-scenario models, that consid-

ered simultaneous attacks from multiple sources, and from the gained information make an optimal investment (Huang et al., 2006, 1). Their model would show how an organization should allocate resources to defend against distributed and targeted attack simultaneously. They followed Gordon and Loeb (2002) by assuming that the firms are risk-neutral, and used their classes in the calculations. As a result, organizations with small InfoSec budgets should allocate most or all resources against one class, distributed or targeted, of attack.

Huang et al. (2008) made economic analysis of the optimal InfoSec investment in the case of a risk-averse firm using the expected utility theory. They identified that earlier academics has primarily focused on the technical and behavioural side of the InfoSec, and that analyses based on economic principles were rare. They refer to Gordon and Loeb (2002) in their article, but state that their study was too limited. Huang et al. (2008) applied classical economic theories to offer new insight to determining the optimal InfoSec investment. (Huang et al., 2008, 793-794.)

Huang et al. (2008) did their analytical framework similar to Gordon and Loeb (2002), but with different boundary conditions and assumptions, such as the decision maker in a firm is risk-averse as opposed to the risk-neutral decision maker in Gordon and Loeb's (2002) study. They believed that a significant number of firms willing and able to invest in InfoSec are risk-averse, and thus their model would offer valuable insight how firms should make decision when investing to InfoSec. (Huang et al., 2008, 795.)

Like Gordon and Loeb (2002), Huang et al. (2008) used two broad classes that determine the investment values for InfoSec investment. Their model offers insight in three propositions, which include relationship between optimal InfoSec investment and potential loss, extent of risk aversion, and investment effectiveness. Thus, their model indicates that not all InfoSec risks are worth protecting against and optimal investment in InfoSec does not always go up with the effectiveness of such investment. Therefore, InfoSec managers should evaluate the vulnerabilities and potential losses before deciding whether the investment to address the vulnerabilities is justifiable. They also identified that optimal InfoSec investment does not necessarily increase with one's aversion to risk, because like other investing, investing in InfoSec carries its own risk, e.g. not working. Organizations should also identify the main IS threats before determining the investments. (Huang et al., 2008, 801.)

Cavusoglu et al. (2008) assessed decision-theoretic techniques and adapt game-theoretic approach to InfoSec investments. They state that decision theoretical traditional risk analysis methods provide useful starting point for determining the InfoSec investment level, but are incomplete because of the strategic nature of InfoSec issues. The strategic nature implies that hackers do not randomly select their targets, but make their choices rationally and based on the amount of effort to succeed in hack. The traditional models are limited, when applied to InfoSec problems, because they do not allow organizations' InfoSec investments to influence the behaviour of hackers. (Cavusoglu et al. 2008, 282-283.)

Cavusoglu et al. (2008) state that also their work was inspired by Gordon and Loeb (2002) (Cavusoglu et al. 2008, 285). Cavusoglu et al. (2008) describe the InfoSec investments as general information technology (hereafter IT) investments, but the context is different as in InfoSec, organizations are often dealing with strategic adversaries who attack systems that are vulnerable. Therefore, organizations should act strategically when investing in InfoSec. Choosing the InfoSec investment level organizations cannot treat the InfoSec risk environment as static. To accurately analyse the InfoSec investment decision, one needs to model the threats and vulnerabilities, which are determined by the strategic interaction between organizations and hacker(s). (Cavusoglu et al. 2008, 285.)

In the decision theory, the firms assume that their decision has no impact on the adversary and thus they estimate adversary effort along with probabilities and use them as parameters in its payoff maximization model to find the optimal investment level (Cavusoglu et al. 2008, 8). In the game theory, firms make decisions by anticipating the behaviour of the strategic adversary in response to its action. Timing of actions, both organization's and adversary's, state the nature of the game as actions can be simultaneous or sequential. In the simultaneous game organization and adversary make effort and investment decisions simultaneously, whereas in sequential game the other makes investment decision first and the other makes it decision after learning the preceding investment decision. (Cavusoglu et al. 2008, 9.)

Cavusoglu et al. (2008) conclude their study by stating that organizations realize maximum payoff when the organization and adversary play a sequential game, in which the organization is the leader and makes the decisions first as well as commits and communicates the strategy to adversary. Even though the organizations do not communicate their decisions and thus play a simultaneous game with adversary, the organization gets higher payoff than using decision theoretic approach to determine investments. However, they found that if an organization uses traditional decision theory to set the investment level, then over time its behaviour approaches the simultaneous theory game. (Cavusoglu et al. 2008, 298-299.)

Huang and Behara (2013) developed an analytical model for InfoSec investment that considers concurrent heterogeneous attacks with distinct characters. The relationships among major variables can be investigated via analytical and numerical analyses subject to various boundary conditions. The results state that organizations with small InfoSec budget should concentrate their investments on only one class of attack, even other threats from other classes exist. When organization's information systems are highly connected and open, and thus vulnerable to targeted attacks, it is more beneficial to allocate InfoSec budget to defend the targeted attacks.

Gal-Or and Ghose (2005) used game theory to develop an analytical framework to study competitive implications of sharing information and investments in InfoSec technologies. They attempted to answer to question, "what are the economic incentives for competing firms in a given industry to share security infor-

mation?" They used mathematical model to investigate the topic, and their results indicate that sharing information is more valuable when product substitutability is higher and sharing alliances result in greater benefits, which increase with the size of the firm.

Chai, Kim and Rao (2011) utilized event methodology to study value of InfoSec investments based on stock market investors' behaviour towards organizations' InfoSec investment announcements. They had recognized that organizations have problems allocating resources to InfoSec and measure the costs and benefits of the investments. Also, due to rapidly developing technologies, it is difficult to get enough information to evaluate InfoSec risk likelihood and costs. They proposed that organizations InfoSec investment activity affects the (market) value of the organization, and if disclosing the InfoSec investments have tangible valuable impact to organization, it is evidence for value of the InfoSec investment. As a result, they found support for their hypothesis that InfoSec investment announcements lead to positive abnormal returns for organization's stock market price.

2.2 Behavioural economic approach

Cavusoglu (2010) investigated the obstacles what decision-makers face when making InfoSec investment decisions and how to deal with them. Traditionally, economics assume that decision-makers are fully informed about available alternatives and eventualities regarding the decisions, and thus capable of making the best investment decisions. However, they do not always have enough time of computational capability to make use of available information, and they also have cognitive and computational limits that are prone to psychological biases and rely on shortcuts in decision making. (Cavusoglu, 2010, 53.)

Cavusoglu (2010) examines literature in behavioural economics and psychology, which have studied the hindrances in decision-making. Cavusoglu examined Gordon and Loeb (2002) as well and other economic theories, but added the behavioural and rational human biases and fallacies to the mix. (Cavusoglu, 2010, 54-55.)

Decision-makers in many organizations base their investment decisions on the identified InfoSec risks, associated initiatives, and how they perceive them. The purpose of the InfoSec investments is to eliminate or mitigate the risks and ensure the safety of organizational assets. However, the negative outcomes associated with InfoSec risks are not easy to fathom, and thus executives may not comprehend the potential damage InfoSec risks can cause when materialized, because they may not be familiar with or have experience of them. Therefore, incomplete information limits the ability to make reasonable InfoSec investment decisions. In figure 2 can be seen the incomplete information used in decision-making, and influencing cognitive/ psychological biases affecting the InfoSec investment decision-making. (Cavusoglu, 2010, 57-59.)

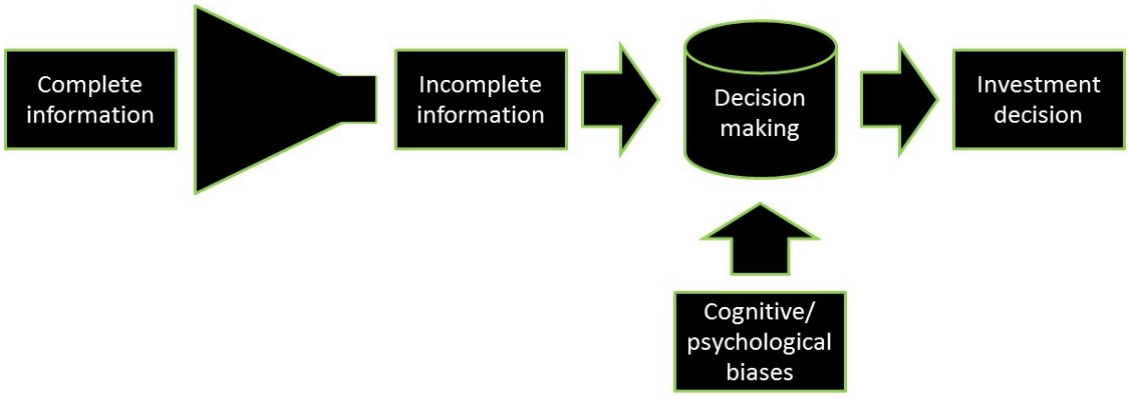

FIGURE 2. Drivers of decisions and impediments of proper decision making. Modified from Cavusoglu (2010, 58).

Even though the InfoSec investment decision are mostly based on risk evaluation, decision-makers might not properly evaluate them, since the absence of InfoSec risk might be due to sheer luck. The organizations that have not been the target of a breach might believe that their InfoSec management is stronger than average, even the industry reports state that they are exposed, and thus underinvest to InfoSec. (Cavusoglu, 2010, 61-62.)

No organization is immune from biases and fallacies when assessing InfoSec risks, but being aware of those, decision-makers can focus on eliminating them or to reduce their impact. Cavusoglu (2010) states three ways to help decision-makers in decision making: removing ambiguity about InfoSec risks, clarify benefits of the risk-mitigating investment, and fostering awareness of InfoSec. However, organizations should first identify the existing biases, and just then can they determine solutions rooted in the one previously mentioned solution. (Cavusoglu, 2010, 63-67.)

Beebe, Young and Chang (2014) investigated the presumption that InfoSec decision makers are entirely rational and empirically validated their hypothesis, which pointed out that decision makers exhibit preference reversals when facing competing budget alternatives. They also argued that the accepted rational choice and economic models for InfoSec investments needs to consider risk perception and individual level decision biases.

As Cavusoglu (2010) above showed in figure 1, also Beebe et al. (2014) see that individual decision-makers are significant input variables and thus influence the organizational decision-making. Therefore, the individual decision-making biases need to be considered. Beebe et al. (2014, 135) see this important, as the classical economic models for InfoSec do not account for or acknowledge the potential for preference reversals, but see the decisions as rational. They argue that the classical economic models could improve, if the framing effect and other biases are incorporated.

2.3 Alternative approaches

Earlier research on the covered topic has developed economic models and frameworks for InfoSec investments and has focused on how much to optimally invest to InfoSec. However, they are mostly relevant in specific phases of investment decision-making. Also, the classical models assume laboratory conditions and do not include decision making process and factors affecting it (Dor & Elovici, 2016, 2). As the previous research focuses mostly on economic models, Dor and Elovici (2016) identified the need to develop an up-to-date conceptual model that represents InfoSec investment decision-making process. They also modelled concepts that affect each phase of the process and what actions should be taken to avoid biases.

Shao (2015) made a doctoral thesis about understanding the information system security investments and argues that the prior models are flawed for two reasons. Firstly, benefit maximization is not appropriate model for InfoSec investment as the benefits and costs of InfoSec investment cannot be reliably calculated. Secondly, decision-makers are not unbiased rational actors. (Shao, 2015, 3.)

Shao (2015) stated that information regarding the risks, costs and benefits of InfoSec investment are important in decision-theoretic models, but it is challenging to have reliable data. In the game-theoretic models, on the other hand, it is essential to understand adversary's strategy, which, however, is difficult as they often have different value system from organizations.

Shao (2015) argued that the prior InfoSec investment studies were based on neoclassical frameworks of decision-making and assumed that decision makers have rational preferences, have complete information, and seek maximal benefits or payoff. Also, the previous studies ignored the characteristics of InfoSec investment described by Shao (2015, 37-41) and none of them discussed intangible benefits of InfoSec investment. (Shao, 2015, 24;31;36;43.)

The results of Shao's (2015) research indicate that reputational herding is a significant motivation for InfoSec investment and confirm the proposed framework (Shao, 2015, 51;58; 83-84). Firstly, it confirms that maintaining compliance is strong motive on InfoSec investments. Secondly, as the decision makers have limited ability to measure the value if InfoSec investments, they increasingly tend to follow other organizations to maintain good reputation. Also, as the decision makers have inaccurate knowledge and incomplete information, they are highly unlikely to discover or maintain the optimal profit-maximizing solutions. (Shao, 2015, 109-110.)

Moore et al. (2015) conducted a research, in which they kept semi-structured interviews with CISOs about threat management, management support, metrics in investment decision-making, as well as recent large InfoSec investment projects. (Moore et al. 2015, 2-3.)

In the interviews came up that CISOs make their case to get more budget to InfoSec by using frameworks to articulate message to senior leaders. For example, one organization hired a new CISO after a large breach and the CISO created a

custom framework based on ISO and NIST guidelines, and satisfied the management that it was a solid investment plan. Other way to win budget was to point out compliance obligations. However, one CISO remarked that it is not the main reason, as it is often seen as minimum thing to do to "get a check mark". (Moore et al. 2015, 5.)

Moore et al. (2015, 7;15) also asked from the CISOs that how InfoSec investment decision are made and how they deal with asymmetric information. The biggest drivers for InfoSec investments, based on the interviews, were perceived risk reduction and compliance. CISOs reported that compliance drives significantly and most reliably the overall InfoSec budget, but at least one CISO stated that "good compliance does not equal good security." Unlike the prior theories above tried to reach benefit maximization, CISOs saw that cost reduction was the least important driver. (Moore et al. 2015, 7-8.)

Organizations identified and prioritized the most important threats to their organization by using mostly industry best practices and frameworks, closely followed by past attacks on the organization. Quantitative measures, e.g. return on investment and net present value, came in fourth, and only a few CISOs mentioned using numeric metrics when prioritizing investments. (Moore et al. 2015, 8-10.)

InfoSec self-assessment tools are usually based on one or multiple acknowledged frameworks, and frameworks are used for multiple purposes ranging from compliance to risk assessment to prioritization. In self-assessment tools, frameworks are usually used to assess InfoSec maturity, to identify gaps, and prioritize investments. Many organizations utilize well-known frameworks, such as NIST, ISO 27000, and COBIT, while others create their own frameworks based the aforementioned or entirely their own. The use of frameworks varies from organization to organization, and from country to country. For example, in US NIST guidelines are required by Federal Information Security Management Act of 2002 and thus create the priority for local CISOs to comply. However, there is dissonance between the frameworks and organizations' perceptions of risks, which has led the organizations to consider simpler frameworks that align with their expectations. (Moore et al. 2015, 11-12.)

The framework development at higher level, whether standard or custom, incorporates elements of business assets, processes, vulnerabilities, and probabilities. The differences that came up in the interviews lie in specific environments, cost of remediation, and other internal or external knowledge. One custom framework was based on FFIEC handbook and ISO27001, and NIST CSF was added later to make it more comprehensive. As a result, the framework is used to assess assets, controls and compliance across the entire enterprise. (Moore et al. 2015, 13.)

The InfoSec frameworks commonly used nowadays make executives think about their organization form risk perspective and their use indicate maturation of InfoSec management. However, there remains concern that even CISOs use mature tools, they may not be using them effectively, i.e. they are using them as

"checkbox" lists. Thus, Moore et al. (2015) sense that the organizations developing their own InfoSec frameworks are more likely to have better understanding of their InfoSec risks, and better answer to question "where our security begins and ends". (Moore et al. 2015, 14-15.)

As e.g. Cavusoglu (2010) shows in figure 1 and Shao (2015) states above, CISOs deal with asymmetric/incomplete data/information. For example, organizations misunderstand the severity of threats and thus do not know how it is being attacked, possibly leading to wrong allocation of resources. However, 45% of the interviewed CISOs felt they had enough information to manage InfoSec risks and prioritize threats. On the other hand, those who answered "no" were worried about blind spots. (Moore et al. 2015, 15.)

Moore et al. (2015) identified that almost every CISO they interviewed used frameworks to define organization's InfoSec status and to prioritize investments. They also found that there was more focus on process measures than outcome measures, i.e. finding gaps between current and desired InfoSec posture, and focusing on controls. CISOs also discuss about threats and opinions on InfoSec applications and devices, which indicates that Shao's (2015) reputational herding is on the spot. However, they conclude their study speculating the contradiction between CISOs' confidence in frameworks and continuous high-profile breaches, as this might be the result of overconfidence in process-based measures and lack of measuring IS outcomes. (Moore et al. 2015, 29-30.)

2.4 Summary of the literature

The examined literature shows that the InfoSec investment theories and tool models are various, and approaches have changed during the last fifteen years. The transition from stricter mathematical, quantitative models from classical economic approaches to more open, qualitative models and theories of alternative approaches can be seen in the literature.

The main view in the alternative approaches is that the classical theories and models are problematic in InfoSec investment decision-making, and more holistic approach should be taken in InfoSec investments. For example, as the behavioural economic approach describes, decision-making in general contains several cognitive/psychological biases and fallacies that should be considered in (InfoSec investment) decision-making process. Also, InfoSec investment decision-makers do not possess complete and perfect information to make fully rational decisions, which are affected by non-economic forces.

3 RESEARCH DESIGN

This chapter sheds light on the research design used in this research and the reasoning for it. Firstly, the research approach of this research is explained. Then design science process is described in detail. Empirical part of the research, along with the data collection and analysis methods, are explained in chapter 4.

The scope of this research was set to cover responsible persons of InfoSec, such as CISOs, from manufacturing industry companies. Initially, 8 organizations were contacted, but only 50% of the contacted persons accepted the interview, and thus adjustments to the research were made accordingly. More organizations were contacted, but author did not get any more interviews, and therefore the population in this study remained in 4 cases.

The problem centred approach (entry point) to DSR is used to find solution to the research problem and working life needs. DSRM is a justified (prescriptive) method as it permits the author to create an IT artefact that would contain features that it *should have,* instead of describing how *things are*, as in descriptive approaches.

The research problem (chapter 1.1), and motivation and objectives for this research (chapter 1.2) form the beginning for the DSR process. First, the assumptions for the preliminary blueprint (v1.0) were examined using descriptive literature review, which is described in the previous chapter. Then the preliminary blueprint was designed informed by the existing literature. Secondly, empirical case studies were used to demonstrate and evaluate the preliminary blueprint. Lastly, based on the case study, author refined the preliminary blueprint and developed a consensus-built and empirically grounded InfoSec self-assessment tool blueprint (v2.0).

3.1 Research approach

The approach and nature of this research is qualitative (Hirsjärvi, Remes & Sajavaara, 2009, 160-166) and more specifically prescriptive (design-science), which means that author attempted to identify what kind of (effective) features InfoSec self-assessment tools "*should have*" (Gregor, 2006, 613; Hevner, March, Park & Ram, 2004, 98), instead of descriptive approach that examines how "*things are*". Based on the background described in previous chapters, author decided to conduct Design Science Research (DSR), which is inherently a problem-solving process (Hevner et al., 2004, 82). In the chapters below the research design is described in more detail.

The research methods in this research were Design Science Research Method (DSRM) (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007) and case study (see chapters 4.2.1 and 4.2.2 for more details), through which author attempted to develop a blueprint for an InfoSec self-assessment tool. Like Peffers

et al. (2007) refer to Simon (1969), "Whereas natural sciences and social sciences try to understand reality, design science attempts to create things that serve human purposes (Simon, 1969, 55)". They, however, state that reasonably sound idea of design science is that it creates and evaluates IT artefacts intended to solve identified organizational problems (the lack of effective usage of InfoSec self-assessment tools in IS investment decision-making to identify" to what" to invest). These artefacts vary from constructs to models and may include social innovations or new properties of technical, social, of informational sources. This includes any designed object with solution to understand research problem, or business need. (Peffers et al., 2007, 49; Hevner et al. 2004, 79-80.)

Peffers et al. (2007, 49) refer to several rules that should be followed when conducting a design science study, and the most important one is the mentioned creation of artefacts to address a problem in hand. Artefact's utility, quality and efficacy must be evaluated, research must attempt to represent verifiable contribution, and rigor must be applied in development and evaluation. The development of an artefact should draw from extant literature and knowledge to come up with a suitable solution. Lastly, the results must be communicated to appropriate audiences. (Peffers et al., 2007, 49.)

3.2 Design science research process

Peffers et al. (2007) built a process for DSR that was constructed of well-accepted elements from influential prior research. The process model consists of six steps that the author followed in this research. Figure 3 describes the process phases and below is detailed description of each phase. (Peffers et al., 2007, 52.)

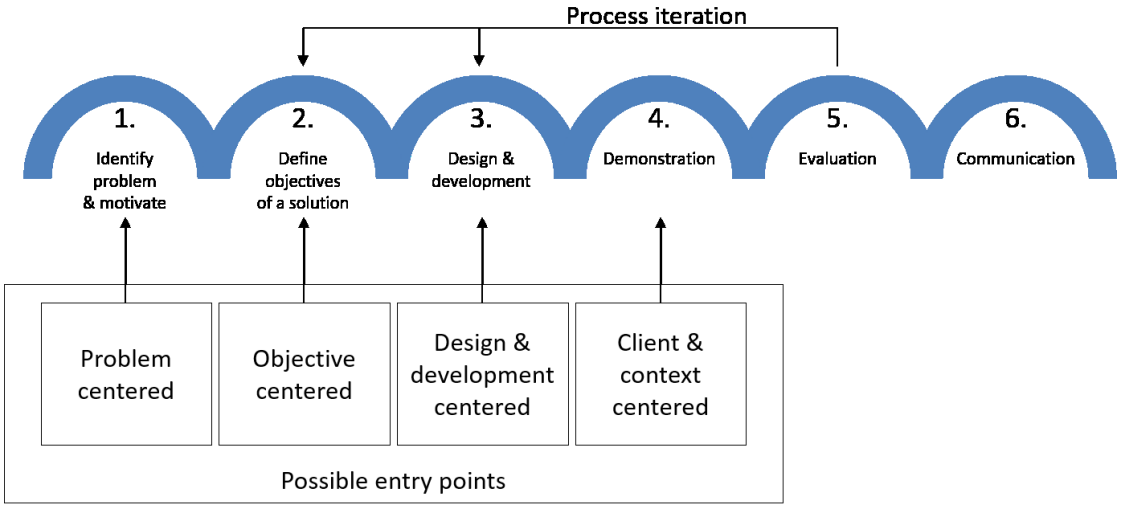

FIGURE 3. DSR process model (Peffers et al., 2007, 54).

The first activity is problem identification and motivation, which defines research problem and justifies the value of the solution. Justifying the value of a

solution (artefact) motivates both researcher and audience of the research to pursue the solution and to accept the results. It also helps to understand the reasoning of the author's understanding of the problem. Knowledge of the state of the problem and the importance as well as motivation of this research are described earlier in chapter 2. (Peffers et al., 2007, 52-55.)

Identified problems do not always translate into objectives, because the process of design is one of partial and incremental solutions, and thus, after the problem is identified, the next step is to determine the performance objectives for a solution. Therefore, the next activity is to define the objectives for the solution, which means inferring the objectives from the problem definition and knowledge of what is possible and feasible. Objectives can be quantitative or qualitative, but author aimed for qualitative objectives, such as how the new artefact is expected to support the identified problem not addressed before. Knowledge of the state of problem and current solutions, if any, is needed and author has described them in the chapter 2.1. (Peffers et al., 2007, 55.)

The core of design science is the design and development step. The goal is to create a purposeful artefact that can be e.g. constructs, models, methods, or instantiations. The artefact can be any designed object, in which the research contribution is embedded. Artefacts are rarely full information systems, but innovations that define the ideas and products through analysis, design and implementation and use of information systems (Hevner et al. 2004, 83). This, third, step includes determination of desired functionality, its architecture, and the creation of the actual artefact. (Peffers et al., 2007, 55; Hevner et al. 2004, 82.)

The next, fourth step is to demonstrate the use of artefact to prove that the idea works, or see if not. The objective was to see if the artefact solves one or more instances of the research problem. This could have involved e.g. experimentation, simulation, case study, proof or other suitable activity. In this research, author used case study, i.e. interviewed representatives of manufacturing industry organizations to demonstrate the current blueprint and to get evaluation from these organizations (see next step) to see if it needs refinement or not. (Peffers et al., 2007, 55.)

The next step, evaluation, means observing and measuring how well the artefact supports the solution to research problem. Evaluation means comparing the determined objectives to actual results from the demonstration. Evaluation can take many forms, such as quantitative performance measures, satisfaction surveys, or client feedback. Artefacts can be evaluated by e.g. completeness, accuracy and usability (Hevner et al., 2004, 85). At the end of the evaluation, researcher decides whether to iterate back to step 3 to improve (see chapter 4) the artefact or to continue to the last step, communication, which in this case is the final thesis. (Peffers et al., 2007, 56.)

The last step is communication, which includes problem definition and its importance, the artefact itself, its utility and novelty, rigor of its design, and its effectiveness to researchers and other audiences (Peffers et al., 2007, 56). Also, research should be presented to both technical and management-oriented audiences (Hevner et al., 2004, 90).

The process described above is structured in sequential order, but it is not expected to be followed in order from step 1 to step 6. A research can start (figure 2) almost from any step and proceed as seen suitable for research's needs (Peffers et al., 2007, 56.)

Peffers et al. (2007, 57-70) gave examples of different approaches to DSRM and author adapted the first example (case 1) in this research. In the case 1, the investigators adopted a problem-centred approach, in which they identified the lack of automated support in data gathering in health care. This caused trend analyses to be cost prohibitive and, therefore, the need for more efficient automated data access arose to develop a better data warehouse. (Peffers et al., 2007, 57.)

Above described, problem-centred, approach was a justified approach and logical choice as the author has worked with the InfoSec self-assessment tools and identified the need for investigation of InfoSec tools in InfoSec investment decision-making. The chosen approach was suitable for solving the research problem and it was possible to conduct within the planned schedule. Author started with problem identification (step 1) and setting the objectives (step 2) for the results, followed by the design (step 3) of a preliminary blueprint of InfoSec tool for InfoSec investment decision-making.

After this, demonstrations (step 4) in selected organizations (cases) were conducted to demonstrate the preliminary blueprint and get more information on what kind of tools these organizations use, if they use any, in InfoSec investment decision making. To evaluate (step 5) the artefact, author used the previous knowledge base to build arguments for artefacts utility (Hevner et al., 2004, 86), and the interview results indicated needs to improve the blueprint (see chapter 4). There emerged a need to refine the previous blueprint, and author iterated back to step 3 to develop the blueprint further. Then step by step author proceeded towards the communication (step 6) and the final thesis communicated the results to relevant audiences.

Connection between understanding, executing and evaluating the research can be seen in figure 3. Business need and preliminary blueprint, applicable knowledge, leads to development of the artefact (new blueprint, i.e. the artefact), which in turn is applied in appropriate an environment and increases the knowledge base.

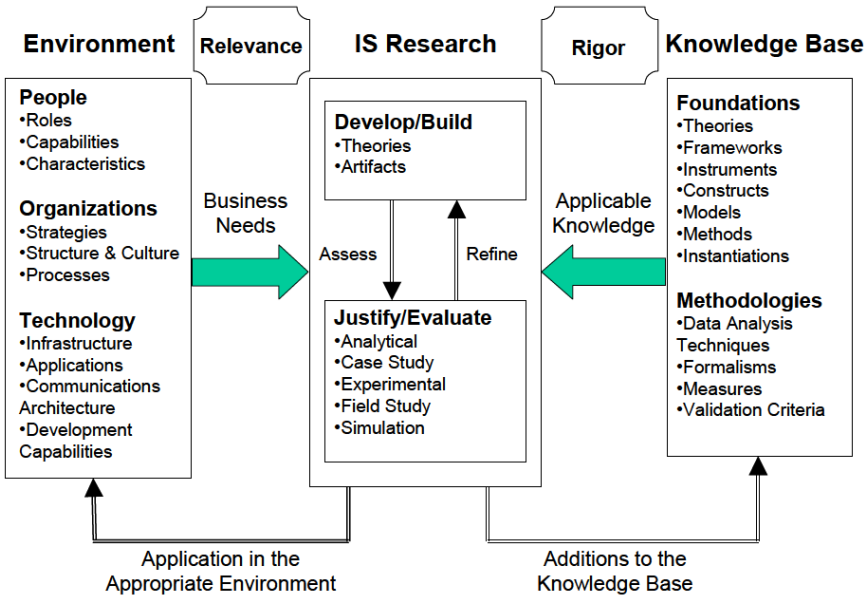

FIGURE 3. Relevance and rigor of research (Hevner et al., 2004, 80).

4 INFORMATION SECURITY SELF-ASSESSMENT TOOL BLUEPRINT

This chapter describes the process of the development of the conceptual InfoSec self-assessment tool blueprint. First, the preliminary blueprint (artefact v 1.0) and its development is described within design science process steps 1-3. Second, refinement needs for the tool concept were identified through case study and preliminary tool concept demonstration and evaluation. Lastly, tool refinement is described based on the empirical study.

4.1 The artefact (v. 1.0)

To further investigate the topic regarding the research questions, some self-assessment tools were examined to get broader and better view of the existing tools, and to evaluate their feasibility in InfoSec investment. Existing literature (chapter 2) was examined to see what is lacking in the current research and then author proceeded to create the preliminary blueprint for an InfoSec self-assessment tool that aims to help in "*to what*" InfoSec area(s) to invest, as opposed to "*how much*" handled in the extant literature. The chosen literature review languages were limited to Finnish and English, because of the limited time and other resources to examine the literature in other languages.

The InfoSec self-assessment tools were identified in both international and national, Finnish environments. The tools were identified from author's previous work and information retrieval of other tools were searched via Google and Google scholar. InfoSec investment literature information retrieval was conducted also via Google, Google scholar, and university literature databases.

4.1.1 Problem

Organizations need to understand their operational environment, current InfoSec capabilities and status of the InfoSec to make informed decision regarding InfoSec investments that mitigate InfoSec risks to acceptable level. This is where InfoSec self-assessment tools can help. Tools can help to understand the needs for InfoSec improvements, what is the effectiveness level of InfoSec, and helps e.g. auditors to assess organization's InfoSec posture. Therefore, whatever the organizational need is regarding InfoSec investments, a self-assessment tool that fills these needs can provide significant support to InfoSec investment decision makers. (e.g. Swanson, 2001, Bodin et al., 2005.)

Earlier self-assessment tools, such as Federal information technology security assessment framework (NIST, 2000), have provided help in evaluation of organizational InfoSec programs. They were implemented commonly in Excel, but had also similar features as current self-assessment tools, such as questionnaires

and effectiveness levels, i.e. capability maturity levels (Swanson, 2001). Nowadays, the InfoSec self-assessment tools range from comprehensive Governance, Risk, Compliance (GRC)-tools to singular tools, usually covering one or a few InfoSec frameworks, e.g. NIST cybersecurity framework (NIST, 2016), and hence their structure varies from product to another. Some tools are more advanced and have integrated frameworks that cover multiple InfoSec frameworks in one assessment, and thus offer comprehensive support for InfoSec investment decision-making, but are usually more expensive and require skilled implementation. Other, more limited and less integrated, tools may serve their purpose in certain organizations, because they are more affordable, less complex to implement, and suitable e.g. for smaller organizations. Organization's size, industry, and other organization-specific needs should be assessed before self-assessment tool selection.

Even though the self-assessment tools are in the market in various forms, to author's best knowledge there is not much, if any, research regarding InfoSec self-assessment tools that can be used to help organizations to assess *to what* to target InfoSec investments. Tools are mentioned in some studies (e.g. Moore et.al., 2015), but they are seen mainly as supporting factors in InfoSec management.

Decision-making in InfoSec investments has been under research for quite a long time (e.g. Cavusoglu, 2008; Gordon & Loeb, 2002; Huang et al, 2008 & Shao, 2015). The theories vary from Gordon and Loeb's (2002) two-class model to analysis of risk-averse decision-maker by Huang et.al. (2008) to decision- and game-theoretic approaches by Cavusoglu et.al. (2008) to Shao's (2015) framework of information system security investment based on reputational herding.

However, as Shao (2015) states, benefit maximization is not suitable goal for InfoSec investment in practice, but needs e.g. balancing the organizational needs, reduce InfoSec risks, and maintaining compliance (also Moore et.al., 2015). Thus, prior research treats InfoSec investment as a calculation problem (Shao, 2015, 17). Shao (2015) attempted to answer to question "what needs to be considered to understand InfoSec investment" and developed a framework as an answer. The framework was not tested regarding the distribution of InfoSec investment and the study did not cover self-assessment tools in the context of InfoSec investment (Shao, 2015, 109). Therefore, based on the content of the extant literature, author identified the need for and importance of research around InfoSec self-assessment tools in InfoSec investments.

4.1.2 Objectives

The goal regarding the preliminary blueprint was to investigate how the InfoSec self-assessment tools can support the decision-making in InfoSec investments. Then based on the examined literature, author creates a theory-grounded blueprint that depicts what is needed in the tools to bring value to InfoSec investment decision-making, specifically regarding "to what" to invest, as this would be the main solution to the presented research problem.

The goal was to create as exhaustive blueprint as possible to identify the key functionalities that affect the InfoSec investment decision-making. The literature was examined to identify the critical components in InfoSec investment decision-making, to which InfoSec self-assessment tools might provide support. After the theoretical part of the research, in empirical part the preliminary blueprint was demonstrated to the case organizations, after which the objective was to refine the preliminary blueprint based on the collected information.

4.1.3 Design

This chapter describes the creation of the preliminary blueprint for InfoSec self-assessment tool that would aid organizations in InfoSec investment decision-making. The creation of the blueprint is discussed and how it was formed based on the examined literature and author's experience with the existing tools.

As the organizational assets have become more and more informational and the need to protect these assets is increasingly critical issue (Shao, 2015, 120), the tools should have the functionality to describe the organizational structure and organizational assets (Moore et al. 2015, 12-13; Shao, 2015, 37). Criticality assessment should be available to sort the (business) units and assets to identify the InfoSec development needs and priorities. The assets should be identified and allocated to organizational structure, if needed, to gain more precise understanding of distribution of assets. Therefore, the structure of the organization should be described, in as detail as possible, to provide ability to drill-down to e.g. specific unit's assets, risks (see requirement 3), and InfoSec maturity level (see requirements 5-6). Thus, the following requirements (R):

R1: *the InfoSec self-assessment tool should have the ability to describe the organizational structure, as detailed as possible, to provide the ability to see organizational- and unit-level assets, risks, and maturity levels to help with InfoSec investment target identification.*

R2: *the InfoSec self-assessment tool should have the ability to allocate assets to the organizational structure for better analysis of their impact on overall InfoSec needs and better targeting of the InfoSec investments to critical area(s).*

The InfoSec self-assessment tools, international and national, commonly use some capability maturity model to evaluate the maturity level in InfoSec areas. In the evaluation of the maturity level, a risk-based approach is commonly used. Thus, the self-assessment tools should have ability to, for example, assign organization's risk appetite (Shao, 2015, 39) to indicate the minimum maturity level, ability to create response plans, and risk register, which has ability to prioritize the identified risks. In other words, the ability to provide a good overall understanding of InfoSec risk situation and to target the reduction to the perceived risks, as they are the biggest drivers in InfoSec investment (Moore et al. 2015, 1; 7-8). In the best case, tools are modifiable to some extent to allow the tool

to be aligned with the risk management policy and procedures of the organization. Therefore, the next requirement for the tool is:

R3: *the InfoSec self-assessment tool should be modifiable to some extent to align the tool with enterprise risk management, and to provide better understanding of the InfoSec risk landscape that affects the InfoSec investment decision making*.

As Moore et al. (2015) stated, organizations identify and prioritize the most important threats to their organization by using industry best practices and frameworks. Threats are incorporated in most of the economical investment models in varying role (e.g. Gordon & Loeb, 2002; Huang et al., 2008; Cavusoglu, 2008), but they use threats as a numerical value in calculations. The threat assessment is not only useful for the classical models, but it also shows what threats require focus as the priority of threats varies from organization to organization (Moore et al., 2015, 11). Thus, the following requirement:

R4: *the self-assessment tool should incorporate threat assessment to gain better overall view of InfoSec threats targeting the organization and its assets, to prioritize the threats, and to gain more complete information to support InfoSec investment decisions.*

One characteristic of InfoSec investment is the distribution of InfoSec investment areas (Shao, 2015, 37), and they are widely covered in the InfoSec frameworks. The InfoSec frameworks have become a common tool to manage InfoSec and as Moore et al. (2015) earlier stated, they are used in various situations, including InfoSec investment prioritization (Moore et al., 2015, 11-12). As the organizations develop their own, custom InfoSec frameworks for their specific environments (Moore et al. 2015, 13), the InfoSec self-assessment tools should have a selection of commonly used InfoSec frameworks to choose the most suitable framework(s) for the organization.

An advantage for a tool would be a functionality to integrate the chosen frameworks to have an InfoSec area/control mapping, without the need to check same areas/controls repeatedly covered in different frameworks. Also, the InfoSec maturity of the whole organization, as well as the units within, should be described to get better understanding of the varying levels of maturity throughout the organization (see requirement 1). Thus, the following requirements:

R5: *The InfoSec self-assessment tool should incorporate the commonly used* InfoSec *frameworks to choose from, and if possible, functionality to integrate the selected frameworks to gain an integrated map of InfoSec areas/controls to identify InfoSec investment areas, and to confirm compliance if needed.*

R6: *The InfoSec self-assessment tool should be aligned with the organization's used compliance maturity model to better manage the InfoSec maturity against the internal and external (frameworks') requirements.*

The first three steps of the design science process helped author to create the preliminary blueprint for the InfoSec tool and reach the first objective, which

was the theoretically based blueprint. In addition to theory-base, author's previous experience with the InfoSec tools helped in the creation of the preliminary blueprint.

The tool is intended to help the user to have a holistic view of their organization's InfoSec posture and environment to make justified and sound InfoSec investment decisions. The former requirements shed light on the functionalities required within the tool that help in the investment decision-making.

Firstly, organizations should know their organization (structure) and assets within that are essential for normal continuity of operation. In the InfoSec tool mode, the organizational structure functionality would describe the structure, to which organization can target assessments against InfoSec frameworks (see requirements 5-6), and allocate assets (requirement 2). These functionalities would help an organization to improve the InfoSec assessment considering the (business) operation. Thus, the requirements 1 and 2.

Organizations make the InfoSec assessments that usually have some maturity scale to assess InfoSec posture. In addition, a risk-based approach is commonly used. Perceived risk reduction is considered as one of the biggest drivers for InfoSec investments (Moore et al., 2015, 7-8), and thus, risk management functionality should have the ability to provide a good overall understanding of InfoSec risk situation, so that an organization can target the investments to the most needed InfoSec areas. Risk management functionality should have ability to target the identified risks to the organizational structure and assets to prioritize the criticality of InfoSec investments between the organization's units and assets (see requirements 1 and 2). Therefore, the third requirement.

Threat management functionality would provide a register of identified, organization-specific threats that target organization (structure) and assets (see requirements 1 and 2). Threats may stem from operational environment, risk and InfoSec maturity assessments (see requirements 1, 3, 5 and 6), as well as InfoSec frameworks (Moore et al., 2015, 8-9). Threats can be identified also from common vulnerability lists, such as OWASP (OWASP, 2017), and organization can better assess the threats targeting common vulnerabilities e.g. in their information systems, and thus better assess to what to invest. Therefore, the requirement 4.

Lastly, the InfoSec investment areas should be identified to allocate the resources effectively. There the InfoSec are the last, but probably the most critical area in the tool. Firstly, the frameworks are used in the InfoSec maturity assessments and these assessments are conducted in the organization and in specific units (see requirement 1), if needed. Risks arise from these assessments and should be managed accordingly (see requirement 3). As Moore et al. (2015, 8-9) identified, frameworks are used to identify the threats (see requirement 4), and can be seen also as "industry best practices", which is also another main source of threat identification.

The use of InfoSec frameworks varies between organizations, and thus the tool should have a selection of InfoSec frameworks, from which organization can select the most suitable one(s) (requirement 5). To be more useful, the framework

functionality should have an integrated InfoSec framework area/control mapping, so that an organization can cover multiple frameworks, if needed. As e.g. CISOs make their own, organization-specific InfoSec frameworks from the common frameworks, the integration is a needed feature (see requirement 5). Also, the tool's maturity model should be modifiable to some extent, so that an organization can align it with the used compliance maturity model (requirement 6).

Overall, the tool functionalities should serve the InfoSec investment process that author described in chapter 1.3.5. First, organizational elements should be identified to know the operational InfoSec environment, including risks and threats. Then the InfoSec maturity assessments are made against the used InfoSec framework(s), from which more risks and threats may be identified. After this, organization has a better overall understanding of their InfoSec situation, and thus they can make better InfoSec investment decision supported by the information gained from the tool. Lastly, organization can select the InfoSec investment projects, and start new cycle as needed.

Based on the requirements and description above, the preliminary tool blueprint (Figure 4) was designed to describe the required functionalities in an InfoSec self-assessment tool, so that it can help effectively in the InfoSec investment decision-making. The blueprint serves as the base for refinement that is described in the next chapters.

FIGURE 4. Preliminary blueprint of required functionalities in InfoSec self-assessment tool.

4.2 Case study

This and next chapters describe the empirical part of this research. Chapters are based on the organizational case studies and describes the results collected from

the interviews. All cases were analysed within each interview theme and the cross-case findings are described on general level (chapter 4.3), but the detailed within-case analyses can be found in attachment 2. Cross-case analysis is discussed to have a comprehensive lookout to the interview results, and more specifically go through the similar patterns and differences between the cases. The demonstration and evaluation of the preliminary InfoSec self-assessment tool blueprint is described in chapter 4.4, and it explains how the organizations evaluated the preliminary blueprint (artefact), as well as goes through the refinement needs that came up in the interviews.

Author recruited five persons responsible, or having responsibilities, regarding InfoSec from four organizations for this research, and the interviewee titles were various; vice president of risk management (hereafter VP), IT manager, InfoSec manager, CISO and Chief information officer (hereafter CIO). The interviewees were scoped and selected from manufacturing industry to get similar cases for comparison. The organizations were various on personnel size, but all have international operations, also out of manufacturing in one case. Thus, the results were somewhat generalizable and connected.

All the organizations had offices in Helsinki capital area, organization 3 being the biggest and organization 4 being the smallest. In organization 1 InfoSec was seen much like in any organization, the goal being to protect the critical information and other assets. Pressure to manage InfoSec came mainly from customers as they require secure products, which was seen especially important for organization 1, as digitalization is important part of strategy and products are more and more connected to the Internet. Overall, VP saw that, on general maturity scale 1-5, organization 1 was around 3 compared to the peers in industry.

Organization 2's IT manager did not see that InfoSec is a very critical component in the manufacturing industry and InfoSec manager saw that InfoSec is critical mostly regarding patents and other critical information, but also industrial control systems. In their case pressure to manage InfoSec came mainly from internal needs. Both saw that their organization's InfoSec maturity is currently around 3 on scale 1-5.

In organization 3, with digitalization, the importance of InfoSec has increased both in business and products. At the same time organization has identified that operational environment has changed, and I InfoSec risks have increased and their criticality alongside. On general level CISO saw that their organization is around 3 overall, and on some business areas objective is above 3.

Organization 4's CIO saw that the organization is not exceptional regarding InfoSec, but the organization must consider the general InfoSec responsibilities in everyday business. CIO saw that organization's IS maturity level is, with IT emphasis, around 3 on scale 1-5. Table 3 describes the general overview of the case organizations.

TABLE 3. Case study organizations.

Organization	Field of operation	Size: employees	Number of Interviewees	Interviewee's position	Interview date and duration
Org. 1	Manufacturing industry	Circa 11000	1	Vice president of risk management	18.8.2017 32 minutes
Org. 2	Manufacturing industry	Circa 5000	2	IT manager	25.8.2017 42 minutes
				InfoSec manager	6.9.2017 50 minutes
Org. 3	Manufacturing industry	Circa 52000	1	CISO	18.9.2017 43 minutes
Org. 4	Manufacturing industry	Circa 400	1	CIO	21.9.2017 51 minutes

4.2.1 Data collection

The main data collection method in this research is InfoSec subject matter expert (e.g. CISO) interviews. Interviews are suitable in this case, as the organizations in scope could tell themselves about the topic in hand and how it appeared in their organization. In an interview, the people involved are in direct linguistic contact with each other. Interview has its advantages and disadvantages, but it makes the data collection flexible (Hirsjärvi et al., 2009, 204), which was needed in this kind of research. Interviews were selected as the data collection method, because the covered topic is mapped out very lightly, and thus, author did not know the possible answers beforehand (Hirsjärvi et al., 2009, 205).

The interviews were semi-structured (Myers & Newman, 2007, 4) by type, as it was not reasonable to use neither fully structured forms nor fully open discussion on topic. The interviews were separated to four themes, which were suitable to cover the subject, but kept the questions and their order somewhat open (Hirsjärvi et al., 2009, 208). The themes were 1. contextualization 2. InfoSec investment decision making process 3. InfoSec (self-assessment) tools in InfoSec investment decision-making process, and 4. Evaluation of the preliminary InfoSec tool blueprint. The questions to each theme can be found in attachment 1 and were derived from the themes and previous literature (e.g. Dor & Elovici, 2016) described in chapter 2. The interviews were conducted as individual interviews, which was a better choice than pair interviews as the interviewees seemed to be more open to discuss alone.

4.2.2 Data analysis

The data was analysed with within-case analysis, which means becoming intimately familiar with each case (interviewed organization) as a stand-alone entity, to identify unique patterns in each case before generalizing patterns across all cases. After this, cross-case patterns were identified by looking the data in divergent ways (Eisenhardt, 1989, 540).

All interviews, except one, were recorded for better data analysis. Notes were taken in all interviews, but more extensively in the interview that was not recorded. The notes taken in interviews and from the records were in Finnish, so that author could send them to the interviewees for examination to confirm their validity. Full transcripts were not written as some of the discussions were not relevant to the topic, but only the relevant parts were transcribed and translated into English for research use.

The cross-case analysis was adjusted and sharpened during the data collection, as the data indicated the best way to compare the cases. This way capturing of novel findings from the data was possible (Eisenhardt, 1989, 541). The data was analysed during and after the data collection, because it allowed author to adjust research during the data collection process (Eisenhardt, 1989, 539; Hirsjärvi et al., 2009, 223). Author saw this as the best way to analyse the collected data to get answers to the research problem. The analysis was only qualitative by nature, as the study population was minimal to make any reliable quantitative analyses.

4.3 Findings

The following chapters look across the case studies to present what was learnt of both common patterns as well as the differences between the cases. The cross-case analysis permitted author to identify within covered themes, patterns and differences, which stemmed from the within-case analyses. One should bear in mind that the cross-case analysis does not consider organization 1 in following chapters as author did not get information from it regarding these.

As revealed in the within-case analyses (attachment 2), case organizations did not vary considerably regarding the topic in hand. All organizations were from manufacturing industry and represent international organizations, and despite being quite different on personnel size, the InfoSec (investment) management was somewhat the same. There were many commonalities between the organizations regarding their current InfoSec investment processes and InfoSec tools, and the used InfoSec investment tools were somewhat the same across all organizations. However, there were some differences between the organizations as well, and these are described in the following chapters.

4.3.1 No specific InfoSec investment process

None of the organizations in the sample had a specific InfoSec investment decision-making process, but followed either general or IT investment processes. Organizations 3 and 4 followed IT investment process, and organization 2's InfoSec investments followed general investment process, if needed. In organization 2, InfoSec "investment" is seen more as an allocation of money or budgeting, which does not always require formal investment process. Overall, there was a clear understanding in each organization how InfoSec investment process is conducted, which indicates that the processes do not require drastic development, if at all. However, the processes were not described in detail, and as organizations had not mapped possible InfoSec tools to use, InfoSec investment process descriptions might have been left in the dark as well.

4.3.2 Clear InfoSec investment governance

All organizations had clear chain of reporting or governance structure alongside InfoSec investment process. In organization 2 board was responsible of the InfoSec budget, but in organizations 3 and 4 IT could made decisions up to some financial threshold, after which executive committee made the investment decisions. All the interviewees saw that their InfoSec investment proposals had not been pushed back from upper management, or if had, the investment was not off the table but postponed. In all organizations IT or InfoSec team usually assesses the InfoSec investments before presenting them to upper management, if needed, which means that the investments are in majority of cases well justified, and thus are not usually pushed back.

4.3.3 Improved upper management InfoSec awareness

All interviewees stated that upper management's awareness of InfoSec has improved during the recent years and thus support has shifted to positive direction. This has positively impacted InfoSec funding as the upper management is more knowledgeable about InfoSec overall across the case organizations. Nevertheless, e.g. organization 3's CISO stated that there are challenges in the clear articulation of InfoSec investment target area(s) to upper management to justify the investment needs, which indicates that there is still room for improvement in upper management InfoSec awareness. However, CISO saw that the justification would be better with the use of common InfoSec framework(s) as reasoning.

4.3.4 Frameworks in InfoSec investment target identification

InfoSec investment targets were identified and assessed somewhat similarly in most but one organization. Organization 2 and 3 used common InfoSec frame-

work(s) to assess their InfoSec maturity to see to what area(s) to invest. Organization 2 also uses external consultants assess specific InfoSec domains to get better understanding of their InfoSec maturity. In addition to InfoSec maturity assessments, these organizations use risk information (organization 3) and IT/Infosec roadmap information (organization 2) to bolster the assessments, and to make sound InfoSec investment decisions.

Organization 4, on the other hand, identifies and assesses InfoSec investment needs typically through IT, but sometimes InfoSec investment targets rise from outside IT, e.g. from health, safety, environment, and quality (HSEQ) assessments. Thus, organization 4 is the only one not using common InfoSec frameworks in Infosec investment target identification, but CIO stated that they would need Infosec maturity simulation or tool to see where their maturity is compared to one or more common Infosec frameworks. Finding indicates that InfoSec frameworks are identified as a justifiable frame, against which an organization can assess their InfoSec maturity and identify InfoSec investment targets, even they are not currently used.

4.3.5 Risk-based drivers in InfoSec investment

The biggest InfoSec related investment driver in all organizations was internal and external compliance, externally especially GDPR, because of its relevance and urgency. In addition to compliance, risk assessments, InfoSec maturity assessments and threat landscape knowledge were the biggest drivers for InfoSec investments.

Organization 2's IT manager emphasized internal risk assessment and InfoSec manager general threat environment. Organisation 3's CISO emphasized the InfoSec maturity and risk assessments. And organization 4's CIO emphasized business continuity with internal compliance and risk assessments. This indicates that InfoSec investment decisions are usually supported with risk-based decision-making, which was also the main driver (perceived risk reduction) in Moore et al. (2016, 8) study.

4.3.6 Use of financial metrics

All interviewees concurred that financial metrics are not suitable, or are hard to use, for measuring security matters, including InfoSec investments. Organization 2 and 3 used fact-based metrics, i.e. risk and maturity assessment results, and threat information to measure InfoSec investments and their effectiveness.

However, organization 4's CIO saw that financial metrics, e.g. ROI, can be used, because they are strongly present in other business investments. Organization 4 justified the use of financial metrics to better articulate and justify the InfoSec investment needs to business, especially to upper management. However, organization 4's CIO saw that it is hard to calculate financial values, e.g. ROI, but when well justified, financial metrics can be used in InfoSec investments. Finding

appears to be in line with e.g. Moore et al. (2016,8) study, in which cost reduction was seen the last driver in InfoSec investments.

4.3.7 Need for information to InfoSec investment decisions

All interviewees stated that, in their organization's current state, they have enough and adequate information to make sound InfoSec investment decisions. However, all interviewees brought up that the organization could have more or better information, or manage better their InfoSec information or resources.

Organization 2's IT manager saw that the problem is the operational level InfoSec resourcing. Organization 2's InfoSec manager saw that they could collect and present the InfoSec information in clearer and better way, and have more visual ways to present and manage InfoSec (information). Organization 3's CISO saw that as organization's maturity increases, the amount of metrics and information increases as well, and thus can better assess their InfoSec maturity. Organization 4's CIO stated that the most technical InfoSec investment needs arise from the IT organization, and thus their resources and skills are the key for the adequate information, but it is not shared due to personal responsibilities. Therefore, having enough and adequate information is more resourcing and skill question.

4.3.8 Identification of new tools

All organization stated that their current tools are adequate for their purpose at the moment, but also stated that they could have better tools for InfoSec (investment) management. However, no organization had systematically mapped or tested potential tools to identify possible commercial tools for InfoSec investment management. For example, organization 2's interviewees stated that that it takes too much time to get acquainted with and test the new tools, and that tool content management takes too much resources compared to the possible benefits.

However, finding indicates that some existing InfoSec tool, e.g. InfoSec self-assessment tool, might be suitable for the organizations in this research, but they have not identified them or have missed them for various reasons.

4.3.9 Current tools in InfoSec investment

Across the cases, mainly excel and power point based tools were used in InfoSec investment management, and no commercial tools were used specifically for InfoSec investment management. Power point tools varied from IT/InfoSec roadmap to InfoSec maturity assessments to risk management. Excel tools were used for financial calculations, e.g. budgeting, and were mainly supporting the power point tools. Also, organizations transferred some of the data from excels to commercial systems, such as ERP (e.g. organization 2).

The currently used tools in organization 2 have been chosen by the organization and both interviewees stated that no new tools are needed at the moment as existing ones provide adequate information for now, however mostly within IT. Organization 3 might IT map and purchase expense management tools in the future.

The finding indicates the lack of specific tools for InfoSec investment decision-making support in the market, and/or the complexity of existing tool, e.g. GRC-tool, application in InfoSec (investment) management. However, as mentioned, neither of the organization had actively mapped potential tools that they could use in InfoSec (investment) management, because of resource-consuming effort.

4.3.10 Tool usage in practice

Organization 2 used the integrated InfoSec framework and IT/InfoSec roadmaps to manage the InfoSec investments. More specifically, the framework is used to assess the InfoSec maturity and based on the assessments the roadmaps are updated accordingly. Organization 2 also followed the IT/InfoSec portfolio to monitor the budgets after the investment decisions. Organization 2's InfoSec manager stated that in the future commercial InfoSec benchmarking tools might be tested.

Like organization 2, organization 3's CISO had made InfoSec maturity assessment based on a single framework, NIST CSF, on power point to manage InfoSec maturity. Organization 3's CISO stated that they use excel-based tools for InfoSec investment calculations that are used throughout the organization to follow the annual budgets. Organization 3 also transfers excel data to other systems for portfolio management.

Organization 4 uses excel for InfoSec investments' financial evaluation and budgeting to evaluate expenses and benefits. They, however, do no use InfoSec maturity assessment tool, but have identified a need for that kind of a tool or at least simulation. Organization 4 uses power point in general risk management and risk matrixes, but these are rarely used in InfoSec investment. In most cases, InfoSec investments are based on discussions on the identified development area(s).

The finding indicates that excel-based tools are adequate in practice for financial evaluation of InfoSec investments as the data is also transferred into other systems, such as ERP (organizations 2 and 3). On the other hand, regarding InfoSec (investment) management, all organizations stated that they could have better tools. Thus, better tools for InfoSec maturity assessment and roadmap/project management would be needed. Table 4 describes the support for each of the ten key findings.

TABLE 4. Support for the key findings from case study.

	Cases				
Finding	1	2	3	4	**Notes**
1	N/A	x	x	x	Organizations 3 and 4 followed IT investment process, and organization 2's InfoSec investments followed general investment process.
2	N/A	x	x	x	All organizations had clear chain of reporting.
3	N/A	x	x	x	All interviewees stated that upper management's awareness of InfoSec has improved.
4	N/A	x	x		Organization 2 and 3 used common InfoSec framework(s). Organization 4 typically through IT, but sometimes outside of IT.
5	N/A	x	x	x	InfoSec investment decisions are usually supported with risk-based decision-making.
6	N/A	x	x	x	All interviewees concurred that financial metrics are not suitable, or are hard to use.
7	N/A	x	x	x	All interviewees brought up that the organization could have more or better information.
8 & 10	N/A	x	x	x	All organization stated that their current tools are adequate for their purpose at the moment, but also stated that they could have better tools.
9	N/A	x	x	x	Across the cases, mainly excel and power point based tools were used in InfoSec investment.

4.4 Demonstration and evaluation

The demonstration and evaluation of the initial tool was conducted in the case interviews, and their results are described in this chapter. To all organizations the preliminary tool (blueprint) usage was demonstrated and explained the same way in high-level, and the objective was to see if the interviewees see that does the artefact solve one or more instances of the research problem, or not any at all.

Then each interviewee evaluated the blueprint on the described maturity scale between 1-5 (attachment 1). Evaluation criteria was derived from common maturity scales that use scale 1-5 levels being initial, basic, intermediate, advanced, and optimising, respectively (e.g. CMMI institute, 2017). The level descriptions were modified to refer more to the topic in hand, the InfoSec tools.

Organization 1's VP saw that overall the areas of the blueprint are logical, but need clarification, especially regarding risk and threat management, because these can be seen connected from different perspectives, and threats can be seen more within the risk management. Also, regarding the risk management area, there should be an action management functionality regarding the risks to follow up the identified risks. Governance model that includes e.g. distribution of responsibilities among and between IT and business, as well as owners of assets, should be included in the organizational structure area, because one must first know what assets organization has and how to manage them before it can evaluate e.g. threats targeting these assets. The interfaces between the tool areas should be well described, because this would make the usage of the tool more effective. Also, if there is changes in the organization, then the governance model should be updated accordingly. VP saw that perhaps the asset management area is not needed here. VP also saw that frameworks and compliance areas bring guidelines and boundary conditions to InfoSec management. Therefore, based on the organization 1 evaluation, the results mostly support the preliminary blueprint requirements (see chapter 4.1.3) R1 and R2, excluding the assets. R3-R4 are supported to some extent and somewhat disagrees with R5-R6.

Organization 2's IT manager saw that, firstly, the proposed InfoSec self-assessment tool should be possible to integrate to the existing tools organization uses to be useful. Explanation for this is that InfoSec related matters do not possibly rise to upper management, if InfoSec is managed in a different, "siloed" location. The areas proposed in the preliminary InfoSec tool blueprint were seen relevant, but in their organization, for example, organizational structure, asset, and risk management were managed in different solutions, and thus the integration requirement. Therefore, the tool should get input from other used solutions, but not contain fully the same data as in other solutions, because it is not desirable to store duplicate data.

Organization 2's InfoSec manager stated that to evaluate the blueprint, author should describe the presented areas even in more detail and how they work, and how the whole tool would work. As IT manager above stated that the tool should be integrated to the existing tools, InfoSec manager did not see that the integration is possible. InfoSec manager saw that InfoSec frameworks should be the "backbone" of the tool and other presented areas should be reflected on the used framework(s). Therefore, there should be a centre or middle area, through which other areas could be managed and to which other areas are connected. There should be also less main areas and more sub-areas within the main areas. Lastly, InfoSec manager stated that whatever the used frame(work) in the tool is, it should be modifiable. Therefore, based on the organization 2 evaluation, the results do not mostly support the presented requirements (see chapter 4.1.3) R1-

R4, but supports R5-R6 as the frameworks are considered the most essential part of the tool.

Organizations 3's CISO saw that the presented InfoSec tool blueprint logical and includes most areas of general GRC-tools, such as RSA Archer. CISO stated that the tool (blueprint) would be practical, if it can be modified according to organizations' needs. As above organization 2's InfoSec manager stated, CISO concurs that an organization should be able to compare different frameworks, even the organization uses only one. CISO stated that if customer or another interest group inquires how organization manages InfoSec against e.g. ISO27001, even e.g. NIST CSF is used. In other words, the tool should have mapping between InfoSec frameworks regarding similarities, and have capability to create an integrated framework based on organizational needs. CISO continued that perhaps presented compliance maturity model should be within framework section. Also, the maturity assessment should include a target state definition functionality in addition to the current state assessment, so that an organization could visualize and describe the maturity development over time. Therefore, based on the organization 3 evaluation, the results strongly support the presented requirements (see chapter 4.1.3) R5-R6 as the frameworks were identified as the most important part of the tool, and R3 as CISO saw the need for better risk management tool. However, as in organization 2, requirements R1 and R4 were only vaguely supported, if at all.

Organization 4's CIO saw that the presented blueprint was comprehensive regarding the presented areas and all the areas were seen relevant. CIO saw that the blueprint could be presented as a stack, where frameworks would be at the bottom as the base and other areas on top of them. The stack could follow the IT-stack and the InfoSec would go through all levels of the stack. The presented blueprint could also be more multidimensional, because InfoSec touches most of the business operations. CIO also saw that the risk and threat management areas should not be combined, at least not fully. Therefore, based on the organization 4 evaluation, of the presented requirements (see chapter 4.1.3) R2-R4 were vaguely supported and R1 even less. However, as CIO earlier stated that their organization would need InfoSec maturity assessment against common InfoSec frameworks, R5-R6 were somewhat supported.

Overall, the organizational evaluations support mainly the presented propositions 5 and 6, which indicates that the InfoSec frameworks should be the "backbone" of these self-assessment tools. In other areas various views were given, but mainly other areas were seen as a support to the InfoSec framework area, and assessments based on the frameworks. Many of the "supporting" areas were already managed in other tools, so they were not seen as necessary as the InfoSec frameworks.

4.5 Needs for a new tool

All organizations stated varying needs for new tools they would need. Organization 2's interviewees saw that they would need a tool, which contains holistic and visual examination and management of their IT and InfoSec roadmaps, and possibility to assess dependencies between the projects. InfoSec manager also saw that identified risks and their mitigation plans should be in the tool as well. This approach would bolster their current IT/InfoSec roadmap management, and is clearly different from other examined organizations.

Organization 3's CISO saw that they would need a better InfoSec risk management tools to better assess organization's risk landscape compared to e.g. threat reports. The tool should contain a risk library, from which organization could pick the most relevant risks to manage. This would lead to risk-based justification and allocation of resources in InfoSec investments. This has more risk-focused approach, but is like organization 2's threat landscape management and the need to manage risks in the IT/InfoSec portfolio.

On the other hand, organization 4's CIO saw that they would need an InfoSec maturity simulation or tool to see their InfoSec maturity against common InfoSec framework(s). This is clear difference from the other organizations' needs as they already have an InfoSec maturity assessment tools. However, this also confirms that the InfoSec frameworks have been identified as a key factor in InfoSec management, even they are not currently used. Also, this indicates that less mature organizations would need a better, yet affordable self-assessment tools containing InfoSec frameworks.

4.6 Empirically supported new artefact (v. 2.0)

This chapter discusses the refinement of the preliminary blueprint described in the previous chapters. In the chapter, the further refinement (DSR development step 3) of the preliminary InfoSec self-assessment tool blueprint is described, and the new blueprint (artefact) is explained. The discussion and results of this research are described in more detail in chapter 5.

The cross-case analysis permitted the author to identify several patterns and differences regarding InfoSec investment processes and InfoSec tools used in the case organizations. The patterns of commonalities as well as differences emerged during the case interviews and cross-case analyses. The results permitted author to refine the preliminary tool blueprint and in this chapter the refinement cycle (second DSR step 3) is described in detail.

Based on the cross-case analysis, the case organizations had not identified new tools, in addition to the existing ones, to support the InfoSec investment management and its process. However, based on the interviews it became clear that all organizations could use better tools, even none of the organizations had mapped existing commercial tools to purchase suitable ones. Discoveries from

the interviews (attachment 2), ad cross-case analysis (chapters 4.2-4.4), and needs for a new tool (chapter 4.5) shed light on the refinement needs regarding the preliminary InfoSec tool blueprint.

4.6.1 Empirical analysis

All organizations had identified the importance of the InfoSec frameworks in InfoSec (investment) management, and it indicated that they should be the central part of the new tool. Organization 1's VP saw that frameworks and compliance bring guidelines and boundary conditions to InfoSec management. Organization 2 and 3 assessed the InfoSec investment areas using the tools based on InfoSec frameworks, and organization 4 had identified a need to make InfoSec maturity assessment against common InfoSec framework(s) to get better understanding of their InfoSec posture. Also, main InfoSec investment driver in all organizations was internal and external compliance, which is often assessed against InfoSec framework(s). Thus, the InfoSec frameworks are placed as the "backbone" of the refined tool blueprint, to and through which other areas are connected to.

As the InfoSec frameworks are the "backbone" of the tool, there should be as many InfoSec frameworks as possible, so that organization can select the most suitable framework(s) for their organization to use. As some organization use only one InfoSec framework (e.g. organization 3) and some use multiple, integrated frameworks (e.g. organization 2), the tool should have a mapping of the framework areas/controls, so that an organization can create the needed framework, i.e. backbone, for their needs. Also, as some stakeholders might require proof of compliance against some InfoSec framework, an organization using another framework can see from the mapping their compliance status against the required framework. Thus, the integrated area/control framework/mapping or modifiable functionality is needed to answer the organizational needs.

The InfoSec maturity assessments are an essential part of the InfoSec self-assessment tool, because using InfoSec frameworks only to "get a check in the box" is not effective way to manage or improve InfoSec (investment decision-making). Therefore, as organization 3's CISO stated, the tool should incorporate a current InfoSec maturity assessment, as well as the target state definition, so that organization can track the progress towards the desired maturity level and development over time. Gap analysis between the current and target state bolsters the development need identification and risk assessment, which was emphasized the most in InfoSec investments in all organizations.

In all interviews it became clear that organizational elements are essential for InfoSec investment management and without knowing the elements, e.g. assets or governance model, organizations cannot effectively manage InfoSec investments. However, e.g. organization 2 managed organizational structure, assets and risks in separate tools, which indicated that these elements are not needed necessarily within the InfoSec self-assessment tools, but the tool should get the information as external input, if needed. Therefore, organizational elements must be identified (see chapter 1.3.5), but not all must be managed within

the InfoSec self-assessment tool, but got or taken into account as external information.

On the other hand, some organizational elements, e.g. governance (model), people, processes, and technology regarding assessment entities, should be incorporated on some level to manage the necessary elements in the InfoSec maturity assessments, for example distribution of responsibilities in assessment entities or development projects. Also, these organizational elements can be InfoSec assessment targets, i.e. the organizational entities to which InfoSec framework assessments are targeted, and thus needed in the InfoSec self-assessment tool to manage the InfoSec maturity assessments and their development roadmap in organizational context.

All organizations had various needs for a possible new tool as well, and these needs were considered in the new blueprint refinement. Organization 2's IT manager saw that they would need a tool that incorporates a holistic and visual examination and management of their IT/InfoSec roadmap, and possibility to assess dependencies across the projects. Therefore, the tools should have a development roadmap management functionality to manage the InfoSec investment roadmap and projects within, and to identify interdependences and -connections. With this functionality, organization can better manage the InfoSec maturity progress and follow the effectiveness of the InfoSec investments, and make corrective actions, if needed.

Organization 2's InfoSec manager and organization 1's VP saw that the identified InfoSec risks, organizational and from InfoSec maturity assessments, as well as their treatment/action plans should be incorporated in the self-assessment tool. Also, organization 3's CISO saw the need for a better InfoSec risk management tool, which should contain an InfoSec risk library, from which organization can select the most relevant risks that require attention. This functionality would help organizations in InfoSec risk-focused approach and reduce the perceived risks, which is also seen as the significant driver of InfoSec investments in both case organizations and literature (Moore et al., 2015, 7-8). Therefore, a risk management functionality should include, if not comprehensive InfoSec risk register, a functionality to create an organization-specific InfoSec risk register, in which the identified risks are stored. Also, risk treatment/action plans should be incorporated and possible to assign to the risks in the risk register. Risks in the register should be possible to be assigned to assessment entities, organizational elements, maturity assessments as well as investment projects.

Figure 5 below illustrates the refined InfoSec self-assessment tool blueprint, which was improved based on the gathered information. The main area, or "backbone", of the tool are the InfoSec frameworks, and other sub-areas within are connected to the frameworks as well as between. External input information indicates additional information that must be considered when using the tool. Below is further description of the tool usage.

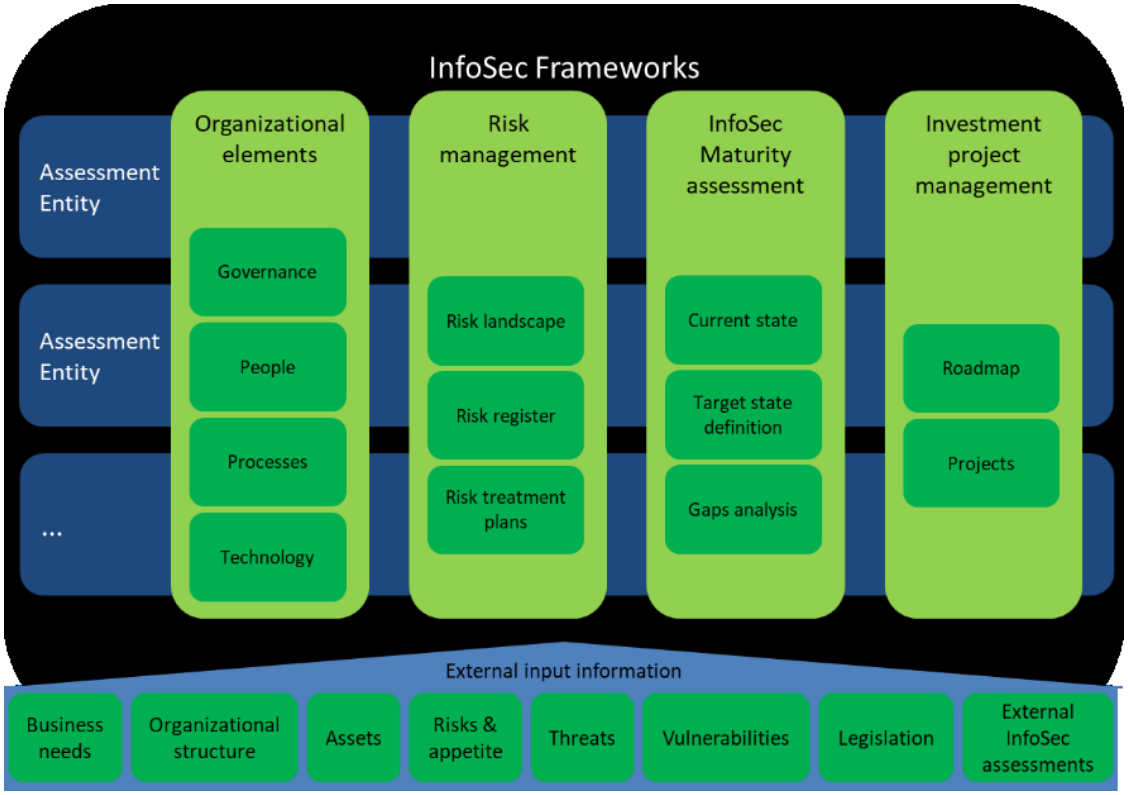

FIGURE 5. Refined InfoSec self-assessment tool blueprint.

As above can be seen, refinement of the artefact lead to several changes from the preliminary blueprint. Firstly, asset (allocation) was moved to external input information, because e.g. organization 1's VP stated that asset management is not necessarily needed as an independent area, but within the organizational elements, yet remarking that (governance) model should mention assets and their owners. Otherwise, it would be difficult to evaluate e.g. risks targeting the assets, if the assets are not identified. Also, organization 2 managed their assets in a different solution, which indicates that asset management is not needed within this kind of a tool, but possibly as external input. Even the assets are external input information, they can be included as assessment entities, such as organization's premises or personnel, to which organization can target InfoSec risk and maturity assessments, as well as development projects.

Secondly, threat management was moved to external input information as e.g. organization 1's VP stated that risks and threats are often connected, or threats can be seen more inside the risk management. However, even organization 4's CIO saw that risk and threat areas should not be combined, or at least no fully, bigger emphasis on the risk management in the InfoSec investment management was identified based on the overall organizational InfoSec investment drivers. Therefore, the risk management functionality should contain the identified risk landscape, earlier described risk register, and treatment plan functionality to manage the identified risks.

Thirdly, as e.g. organization 2's and 3's interviewees stated that for the tool to be practical, it should be modifiable to answer to the needs of an organization.

As above described, frameworks should include several common InfoSec frameworks from which an organization can select the most suitable.

Assessment entities can be organizational structure elements, such as business units, or member organizations, whatever structure is needed. Risk management functionality should get relevant, organization-specific information (internal and external), and organization should be able to bring risk information e.g. from risk libraries, from which an organization can select the most relevant ones.

Maturity assessments should follow possible organizational capability maturity model and support the current, target state, and gap analyses. Lastly, the investment project management functionality should incorporate essential roadmap and project management functionalities to effectively monitor and measure the progress. To summarize, all areas should be modifiable to some extent, so that an organization can manage each area as is defined within the organization.

4.6.2 Tool usage in investment decision making process

The blueprint structure was changed to illustrate better the interconnection and hierarchy of the tool, as well as to better connect it to the InfoSec investment decision making process (see chapter 1.3.5). The external input information brings needed information to InfoSec risk and maturity assessments, as well as investment decision-making, but are not necessarily needed to be managed within the self-assessment tool.

The InfoSec frameworks, as above described, are at the back as the "backbone", and other areas are connected to it. Assessment entities can be organizational structure, e.g. business units, to which other areas are connected throughout the tool usage. Organizational elements need to be identified in each assessment entity to effectively manage and target the InfoSec assessments, and later investments.

When external information and organizational elements, as well as assessment entities, are identified an organization can proceed to InfoSec risk management, which can often get plenty of information from general enterprise risk management, and thus might not take as much time as the maturity assessment(s). In risk management function organization can manage the identified risks from both the maturity assessment(s) and external information. Risks are stored in the register and can be assigned to assessment entities and organizational elements, as well as InfoSec maturity assessment findings, e.g. gaps.

The "workhorse" of the tool would be the InfoSec maturity assessment functionality as it is usually made against the selected frameworks, it targets the assessment entities, and is affected by risks and external information, as well as from which the investment projects stem. Current state assessments can be made internally, but also external assessments or assessors can be taken along. Target state definition usually indicates the objective level to which an organization aims, and based on the gap analysis organization can approximately see how

much work is needed to reach the desired maturity level. After the maturity assessment(s), organization can make sound, justified and risk-based investment target identification to what InfoSec area(s) to invest, and make the investment decisions.

Lastly, development roadmap should be managed to follow the progress from current maturity to target state in a controlled manner in each assessment entity and projects within. Different development projects, based on the InfoSec maturity assessments and external information, can be started to divide the development roadmap to more controllable parts. The project management functionality should have tracking functionalities to visually and logically provide the organization the information they need to manage the roadmap, its projects, as well as changes and other factors in project management.

Overall, figure 6 illustrates the InfoSec self-assessment tool usage through an InfoSec investment decision-making process. At the end of the above described general usage and process, during and after the roadmap and project management, organization should iterate back to steps 1, 2, or 3 as seen necessary to effectively manage the InfoSec investments in a continuous cycle.

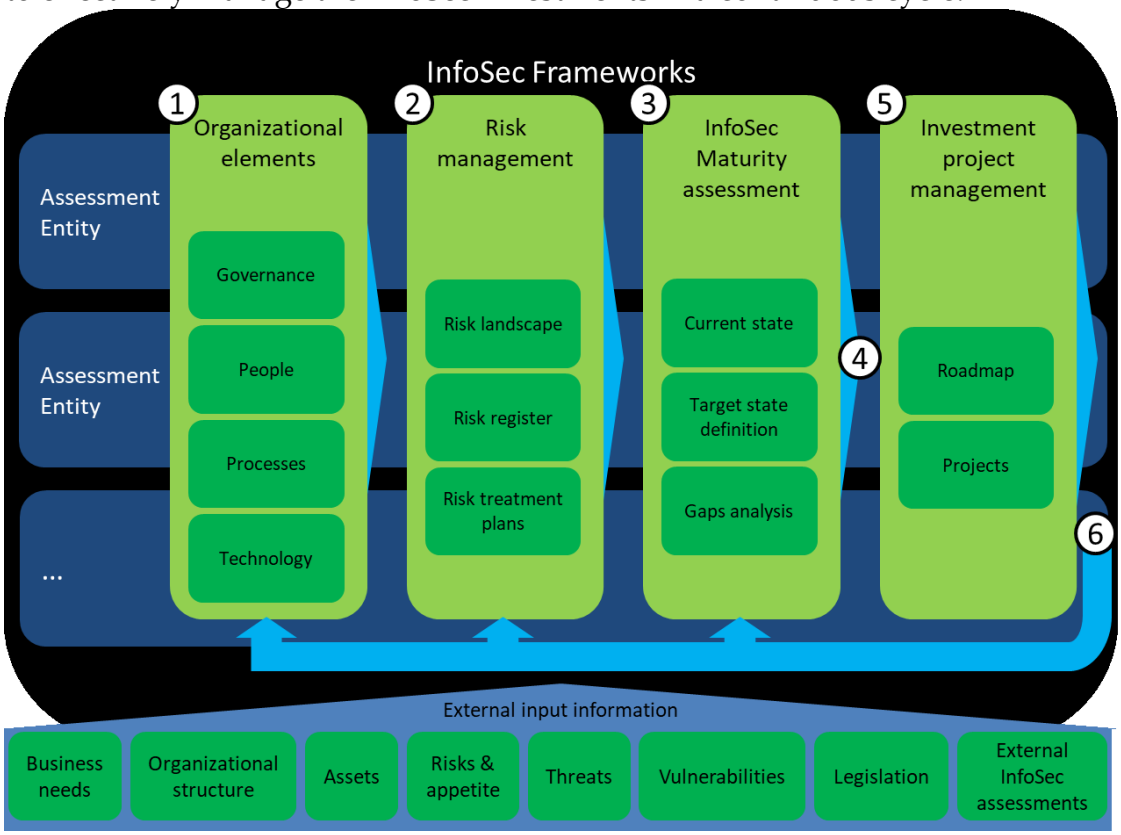

FIGURE 6. Refined InfoSec self-assessment tool blueprint with InfoSec investment decision-making process flow. (see chapter 1.3.5.)

Legend

1. Identify organizational elements and external factors (not exhaustive list)
2. Create organization-specific risk register and their treatment plans
3. Assess (entities') current maturity, set target state, and identify gaps/findings (e.g. risks to register with treatment plan)
4. Identify investment targets and make investment decisions (projects)
5. Create development roadmap, containing investment projects and their information (e.g. resources, schedule, scope)
6. Monitor and measure roadmap/project progress, and return to steps 1, 2 or 3 as necessary

5 DISCUSSION

The thesis was undertaken to better understand the InfoSec investment processes and especially the tools used in organizations during the process. The purpose of the research was to develop a blueprint for an InfoSec self-assessment tool, so that these tools could be effectively used as a support in InfoSec investment decision-making process. The objective was to create as exhaustive blueprint as possible to answer to the research question: What should an optimal InfoSec self-assessment tool include to assist InfoSec investment decision-making?

This chapter draws together the findings, overall contribution, proposed answers to the research problem and question, as well as implications for practice. Then the limitations of this research are discussed with the implications for future studies. Lastly, reliability and validity of this research is discussed.

5.1 Discussion of the main findings

The findings indicated that the recent research (e.g. Shao, 2015; Moore et al., 2015) on this topic (InfoSec investment) has been on right track. The main similarity of this research to the recent studies is that the focus has shifted from optimal investments and benefit maximization (e.g. Gordon & Loeb, 2002), i.e. outcome measures as Moore et al. (2015, 29) presented, to process measures, such as compliance maintenance and risk reduction (Shao, 2015; Moore et al., 2015). Even organization 4 stated that financial metrics can be used when well justified, consensus across the case study was that they are very hard to use in InfoSec (investment) management, which is in line with the recent research (e.g. Moore et al, 2015, 8). Moore et al. (2016) analyse that this may be the results of wide use of InfoSec frameworks, which promotes process measures. This leads to the next important finding.

Another important similarity between this research and recent research is the usage of InfoSec frameworks. Case study findings indicated that all organizations used or had identified the need to use InfoSec frameworks in their organizations' threat, risk, or investment target identification and assessments. CISOs in Moore et al. (2015, 9) study saw that frameworks are the second important approach to assess and prioritize threats, just after industry best practices that sometimes are the frameworks. As above mentioned, this is linked to the process measures, which may be worth for further study to confirm, as well as assess, if there is need for more qualitative outcome measures/metrics.

Other similarity to recent research is a good support and InfoSec awareness of upper management (e.g. Moore et al., 2015, 28), which has also increased in the case organizations. This indicates that upper management is more and more aware of InfoSec and requirements to manage it. Risk assessments, and management overall, were also seen in case organizations as one of the main driver in

InfoSec investment management, and perceived risk reduction was the main InfoSec investment driver in Moore et al. (2015) study as well.

The main difference between the findings in this research and recent literature was that the case study organizations did not have a specific InfoSec investment process, but used IT or general investment processes. This indicates that this might be the case in other organizations as well, and e.g. Dor & Elovici (2016) also identified the lack of up-to-date decision-making process research in InfoSec investments. However, as Dor & Elovici (2016) state themselves, further empirical work is needed.

Another difference between the findings and recent research was that there are no recent studies regarding InfoSec (self-assessment) tools in InfoSec investment (management). Dor & Elovici (2016) identified the need for InfoSec investment process research, but the tools have gotten less attention. Tool providers have developed various tools (e.g. GRC-tools) to manage InfoSec information, but there is no much, if any, recent scientific research to back their usage in InfoSec investment (process). Case study findings indicate that organizations do not have resources to get acquainted with the existing tools, so scientific community could learn from this and study the topic more to provide theoretically, and empirically, grounded guidelines for e.g. tool selection criteria and usage in InfoSec investments for working life.

Overall, the findings indicate that there is not much, if any, scientific research regarding the InfoSec (self-assessment) tools, let alone their usage in InfoSec investments. Also, the working life need for better tools for InfoSec (investment) management was identified. This, with the limitations of this study, makes the generalizability of the findings challenging, which indicates the need for further research. Both scientific community and tool developers can learn from this to provide more research on the phenomenon and make market research what organizations actually need, and provide studies/tools accordingly.

5.2 Contributions of the thesis

In this thesis, the contributions are two-fold, the development of InfoSec tool blueprint and findings from the case study. Firstly, author developed and introduced new blueprints for an InfoSec self-assessment tool that is a basis for a possible tool to be developed. The blueprints were made to fill the research gap in the topic in hand. Despite vast amount of research on InfoSec investments, there is not much, if any, modern studies regarding usage of InfoSec tools in InfoSec investment process. As Dor and Elovici (2016, 10) state, previous models, mainly economical, are relevant only in some phases of an InfoSec investment process as they address specific problems in the process.

The purpose of the preliminary InfoSec tool blueprint was to describe what was needed in an InfoSec self-assessment tool based on the examined literature and existing tools. Then the preliminary blueprint was refined based on the case studies to further understand the working life needs. The new blueprint is

aligned with the InfoSec investment decision-making process, and was derived from the existing theory as well as from the case studies. With the refined blueprint three contributions are clear regarding the InfoSec tools.

First, the refined blueprint describes the required, general functionalities for an InfoSec self-assessment tool, which clarifies what kind of areas it should contain to help organizations in InfoSec investment decision-making. The blueprint is an important qualitative contribution, because previously such tool models or frameworks have been mainly quantitative. Secondly, the tool blueprint is aligned with a general InfoSec investment decision-making process (chapter 1.3.5), which is derived from the recent literature, mainly Dor & Elovici (2016). This is an important contribution, because while previous, economical models addressed mainly some phases of an InfoSec investment process, the refined tool blueprint provides a tool that can be used throughout the InfoSec investment process, as well as InfoSec management overall. Thirdly, the developed blueprint offers a frame to which working life can compare their needs regarding InfoSec tools, and InfoSec tool developers can see what is needed from an InfoSec tool, reasoned with theoretical and empirical base. Therefore, overall theoretical and practical insight was given to InfoSec tool research in InfoSec investments.

Secondly, the case study findings were the other facet of contributions of this research. The similarities that were found are an important contribution as they confirm that the results of the recent studies, Finnish and international, are visible in the Finnish working life. The differences, on the other hand, are also an important contribution as they indicate the need for further studies, both theoretical and empirical. Overall, it was found that there is not much, if any, scientific research regarding the phenomenon from the point of view of InfoSec (self-assessment) tools, let alone their usage in InfoSec investments. The main findings are discussed in detail in the previous chapter (5.1).

5.3 Implications for practice

A couple practical implications need highlighting. Firstly, the new blueprint suggests that InfoSec investment decision-makers should use tools that help their organization identify *to what* InfoSec area(s) to invest, rather than *how much*. . Thus, organizations should identify their organizational elements and their risk/threat landscape, how InfoSec investments can reduce the perceived risks (e.g. Moore et al., 2015; Shao, 2015), assess their InfoSec maturity, and identify required capabilities, and prioritize accordingly. Based on the previous information, organization can assess how much is approximately needed to e.g. reduce the perceived risks. Therefore, organizations should adopt a holistic InfoSec investment process that includes main decision-making phases and involves relevant stakeholders (Dor & Elovici, 2016). One should bear in mind, that all the above is affected by cognitive biases and fallacies (e.g. Cavusoglu 2010), which were not examined thoroughly in this research.

As recent research and this research's empirical study confirms, aiming for optimal InfoSec investment amount is not desired, but where InfoSec professionals should allocate their sometimes-limited resources. Lack of information *to what* to invest may lead to wrong investments and cause losses itself, and therefore the focus should be on InfoSec investment target assessment and identification.

Secondly, the blueprint, along with the InfoSec investment process, provides a useful frame for InfoSec professionals to check what is needed in each phase of InfoSec investment process and how the phases can be managed in an InfoSec self-assessment tool. However, the tools alone are not an adequate support, but need a clear process that the tool can support.

Based on the empirical study, tools based on InfoSec frameworks are used in InfoSec investment decision. However, these tools are self-made (power point), and need for better tools had been identified. In practice, organizations should seek for better tools rather than settle for existing tools, if better ones can be attained. It may be resources-consuming, but along the way an organization may learn to do or improve the used tools independently.

5.4 Limitations and implications for future research

Several limitations to this research can be pointed out, but author attempted to cope with them and made changes to the study accordingly. This research did not consider the earlier monetary models of "*how much*" to invest in the InfoSec area(s), but attempted to identify the InfoSec tool features that give support to decision makers "*to what*" InfoSec area(s) organizations should invest. Also, this research did not cover the decision makers' psychological biases and fallacies affecting the InfoSec investment decision-making, even this factor has a strong influence on the decision-making, especially the decision-makers.

The new InfoSec tool blueprint is not empirically tested nor evaluated. While the basis for the refined blueprint is reasoned with theoretical and empirical data, the blueprint should be tested and evaluated as universal applicability of the tool was not confirmed. This can be done in future research.

Then there were several limitations in the data collection. First, the sample of the case studies was 50 % (4) of the intended sample (8). It is possible that resulting InfoSec tool blueprint might be too limited as generalization was minimal. Therefore, future research is needed with bigger sample as it would contribute to more diversity, detail, and accuracy in terms of InfoSec tools' functional needs. Second, one organization could only provide general information about their InfoSec management and preliminary tool evaluation, but lacked valuable information regarding the InfoSec investment process and, especially, the tools used in the process. Thus, in the case value to this research was limited, yet provided a different and good perspective in the preliminary tool evaluation.

The thesis attempted to open new paths of research regarding InfoSec self-assessment tools, as well as application and improvement of the tool blueprint. First, further investigation is needed on the needed areas in the InfoSec tool, as

the sample of this research was minimal. Second, testing applicability of the tool will be useful to validate the conceptual tool usage in practice. Thirdly, with larger sample and tool testing, further improvement of the tool blueprint, and perhaps testing of an actual tool can be conducted. Lastly, this research did not delve into the cognitive biases and fallacies deeper, but it might be an interesting research path to study how the tools help InfoSec investment decision-makers to avoid biases and fallacies.

5.5 Reliability and validity

As for reliability and validity, all research attempts to avoid mistakes. Even reliability and validity stem from quantitative research, qualitative research needs their assessment as well, even the terms have different interpretations, and possibly not even used in qualitative research. (Hirsjärvi et al., 2009, 231-232.)

The literature review gathered the most relevant research from as quality sources as possible, e.g. from respected journals. Overall, fifteen articles were selected for this research. The amount may be low, but as appeared during the review, the research, especially the recent, is scarce. Therefore, the literature base can be considered reliable, albeit narrow.

As for methodology, author attempted to describe in detail what was done and how the results were obtained. The case descriptions (attachment 2) and the explained results are matching, which indicates their validity. Earlier DSR justified the results with ad hoc justification, because of the lack of accepted DSR methodology. However, the DSRM, used in this research, is consistent with DSR processes in information systems discipline, and it is a common framework to validate DSR, without ad hoc arguments (Peffers et al., 2007, 73). Therefore, author followed the DSR process and attempted to explain the realization of the research ad precisely as possible, which improves the reliability of this research. Also, the data collection, through interviews and case studies, as well as data analysis were described in detail. However, author could have used methodological or methodical triangulation, or other triangulation, i.e. mixing of methods, to improve the validity. Also, more iterations regarding the InfoSec tool blueprint development and evaluation (DSRM steps 3-5) would have improved the reliability and validity of this research.

Regarding the case studies, the sample was minimal. 4 cases, or organizations, were involved in this research, but one of the cases did not provide any information regarding the most important aspects of this research, InfoSec investment process and InfoSec tools. Nevertheless, the sample can be considered sufficient, albeit being minimal, to make the study somewhat reliable and valid. The results the case study provided is in line with the recent studies, which increases the reliability of this research.

Lastly, any shortcomings of the author may have affected the reliability and validity of this research. Lack of experience in execution of DSRM and other

methods most likely affected the communication step of DSRM (step 6), which is this master thesis as a whole.

6 Conclusions

Previous research in InfoSec investment has focused on analysis tools for evaluating *how much* to invest in InfoSec area(s). As e.g. Shao (2015) states, previous studies failed to pay attention to characteristics of InfoSec investments, and assumed that decision makers are unbiased actors. Also, Shao (2015) argued that goal of InfoSec investment is not to obtain maximum benefit and Moore et al. (2016) confirmed this as cost reduction was seen the last important driver in InfoSec investment. Therefore, it was not reasonable to base this research on benefit maximization, i.e. *how much* to invest to InfoSec.

The research problem was the lack of effective usage of InfoSec self-assessment tools in InfoSec investment decision-making to identify "to what" to invest and the research question to be answered was "What should an optimal InfoSec self-assessment tool include to assist InfoSec investment decision-making?". To address this problem, as the main contribution a new conceptual InfoSec self-assessment tool model was developed in this thesis to be used in InfoSec investment process and as aid to InfoSec investment decision-makers *to what* InfoSec area(s) to invest.

The empirical parts of this thesis probed in to the working life to identify their current and desired InfoSec investment process and tool, as well as demonstrated and evaluated the preliminary tool model. Important for this research were that InfoSec frameworks were at the centre of defining risk perception and InfoSec investment, as well as focus on process rather than outcomes, i.e. financial measures.

The results of this research are somewhat aligned with recent studies, e.g. Moore et al. (2016), and the contributions were supported by theory and empiric information. This research contributed to InfoSec field by providing a blueprint for an InfoSec self-assessment tool model that would help organization to better identify *to what* information security area(s) to invest. The empirically-grounded model can help organizations and tool developers to understand what kind of tools are needed in information security investments.

Further study regarding InfoSec (self-assessment) tool usage became evident. Theoretical studies could examine the validity of the InfoSec tool blueprint by conducting more case studies, or using DSRM with design and development centred initiation. Empirical studies could test the tool blueprint in practice, and even develop the actual tool based on the blueprint and test it. Other study path could focus more on the decision-makers cognitive biases and fallacies, and how these are controlled in InfoSec investment process and tool usage, as the tools get the information from the decision-makers, i.e. affected by their decisions.

To the best of author's knowledge, this study may be first recent research that outlines this not yet much studied area, which would aid InfoSec investment decision-makers to better identify and assess their InfoSec investment needs and priorities. Developing the conceptual InfoSec self-assessment tool model author

attempted to pave the way for future research, thus offering new research directions for the InfoSec field.

REFERENCES

Beebe, N. L.; Young, D. K.; and Chang, F. R. (2014). Framing Information Security Budget Requests to Influence Investment Decisions. *Communications of the Association for Information Systems*, 35(7).

Bodin, L., Gordon, L.A. & Loeb, M.P. (2005). Evaluating information security investments using hierarchy. *Communications of ACM*, 48(2).

Cavusoglu, H., Raghunathan, S. & Yue, W. T. (2008). Decision- Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management. Information Systems*, 25:2, 281-304

Cavusoglu, H. (2010). Making sound security investment decisions. *Journal of information privacy and security*, 53-71.

Chai, S., Kim, M. & Rao, H.R. (2011). Firm´s information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Sys-tems*, 50, 651-661.

CMMI institute. (2017). What is capability maturity model integration (CMMI)?. Retrieved 10.10.2017 from http://cmmiinstitute.com/capability-maturity-model-integration

Dor, D. & Elovici, Y. (2016). A model for the information security investment decision-making process. *Computers & security*, 63, (2016), 1-13.

Eisenhardt, K. M. (1989). Building theories from case study research. *The academy of management review*, vol. 14, No.4 (Oct. 1989), 532-550.

Eurlex. (2016). General data protection regulation. Retrieved 03.05.2017 from http://eur-lex.europa.eu/eli/reg/2016/679/oj

Fenz, S., Ekelhart, A. & Neubauer, T. (2011). Information Security Risk Management: In Which Security Solutions Is It Worth Investing? *Communications of the Association for Information Systems*, 28(22).

FFIEC. (2016). Cyber assessment tool. Retrieved 14.02.2017 from https://www.ffiec.gov/cyberassessmenttool.htm

Finlex. (2010). *Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa*. Retrieved 14.05.2017 from http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Gal-Or, E. and A. Ghose. (2005). "The Economic Incentives for Sharing Security Information," Information Systems Research (16)2, pp. 186-208 Backhouse, J., Baptista, J. and Hsu, C. (2006). Rating Certificate Authorities: A Market Approach to the Lemons Problem. *Journal of Information System Security,* 2(2), 3-14.

Gordon, L .A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*. Vol. 5, No. 4, November 2002, 438–457.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, 30(3), 611–642.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, 8(5).

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75-105.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. uud. painos). Helsinki: Tammi.

Huang, C. D., Hu, Q. & Behara, R. S. (2006). Economics of information security investment in the case of simultaneous a tacks. *The Fifth Workshop on the Economics of Information Security*. Retrieved 02.01.2017 from http://weis2006.econinfosec.org/docs/15.pdf

Huang, C. D., Hu, Q. & Behara, R. S. (2008). *An economic analysis of the optimal information security investment in the case of a risk-averse firm*. Elsevier: Boca Raton.

ISF. (2016). The standard of good practice for information security. Retrieved 04.06.2017 from https://www.securityforum.org/tool/the-isf-standardrmation-security/

ISO. (2013). ISO/IEC 27000 family – Information security management systems. Retrieved 04.06.2017 from https://www.iso.org/isoiec-27001-information-security.html

Matsuura, K. (2003). Information Security and Economics in Computer Networks: An Interdisciplinary Survey and a Proposal of Integrated Optimization of Investment. *Computing in Economics and Finance*, 48, 1-13.

Moore, T., Dynes, S. & Chang, F. R. (2015*). Identifying how firms manage Cybersecurity investment.* Dallas: Southern methodist university.

Myers, M. D. & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organizations* 17(2007), 2-26.

NIST. (2016). Cybersecurity framework. Retrieved 04.02.2017 from https://www.nist.gov/programs-projects/cybersecurity-framework

NIST. (2000). Federal information technology security assessment framework. Retrieved 04.06.2017 from https://www.nist.gov/publications/federal-information-technology-security-assessment-framework

OWASP. (2017). OWASP top 10 – 2017 rc 1. The the most critical web application security risks.

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

RSA. (2016). Governance, risk & compliance. Retrieved 04.06.2017 from https://www.rsa.com/en-us/products/governance-risk-and-compliance

Salminen, A. (2011). *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasa: Vaasan yliopisto. Retrieved 04.02.2017 from www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Shao, X. (2015). *Understanding information systems (IS) security investment in organizations*. Tampere: Juvenes print.

Simon, H. (1969). *The Sciences of the Artificial*. Cambridge, MA: MIT Press, 1969.

Swanson, M. (2001). Security self-assessment guide for information technology systems. (No. NIST-SP-800-26). BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.

Tatsumi, K. and Goto, M. (2010). Optimal timing of Information Security Investment: A Real Options Approach, in Economics of Information Security and Privacy. In T. Moore, D. Pym & C. Ioannidis (Eds.), 211-228. New York NY: Springger US.

Wang, S.L., Chen, J.D., Stirpe, P.A., & Hong, T.P. (2009). Risk-Neutral Evaluation of Information Security Investment on Data Centers. *Journal of Intelligent Information Systems*, 36(3), 329-345.

Willemson, J. (2006). On the Gordon & Loeb model for information security investment. *The Fifth Workshop on the Economics of Information Security*. University of Cambridge: England.

Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. *In Proceedings of International Conference on Availability, Reliability, and Security*. 258–261.

ATTACHMENT 1 INTERVIEW QUESTIONS

Contextualization

- Please describe your background and position in the organization?
- Organization's industry and how critical information security is in the industry?
- Level/nature of external pressure to comply with information security compliance? E.g. regulation.
- Your evaluation of your organization's level of information security compared to other organizations in the industry? For example, using capability maturity levels 1-5.

Theme 1: Information security investment decision making process.

- Please describe your organization's IS investment decision making process? If not formal process, please describe usual process and steps.
- What is the reporting chain regarding IS investments?
- Does the upper management support IS investment needs? Has the support changed?

- How do you continue conversation, if support is pushed back?
- How the IS investment target areas are decided?
- What is the most important driver in IS investment? E.g. compliance. Please elaborate.
- When making IS investment decisions, are evidence and/or metrics used? E.g. ROI. If not, why?
- Do you feel you have enough/adequate information to manage and justify IS investments and their prioritization? Could this be improved somehow?

Theme 2: Information security (self-assessment) tools in IS investment decision-making process.

- Please describe the tools you use, if any, in IS investment decision making?

If you use tools:

- Why do you use the selected tools?
- Are the tools or their information used to justify the IS investment decisions?
- Are the tools used adequate for their purpose?

If you do not use (certain) tools:

- Why you do not use any tools?
- Are the tools in market not suitable, too expensive or something else to your needs?
- What kind of tool you would need for IS investments?

Theme 3: Evaluation of the information security tool model.

- Using the following scale (1-5), how would you assess the presented tool model to be used in IS investment decision making?

1. The tool model is illogical
2. The tool model is limited, and only some domains are relevant
3. The tool model has basic domains, but is not generalizable
4. The tool model has relevant domains, interconnections are mostly logical, and it is somewhat generalizable
5. The tool model has relevant domains, is logically interconnected and is generalizable to different kinds of organizations

- Is there something you disagree with?
- What would you add/change/take away etc.?

ATTACHMENT 2 WITH-IN CASE ANALYSES

Organization 1

In organization 1 the interview was carried out with the vice president of risk management (later VP), who is more responsible of the enterprise risk management overall, including InfoSec risks as well. VP stated that InfoSec is seen in the organization much like in any other organization, which means that the goal is to protect critical information and other assets. Especially, being in manufacturing industry, product InfoSec is very important, e.g. regarding automation. Digitalization is an important part of strategy and products are more and more connected to the Internet.

Pressure to manage InfoSec in satisfactory manner comes mainly from customer that require secure products and systems. There are also legal and contractual InfoSec compliance requirements, but e.g. data protection is the same as anywhere. Overall, VP sees that, on maturity scale 1-5, organization 1 is around 3 compared to the peers in industry. However, VP could not tell the exact InfoSec investment decision-making process or what tools are used within, and thus the interview was limited on those parts. Author approached the CISO and CIO of the organization to get more information, but could not get an interview with these persons.

Organization 2

In organization 2 two persons, IT-manager and senior manager, information security (later InfoSec manager), were interviewed. IT-manager had been four years responsible of IT management and InfoSec manager had been responsible of InfoSec since 2006. IT manager did not see that InfoSec is a very critical component in the manufacturing industry, or at least compared to financial sector. InfoSec manager sees that InfoSec is critical mostly regarding patents and other critical information, but also sees that industrial control systems (ICS) increase constantly the criticality of InfoSec, especially in factories. IT manager mentioned also the factories, but saw that biggest risks are more physical by nature.

Pressure to comply with InfoSec comes mainly from internal needs, but organization has identified GDPR and some national, e.g. China and Russia, cyber security legislation affecting their operation. However, both see a challenge in following and complying with global InfoSec and IT regulation. Both interviewees see that their organization's InfoSec maturity is currently around 3 on scale 1-5.

The initiation for InfoSec investments stems from organization 2's InfoSec development roadmap, and there is no specific InfoSec investment process, but InfoSec investments follow the general investment process, if needed. InfoSec "investment" is seen more as an allocation of money or budgeting, which does not require formal investment process. Based on both interviews, the reporting chain is clear regarding InfoSec investments and board is responsible for the whole budget, including InfoSec. Even InfoSec is quite small part of IT budgeting, the awareness of the board regarding InfoSec has shifted to positive direction, as

the board requires reporting on latest changes in InfoSec environment and status reports of organization's InfoSec posture.

IT manager stated that there is no clear prioritization on InfoSec investment targets. Partly the prioritization is done how the investment target fits to the surrounding architecture. A "critical path", i.e. the IT roadmap, for development projects has been identified, and it also indicates in which order the projects should be budgeted and conducted.

However, as above stated, the InfoSec investment targets also come from the InfoSec development roadmap, which is part of the overall IT roadmap. InfoSec manager has created an internal InfoSec framework, which consists of several controls from different frameworks, such as NIST CSF, SANS, and ISO 27001, and it is also a source of InfoSec investment targets. The developed framework is used in organization's InfoSec maturity assessment and the assessment results are discussed in framework domain-specific sessions to identify to what resources need to be allocated. The purpose of the framework approach is to set a "defence in depth" strategy to follow possible anomalies rather than preventing them. Also, external consultants assess specific InfoSec domains to get better understanding of the InfoSec maturity on those areas.

IT manager sees compliance as one of the biggest drivers for InfoSec investments, but also sees that internal risk analysis as important, if not more. It is identified what IT risks rise to corporate level risks, from which needed development actions can be originated. On the other hand, InfoSec manager sees that main driver for InfoSec investment is organization's threat environment, specifically during identification of an InfoSec need. Thus, organization follows threat trend reports and other sources of top level threats targeting them or the industry, as well as internal perception of current and future threats. Based on the previous information the IT and InfoSec roadmaps are updated and followed.

Both interviewees stated that the organization does not use financial metrics regarding InfoSec investment. IT manager stated that mainly risk based metrics are used and InfoSec investments are rarely handled via investment process, but is budgeted when needed. However, some suppliers require some financial information and it is provided accordingly. InfoSec manager stated that financial metrics are not used, because they are hard to use to e.g. assess relative efficiency, and concurs with IT manager that metrics come mainly from risks and threats. In other words, metrics are probabilities and impacts of risks and threats.

Both interviewees saw that the personnel responsible of InfoSec has, in current situation, enough and adequate information to manage and justify InfoSec investments, but both also see that one can always have more and better information. However, IT manager saw that this is not the biggest challenge, but the sufficiency of the operational level InfoSec resources, i.e. do they have enough e.g. time to do the required work. Also, the optimization information of the InfoSec resourcing might be limited. InfoSec manager stated that organization could collect and present the InfoSec information in easier, clearer and better manner, as well as have more visual way to present and manage InfoSec.

The only tools used to support InfoSec investment decision-making are the InfoSec framework developed by the InfoSec manager and the IT and InfoSec roadmaps. They are used to assess the InfoSec maturity in specified InfoSec domains and then the roadmaps are updated according the results. Both are power point and excel based, and no other commercial tools were used specifically in InfoSec (investment) management. InfoSec investments are budgeted in excel and are then put into an Enterprise Resource Planning (ERP) tool. Thinking portfolio is used to monitor the budget after the investment decisions are made. Also, asset and business structures are managed in separate tools. InfoSec manager stated that in the future commercial InfoSec benchmarking tools will possibly be tested.

The existing tools have been chosen by the organization and other commercial InfoSec related tools have not been identified in addition to the existing ones. InfoSec manager saw that it is easier to justify the use of general investments to tools, such as anti-virus, but regarding more expensive solutions, such as identity- and access management (IAM), it is harder to justify them e.g. in financial terms.

Both interviewees saw that the existing tools provide adequate information, but mostly within IT, and organization could have better tools for InfoSec (investment) management. However, organization has not systematically mapped and tested potential tools to use in InfoSec (investment) management. The reason is that it takes too much time to get acquainted with and test the new tools, and both interviewees concur that content management within the tool(s) take too much resources, especially time, compared to the assessed benefit of the usage.

The InfoSec investment tool the organization would need, according to bot interviewees, should contain better holistic, visual examination and management of IT and InfoSec project roadmaps, and possibility to assess dependencies between the projects within. InfoSec manager also added that identified risks and their mitigation should be considered here.

Organization 3

In organization 3, the Chief Information Security Officer (later CISO) was interviewed. The CISO role has been established only about a year ago, making the position relatively new. However, CISO has previous experience in InfoSec as both internal and external consultant. As the organization is in traditional manufacturing industry, InfoSec has not been in significant role previously, as quite recent CISO nomination indicates. However, with digitalization, the importance of InfoSec has increased both in business and products. At the same time organization has identified that operational environment has changed, and InfoSec risks have increased and their criticality along it.

Organization 3 has identified external pressure to comply with InfoSec related legislation as well, mainly GDPR, but also earlier mentioned nation-specific, Chinese and Russian, requirements. CISO mentioned that in this specific line of manufacturing industry there is internal motivation, even pressure in similar organizations to implement and follow certain InfoSec standards. Organization uses a maturity model in their own InfoSec posture assessment and on general

level CISO saw that their organization is around 3 overall, and on some business areas objective is above 3.

Organization 3's InfoSec investments are conducted through IT portfolio-process and IT budgeting, in which InfoSec is has a share. General InfoSec investments go through IT, but R&D has its own funding for IS. CISO is part of IT executive committee, in which InfoSec investment decision are made up to specified financial threshold, after which the decision-making is done on upper management level. CISO saw that management support has been good and discussion is done on upper management level as well. Some members of executive committee are part of general security committee, which conducts preparatory discussion about InfoSec investments. Thus, InfoSec investments that go to upper management approval are rarely pushed back, as they are well prepared and justified. Also, the organization has clear governance structure regarding InfoSec investment and discussion, which CISO saw as a positive support to get management support.

The target InfoSec investment areas are identified through NIST CSF maturity assessment, from which development needs arise. In practice, current state of InfoSec maturity is assessed on selected NIST CSF areas and then desired target state is set, followed by identification of gaps between the current and target state. The gaps give some indication to what area(s) to invest, but risk-based evaluation and prioritization are used to get more support for the investment decision, even the gap is small between current and target state. InfoSec risks are part of enterprise risk management and the whole risk map is used for the evaluation and to identify dependencies. Overall, maturity assessment and risk management help in critical InfoSec investment target identification.

GDPR has been identified as the main compliance driver for InfoSec investment in organization 3 as well, but data protection has its own funding. The biggest drivers for InfoSec investment are the maturity and risk assessments that are implemented in a development path over the next few years. CISO stated that they do not use any mathematical model or financial metrics, because they are not suitable for InfoSec or security investments in general. The used metrics also come from the maturity and risk assessment that provide fact based information. CISO saw that in the current maturity level organization has enough information to make sound InfoSec investment decisions. However, CISO saw that as the InfoSec maturity level increases, also the used metrics should and will increase, so that organizations can better assess how the investments affect the InfoSec maturity. In other words, how CISO can justify the investments before and measure afterwards the effects, if any.

In all investments, including InfoSec, mainly excel-based tools are used to make calculations. These excel-tool are coherent throughout the organization as the business can continuously follow the annual budget through the fiscal year. These calculations can be transferred to actual systems for portfolio management and used in power point-based tools as well. IT has also considered purchasing a commercial tool for IT expense management.

The existing excels are adequate for the financial side on investment management. However, CISO saw that the challenge lies in the clear articulation of InfoSec investment target area to justify the investment need. Thus, CISO saw that InfoSec investment process needs something to which to tie the needs, and thus has, like InfoSec manger in organization 2, made an InfoSec maturity model based on NIST CSF on power point, which is supported by excel-tools, e.g. for expense calculation. The InfoSec model, i.e. the NIST CSF within, sets the frame for InfoSec management and with the model CISO can follow the movement, or immobility, towards the target InfoSec maturity. Overall, CISO saw that all InfoSec professional should justify the InfoSec investments to decision-makers based on a commonly accepted InfoSec framework(s).

CISO saw that the above described tools are adequate for their purpose now. CISO has used for InfoSec information management RSA Archer, but stated that generally these kinds of tools are expensive for their purpose and require extensive customization and implementation, so that they fill the needs of an organization. Thus, the resources, mainly time and money, could be allocated to better targets, to keep the tool management to minimum.

CISO saw that their organization would need an InfoSec risk management tool in the future, so that the organization could better assess organization's InfoSec risk landscape compared to e.g. common threat reports and industry specific risk registers. The tool should contain risk libraries, from which an organization can pick the most relevant InfoSec risks for them. This way an organization could justify and direct InfoSec investment with a risk-based approach.

Organization 4

In the last organization, number four, the interview was carried out with the chief information officer (later CIO). CIO has been in the organization almost 10 years, and as the organization is slightly smaller than the previous organizations, CIO is also part of the organization's executive committee. CIO's responsibilities regarding InfoSec are tied to the overall IT management. CIO saw that the organization is not exceptional regarding InfoSec, but the organization must consider the general InfoSec responsibilities in everyday business.

CIO stated that there is no other compulsory InfoSec legislation targeting the organization than GDPR, but there are still some remains of process related requirements from a divested business unit operation. Otherwise, IT and InfoSec management are audited according to the used standards and internal requirements. CIO saw that organization's InfoSec maturity level is, with IT emphasis, around 3 on scale 1-5. In some areas the maturity is higher than 3 and in some lower.

As in previous organizations, in organization 4 there is no specific InfoSec investment process, but InfoSec investments are assessed and made as part of IT, and thus follows the same process as in IT investments. IT department is both presenter and decision-maker regarding InfoSec investments. IT investments, including InfoSec, rise from business needs and perceptions IT has made about organization's InfoSec posture, after which investment needs are brought up in relevant forum. Typically, the responsible persons of IT from each business unit are

involved in the identification and assessment of investment needs, especially regarding technical InfoSec investments. Also, the business unit representatives are involved to bring business point of view to the process. The IT/InfoSec investment needs are brought up, as needed, in monthly executive committee meetings, but the decisions regarding specific investment are usually pushed to the next meetings.

IT department can make investment decisions in some cases, but after specified monetary threshold IT notifies the executive committee, which makes the final decisions. Typically, if InfoSec investment is denied, it means that it is postponed rather than off the table from future investments. On the other hand, the IT/InfoSec investments that rise to the executive committee level are usually essential for business operations, and thus the justification for them is solid.

CIO saw that the upper management supports the InfoSec management and investments. The InfoSec awareness of the upper management has positively increased, as the persons within have become more interested about InfoSec threats targeting the organization, even about the most technical ones. General discussion about InfoSec has increased and regarding e.g. global malware has risen the question "how our organization is protected against these threats?". CIO saw that being part of the executive committee enables better and early understanding of business changes, which helps in making decisions regarding changes in IT/InfoSec. Also, unofficial discussion regarding InfoSec outside the executive committee meetings were seen productive.

Typically, IT identifies the needs for InfoSec development and through that the InfoSec investments are assessed. However, in some cases, e.g. from HSEQ-assessments, some requirements for IT may arise, and thus development needs might arise outside of the IT. Now the GDPR is the biggest single driver in InfoSec, but other essential drivers are internal compliance and risk assessments, with business continuity emphasis.

Unlike in the previous organizations, CIO saw that ROI-type metrics could be useful to use also in InfoSec, because they are strongly present in other business investments. Earlier investment decisions were assessed based on the requirements and capabilities of IT and business, and the assessments considered the operation time of the investment target for the next few years. However, along with this organization saw that more detailed metrics are needed, to better assess e.g. ROI and other possible financial metrics related to InfoSec. Basis for this is better articulation and justification of the InfoSec investment needs to business, especially to upper management. On one hand, business personnel are more and more knowledgeable about InfoSec, even about the more technical side. On the other hand, CIO saw that InfoSec is also abstract by nature and thus it is hard to calculate financial values, e.g. ROI. Regardless of this, CIO saw that, when well justified, financial metrics can be used in InfoSec investments.

CIO saw that the they could always have more information to justify and manage the InfoSec investments. Especially the distribution of information between business unit IT managers should be better and the IT-managers' InfoSec skills should be improved via self-study or with external help. The most technical

InfoSec investment needs arise from the IT organization, and thus their resources and skills are key for the adequate information. CIO saw that the broad IT committee possesses a lot of InfoSec information, but it is not shared due to personal responsibilities. In some cases, external partners are utilized to get more information regarding relevant topics. CIO stated that this is resourcing and skill question, whether information comes from internal or external sources.

Organization 4 does not use any commercial tools regarding InfoSec investment, but the needed information is collected from e.g. public sources and partners. Excels are used for investments' financial evaluation and budgeting, e.g. cash flows, and in evaluation of expenses and benefits. There are no InfoSec maturity assessment tools in InfoSec management, although the need for this kind of tool was identified. Mainly, organizational risk management uses excels and power point, to manage e.g. risk matrix, but these are utilized only in some InfoSec investment cases, depending on the size of the investment and to whom it must be presented. However, in most cases InfoSec investments are based only on discussions.

CIO stated that the organization has not assessed or mapped the possible InfoSec tools in the market to assess their need of feasibility in the organization, because the existing tools are adequate at the moment. Even the organization has not seen the need for additional or other tools for InfoSec investment, however, CIO saw that an InfoSec maturity simulation could be useful to conduct, so that organization sees on which InfoSec maturity level the organization is compared to common InfoSec framework(s). Thus, maturity model (tool) that would contain better InfoSec investment demonstration, better identification of development needs, and monitoring the previous was seen needed.