Towards Rule-based Information Security Maturity

The Next Level

MASTER THESIS

Student	Gabriël C.A. Slot, BSc
Student Number	4005627
Date	07-07-2015

Utrecht University
Master of Business Informatics
Princetonplein 5, De Uithof
3584 CC Utrecht, THE NETHERLANDS

Towards Rule-based Information Security Maturity

The Next Level

Student	Gabriël C.A. Slot, BSc
Student number	4005627
University	Utrecht University
Program	Master of Business Informatics
Project supervisor	dr. Marco R. Spruit
Daily supervisor	Tan Li
Second examiner	dr. Floris J. Bex

Preface

The roots of education are bitter, but the fruit is sweet.

Aristotle

This thesis is the fruit of my educational career at the university and the process towards the final thesis was indeed a bitter one. The research subject was challenging because of the limited available prior knowledge of information security and non-existing knowledge of rule-based technology. Special thanks need to be given to two colleague students and friends, Horia Constantin and Rick Hoving. With their help, I was able to develop the rule-based application prototype.

Abstract

There is a growing need for information security. Not complying with the demand of having high level information security will affect the market position of an organization. Using an information security maturity model can help organizations visualize and identify the steps that need to be taken in order to mature. Maturity in the field of security indicates the degree of development and the strength of the organization's security measures to mitigate risks that threatens its assets.

Unfortunately, one maturity model does not fit all organizations, because organizations have different organizational profiles. According to previous research, eleven organizational characteristics affect the information security, i.e. a financial institution requires different security measures than a bakery. It is necessary to have a well fitted information security maturity model for every organizational profile in order to support the organization.

According to research, the organizational characteristics affect a special kind of maturity model, the focus area maturity model. This type of model consists of focus areas or aspects in a certain domain and uses capabilities, improvement actions in order to reach a level of maturity, in order to assess whether a maturity level has been reached. Although it is clear that organizational characteristics affect the focus area level of the model, it is not clear what happens on the capability level. The research at hand has been set up to study the effects of a selection of the identified organizational characteristics on the capability level of the focus area maturity model in the information security domain. In order to do this, the existing Information Security Focus Area Maturity (ISFAM) model for SMEs is used and based on the experience of information security experts, the effects on the ISFAM model is researched. The experts were selected based on their knowledge and experience in the information security domain in different types of organizations.

Looking at previous research, it is expected that the organizational characteristics have an effect on the capability level of the ISFAM model. In order to handle these effects, the rule-based approach is used in the research. The rule-based approach is an approach that makes it possible to use rules, any bit of knowledge that can be expressed as: when 'something' is true, then do 'this', in a rule-based system, a system using rules, so that non-programmers can make adjustments to a maturity model based on the organizational profile, in order to create a more fitting model for the organization. Although the rule-based approach has been used in other information security maturity models, the combination of the rule-based approach and a focus area maturity model has not been done before.

During the research, however, the interviewed information security experts did not find effects on the lower levels of the ISFAM model. According to the experts, the improvement actions in the ISFAM model to reach a certain maturity level are too generically defined and therefore work for organizations with different organizational characteristics. This is backed-up by the fact that the model has been successfully assessed at multiple case organizations with different profiles.

Although no effects were found, the prototype of the rule-based information security focus area maturity model is still valuable in a way that it gives insight on the possibilities of the rule-based approach in combination with the ISFAM model. The research sets a base for future research where the rule-based approach can be used for other focus area maturity models.

Keywords: Organizational Characteristics, Number of Employees, Revenue, Sector, Information Security, Focus Area Maturity Model, ISFAM, Rule-based Approach.

Table of Contents

List of Figures

List of Tables

This page intentionally left blank

1 Introduction

> *"Through 2016, the financial impact of cybercrime will grow 10 percent per year due to the continuing discovery of new vulnerabilities."* - Gartner Top Predictions for 2012: Control Slips Away, Gartner, December 2011
>
> *"Incidents involving hacking and malware were both up considerably in 2011, with 81 percent utilized some form of hacking and malware incorporated in 69 percent of data breaches."* - 2012 Data Breach Investigations Report (DBIR), Verizon Business, April 2012
>
> *"Most data breach victims fell prey because they were found to possess an (often easily) exploitable weakness rather than because they were pre-identified for attack; 79 percent of victims were targets of opportunity, and 96 percent of attacks were not highly difficult."* - 2012 Data Breach Investigations Report (DBIR), Verizon Business, April 2012

Above statements (In Defense of Data, 2014) are just a small sample from a huge amount of security breach statistics and show the growing number of exploited threats and therefore the growing need for information security. Information security has been defined as the development and implementation of technical, organizational, human-oriented, and legal measures to safeguard the information inside and outside the organization's perimeter, as well as the information residing in information systems (Cherdantseva & Hilton, 2013). Another definition in the Glossary of Key Information Security Terms (Kissel, 2013), states that information security is used to protect information and the information systems to provide three concepts: (**1**) *confidentiality* (the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information), (**2**) *integrity* (guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity), and (**2**) *availability* (ensuring timely and reliable access to and use of information). Together, these three concepts are known as the CIA triad. The CIA triad is also covered in the definition of the most widely used information security standard (Susanto, Almunawar, & Tuan, 2011) of the International Standards Organization (ISO). In the 27K set focusing on information security, information security is the protection and preservation of confidentiality, integrity, and availability of information. However, in addition, the authenticity and reliability of information should be protected and entities can be held accountable.

It should be noted that there is a difference between information security and cyber security. However, the difference between them is often not clear and the terms are often used interchangeable. According to the International Standards Organization 27032 Cyber Security Guideline, cyber security is, like information security, the preservation of confidentiality, integrity, and availability of information but with the addition: "on the internet by means of technology devices and networks connected to it, which does not exist in any physical form". According to Kissel (2013), cyber security is the protection of information in cyberspace, the interdependent network of information systems infrastructures including the internet, telecommunication networks, computer systems, and embedded processors and controllers, from cyber-attacks, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Based on both explanations, cyber security is the security of information focusing on the IT aspect only, whereas information security includes for example the information that is shared between employees by means of speech or the physical security of the building as well. In this research the focus is set on information security as cyber security is just a small part of the information security domain. As can be seen in the paper of Susanto et al. (2011), ISO 27K is the most widely accepted information security standard next to standards as COBIT, BS 7799, PCIDSS, and ITIL. The information security definition as given in the ISO 27K standard is therefore used throughout this research.

1.1 Background

Information security is an important aspect of information technology in almost every domain that handles information. Information security can help not only in securing the assets of an organization and assisting in sharing information in a safe way through various security controls, but by building up a trustworthy relationship between the service providing organization and its stakeholders as well (Lessing, 2008). This bond of trust will eventually improve the cash flow and profitability of the organization due to the organization's reputation for safeguarding information (BS 7799, 1999). Next to the possibility that information security can help the organization to get a stronger market position by presenting itself as being a serious protector of the information of its clients, the organization will not have to spend resources on searching for security breaches (Vacca, 2009).

The growth or maturity towards the level of information security is tough, especially for a Small and Medium sized Enterprise (SME). Due to their small sizes, SMEs often lack the knowledge and resources to mature to the demanded level of information security (Mettler and Rohner, 2009). As stated, not complying with this demand will affect the market position of the organization as clients will switch to service providers that do have their information security at the demanded level.

Maturity models are tools that can help organizations in visualizing the maturity progress in adopting process and standards and to benchmark themselves in their industry (Becker, Knackstedt, & Pöppelbuβ, 2009). Maturity in the field of security indicates the degree of development and the strength of the organization's security measures (Lessing, 2008). Maturity models specifically for information security help organizations mature in the process of implementing the right measures in order to secure the assets of an organization.

A specific type of maturity model is the focus area maturity model. As opposed to the traditional maturity models that have a fixed number of generic maturity levels, the focus area maturity matrix defines maturity levels per aspect or focus area within a functional domain which allows a balanced and incremental development path (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010). A focus area maturity model in the information security domain, specially designed for SMEs, is the Information Security Focus Area Maturity (ISFAM) model (Spruit & Roeling, 2014). The ISFAM model is an in Excel developed focus area maturity model, which was created in 2013. It consists of four focus area categories (organizational, technical, organizational and technical, and support) which cluster 13 different focus areas, and distribute 51 capabilities (A-E) over 12 maturity levels. The maturity levels are grouped into four maturity stages: Design, Implementation, Operational Effectiveness, and Monitoring.

1.2 Problem Statement

An often heard criticism (Bollinger and McGowan, 1991) is that having a static maturity model that applies for every organization is oversimplifying reality and results in a poor model fit, because every organization has its own organizational characteristics that are different from other organizations. It is necessary to change an information security maturity model based on the organization's profile in order to support an organization in their maturity process.

According to the study by Mijnhardt, Baars, and Spruit (In Press), eleven organizational characteristics, such as Number of Employees and Number of Employees supporting IT Environment, affect the information security of an organization and therefore the information security maturity model. A statistical study done by Baars, Mijnhardt, Vlaanderen, and Spruit (2014) followed up on the research of Mijnhardt et al. (In Press), focusing on the effect of organizational characteristics on the ISFAM model. Baars et al. (2014) further evaluated the organizational characteristics and their measurement levels, and how the organizational characteristics pertain to the ISFAM model in order to understand the influence of the organizational characteristics on the focus areas within the ISFAM model. According to the research (Baars et al., 2014), organizational characteristics influence both the maturity framework and the focus areas that the model holds. However, focus area maturity matrices have a lower level object of measurement: the capabilities that reside in a focus area. This research follows up on the previous works of Mijnhardt et al. (In Press) and Baars et al. (2014) by researching the effects of organizational characteristics on the capability level of ISFAM. For example, according to Baars et al. (2014), the focus area Risk Management is subjected to the organizational characteristics. According to the capability level of the focus area, an organization should have implemented a risk management program. However, a risk management program of an organization with five employees will differ from an organization with 245 employees.

Next to the organizational characteristics that have an effect on the information security maturity model, the continuously evolving information security affects the maturity models as well. Organizational processes and technology keep on evolving and information security need to evolve with it. Whenever the core understandings and concepts of information security change, the information security maturity models need to change with it. The formal problem statement for this research is:

> *The organizational characteristics of SMEs have an effect on the focus area level of the focus area maturity model ISFAM; however, the effect on the capability level of the model has yet to be researched. Information security focus area maturity models need to be easily adjusted for SMEs considering their organizational characteristics and the evolving information security.*

1.3 Objective

Looking at the problem statement, there is a need for a flexible information security maturity model that can be changed based on the organizational characteristics of an organization and the ongoing changes of information security. The ISFAM model is used in this research as a base in order to continue the study of finding the effects of organizational characteristics on the ISFAM model done by Baars et al. (2014). As stated, the ISFAM model has been developed in 2013 by Spruit and Roeling and was published in 2014. Since then, the information security has evolved. Next to that, the ISFAM model was created based on five information security standards. However, more information security standards exist. It is therefore necessary to study and possibly update the ISFAM model. The first objective is therefore to:

- Research and possibly update the ISFAM model based on current information security standards;

This research follows up on the previous works of Mijnhardt et al. (In Press) and Baars et al. (2014) by researching the effects of organizational characteristics on the capability level of the ISFAM model. It is therefore necessary to:

- Research the effect of the organizational characteristics affecting the ISFAM model on the capability level;

The technological solution for the stated problem to modify the focus area maturity model for other organizational profiles is searched using the rule-based approach. According to Graham (2007), the advantages of using the rule-based approach is that it is easier to make changes as opposed to for example an Excel form (Spruit & Roeling, 2014), the maintenance and development time are low, and adjustments can be done not only by programmers, but by business people (consultants) as well. Abraham (2005) and Liao (2005) mentioned that the rule-based approach has been used in modern intelligent systems, as for example in strategic goal setting, planning, design, and scheduling. Using rules, if-then statements that that can be expressed in the following format: when 'something' is true, then do 'this'" (Browne, 2009), to change an information security maturity model for organizations with different organizational characteristics, fits the description of Abraham (2005) and Liao (2005) of the list of modern day usage of rule-based (expert) systems, systems that use rules in order to solve problems, due to its strategic planning nature. The rule-based approach in the information security domain has been done before (Walek, Bartos, & Zacek, 2013; Atymtayeva, Kozhakhmet, & Bortsova, 2014; Bartoš, Walek, Klimeš, & Farana, 2014; Tae-Nyeon & Hovav); however, it is uncertain how the rule-based approach can be used for a focus area maturity model within the information security domain. Therefore, the last objective of the research is to:

- Research whether and in what way the rule-based approach can be used for an information security focus area maturity model.

Based on the above stated objectives, the research at hand has been set up to help the SMEs in their maturity process towards the demanded information security level considering their organizational characteristics using rule-based technology. The formal objective is defined as:

> *Provide an up-to-date information security focus area maturity model using the rule-based approach in a way that it is usable for SMEs and can easily be changed for SMEs with different organizational characteristics.*

1.4 Research Questions

Based on the problem statement and objective, the following main research question has been formulated. The research is built upon four pillars: information security, the focus area maturity model, the organizational characteristics, and the rule-based approach. These pillars are the important keywords and are underlined in the research question. The main research question is defined as:

> *To what extent can organizational characteristics be incorporated into an information security focus area maturity model using a rule-based approach?*

In order to answer the main research question, sub research questions have been formulated which will be discussed next.

As explained, the ISFAM model has been developed in 2013 by Spruit and Roeling (2014) and will be used as a base maturity model for this research. Information security changes at a fast pace and the information security focus areas might have been changed after the development of the model. It is necessary to study the focus areas of the maturity model and possibly update the existing list of focus areas in the ISFAM model. The next sub research question is formulated in order to research whether focus areas are missing from the current ISFAM model created by Spruit and Roeling (2014).

a. *Which focus areas are missing in the ISFAM model?*

Organizational characteristics affect the information security and therefore the information security maturity model. Although the paper of Mijnhardt et al. (In Press) concluded that eleven organizational characteristics affect the information security maturity model and the research of Baars et al. (2014) concluded the effects of organizational characteristics on the focus area level, it is not clear in what way the organizational characteristics have an effect on the capability level of the model. Due to the time restriction of the research, only the first theme of organizational characteristics found by Mijnhardt et al. (In Press), comprising Number of Employees, Revenue, and Sector, has been studied in this research. The next question is formulated to study the effects of organizational characteristics on an information security maturity model.

b. How do the organizational characteristics Number of Employees, Revenue, and Sector affect the capability level of the ISFAM model?

As explained in the objective of the research, the rule-based approach is used to solve the research problem. Researching the possibilities of the rule-based approach in combination with information security maturity models is necessary in order to know how rule-base systems can be implemented. The research question focusing on the rule-based approach is formulated as follows.

c. *To what extent can a rule-based approach be used to create an information security focus area maturity model?*

1.5 Thesis Outline

The thesis is organized as follows. The next section entails the research approach. In this section the research design, the schedule, and the challenges of the research will be discussed. After the research approach section, the thesis will continue in section 3 with the approach and results of the literature study of the four pillars on which this research is built, covering the information security, the focus area maturity model, the organizational characteristics, and finally the rule-based approach. Based on the conducted literature study, the information security focus area maturity model, which was initially created by Spruit and Roeling (2014), is updated and evaluated, and presented in section 4. The effects of organizational characteristics are studied using the updated ISFAM model and the results effects based on the expert interviews are presented in section 5. The rule-based approach pillar is discussed in section 6, where a prototype of the ISFAM model is created using the rule-based approach in order to understand the use of the rule-based approach in combination with focus area maturity models. The last section is reserved for the discussion, conclusion, and possible future research.

This page intentionally left blank

2 Research Approach

This section focuses on the research questions, the research design, the schedule, and finally the research challenges.

2.1 Research Design

Hevner, March, Park, and Ram (2004) presented a framework for the realm of Information Systems research. The aim of design science is to develop an innovative problem-solving artifact that will contribute to current research. Hevner et al. (2004) explain seven guidelines: problem relevance, research rigor, design as a search process, design as an artifact, design evaluation, research contributions, and research communication. Their framework will be used in this research due to the design science nature of the research. Figure 1 depicts the framework focused for this particular research and will be discussed next. The guidelines have, where necessary, been specified towards maturity models as followed by Becker et al. (2009).

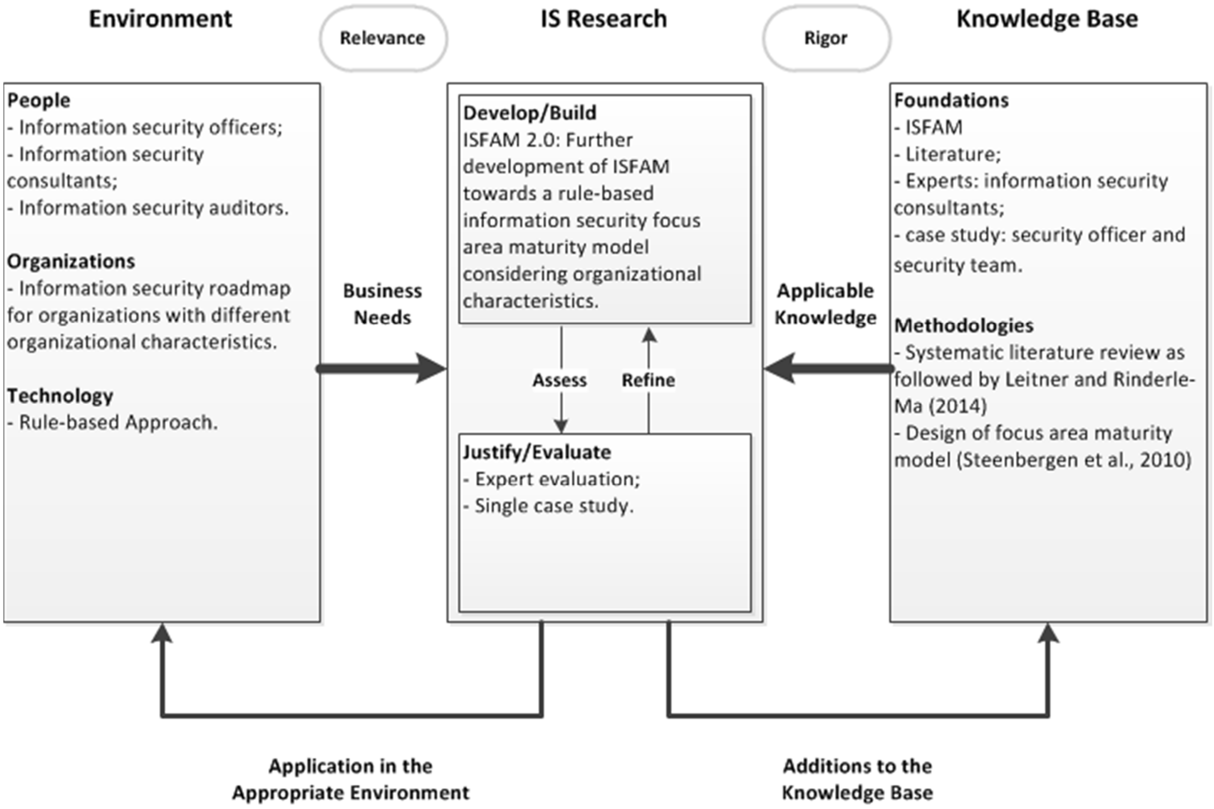

Environment
Relevance
IS Research
Rigor
Knowledge Base
People
- Information security officers;
- Information security consultants;
- Information security auditors.
Organizations
- Information security roadmap for organizations with different organizational characteristics.
Technology
- Rule-based Approach.
Business Needs
Develop/Build
ISFAM 2.0: Further development of ISFAM towards a rule-based information security focus area maturity model considering organizational characteristics.
Assess
Refine
Justify/Evaluate
- Expert evaluation;
- Single case study.
Applicable Knowledge
Foundations
- ISFAM
- Literature;
- Experts: information security consultants;
- case study: security officer and security team.
Methodologies
- Systematic literature review as followed by Leitner and Rinderle-Ma (2014)
- Design of focus area maturity model (Steenbergen et al., 2010)
Application in the Appropriate Environment
Additions to the Knowledge Base

Figure 1 - ***Information systems research framework (Hevner et al., 2004) filled in for this research***

2.1.1 Problem Relevance

Problem Relevance focuses on the development of technology-based solutions in order to solve important and relevant business problems.

The problem relevance of the research has been discussed in the introduction already. The maturity process of information security is tough, especially for SMEs. SMEs often lack the knowledge and resources to mature to the desired level of information security. Maturity models specifically for information security help organizations mature in the process of getting to a higher information security level. The information security focus area maturity (ISFAM) model (Spruit & Roeling, 2014) is an example of an information security maturity model for SMEs. However, having a static maturity model that applies for every organization is not realistic because every organization has its own organizational characteristics that are different from other organizations. Next to that, the information security itself evolves and therefore affects the information security maturity model as well. As stated in the problem statement, it is not clear how an information security maturity model can be easily adjusted for SMEs considering their organizational characteristics and the evolution of information security.

The technological solution for the stated problem to easily change the focus area maturity model for other organizational profiles is searched using the rule-based approach. The rule-based approach in the information security domain has been done before (Walek et al., 2013; Atymtayeva et al., 2014; Bartoš et al., 2014; Tae-Nyeon & Hovav); however, it is uncertain how the rule-based approach can be used for an information security focus area maturity model.

2.1.2 Research Rigor

Research Rigor is the use of rigorous methods in the development as well as in the evaluation of the research artifact.

According to Hevner et al. (2004), an information systems research needs to be conducted using rigorous methods during the development and the evaluation phase of the research artifact. For the development phase of the research artifact, the following methods have been used: systematic literature review, design of focus area maturity models, and explorative survey research using expert interviews. These methods will be further explained in the Design as a Search Process section. The methods that have been used in the evaluation phase of the research artifact are an evaluative survey research using expert interviews and a single case study. These methods will be further explained in the Design Evaluation section.

2.1.3 Design as a Search Process

Design as a Search Process is the process to find the most effective artifact to reach the desired result (Hevner et al., 2004). Maturity models are to be developed using an iteratively approach, i.e., step by step (Becker et al., 2009).

As described by Hevner et al. (2004), a research is a "search process to discover an effective solution to a problem." The artifact in this research will be developed using an iteratively approach following the design of focus area maturity models based on relevant scientific literature, and with the knowledge gained through explorative survey research using information security experts. These methods will be discussed next.

Systematic literature review - According to Levy and Ellis (2006), conducting an effective literature review helps the researcher understand the existing body of knowledge, provides a solid foundation for the proposed research, substantiate the presence of the research problem, justifying the proposed study as to one that contributes something new to the body of knowledge, and finally framing the valid research methodologies, approach, goals, and research questions for the proposed study.

The three stages of conducting an effective literature review are: input, processing, and output (Levy and Ellis, 2006). The input of the literature review consists of keywords. Keywords that are used in the search for relevant scientific literature focus on the four pillars of this research: information security, focus area maturity model, organizational characteristics, and the rule-based approach. Processing the systematic literature review, following the PRISMA process (Moher, Liberati, Tetzlaff, & Altman, 2009) based on the input, will lead to the relevant scientific literature. The process of conducting a systematic literature review according to PRISMA can be seen in Figure 2.

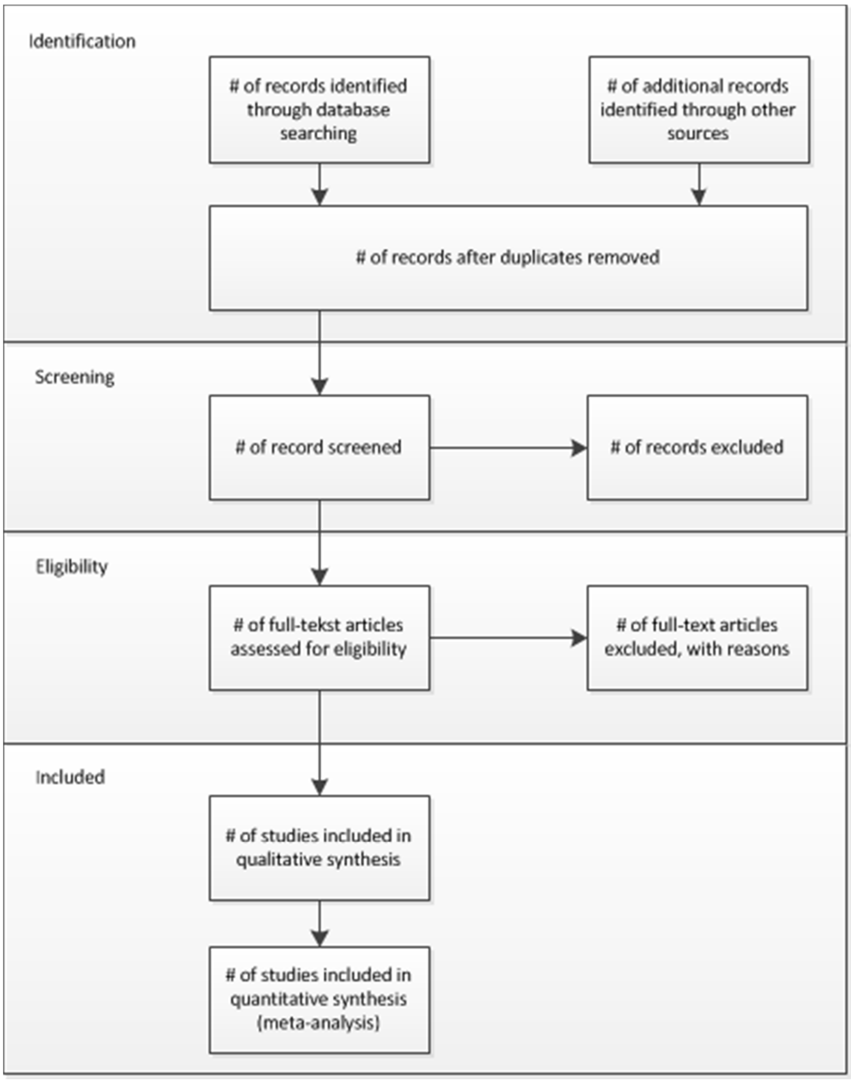

Identification
# of records identified through database searching
# of additional records identified through other sources
# of records after duplicates removed
Screening
# of record screened
# of records excluded
Eligibility
# of full-tekst articles assessed for eligibility
# of full-text articles excluded, with reasons
Included
# of studies included in qualitative synthesis
# of studies included in quantitative synthesis (meta-analysis)

Figure 2 - ***PRISMA process (Moher, Liberati, Tetzlaff, & Altman, 2009)***

Design of focus area maturity models - The artifact of the research, an updated focus area maturity model for information security, is developed following the design of focus area maturity models by Steenbergen et al. (2010). Figure 3 depicts the steps needed for the development of a focus area maturity model and will be followed throughout the research. At step five of the design of focus area maturity models, the rule-based approach is implemented in order to research whether the development of a focus area maturity model using rule-based technology is possible. Step eight to ten will be done using the evaluation process of the artifact as described in the section Design Evaluation.

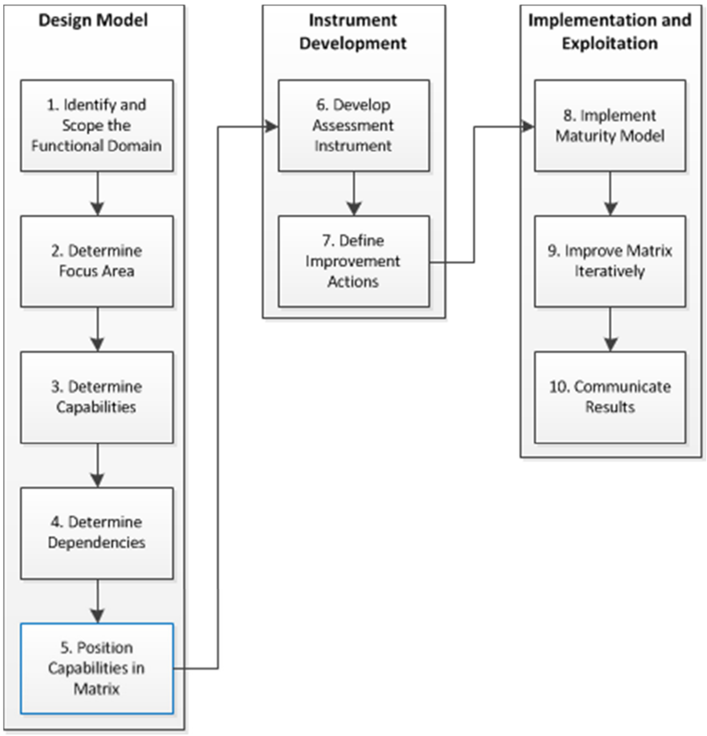

Design Model
1. Identify and Scope the Functional Domain
2. Determine Focus Area
3. Determine Capabilities
4. Determine Dependencies
5. Position Capabilities in Matrix
Instrument Development
6. Develop Assessment Instrument
7. Define Improvement Actions
Implementation and Exploitation
8. Implement Maturity Model
9. Improve Matrix Iteratively
10. Communicate Results

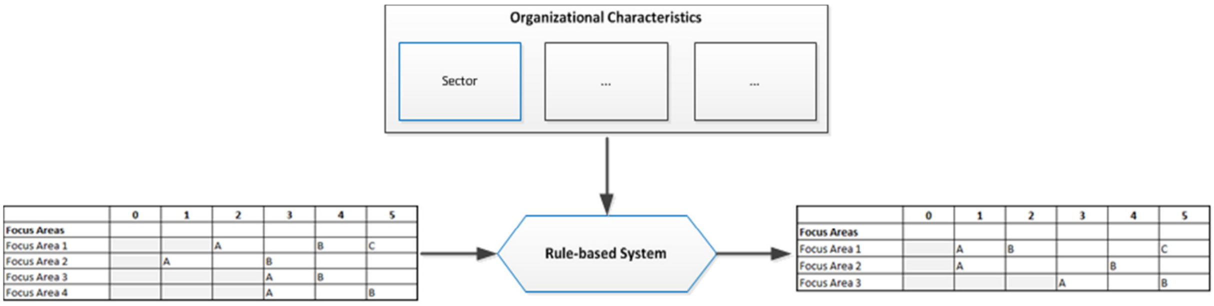
Figure 3 - ***The design of focus area maturity models (Steenbergen et al., 2010)***

Explorative survey research using expert interviews - expert interviews were held to find the effects of organizational characteristics on the capabilities of the ISFAM model. The experts were selected based on three criteria: (**1**) the experts needed to have knowledge of information security, but also of the information security in a wide range of organizations, i.e. organizations of different number of employees, revenues, and sectors. The experts were therefore selected from information security consultants due to their extensive knowledge of and experience with information security in different organizations. (**2**) The information security consults should not be working in the same organization. It might be possible that experts working in the same organization have the same type of ideas, or had the same type of education upon entering the organization. This would lead to experts having the same perspective on information security due to the fact that they have the same background. (**3**) The last criterion is years of experience. Experts with one year of consultancy experience will not have as much knowledge of information security as experts with five years of experience. Next to that, an information security consultant with more years of experience has more likely a wider range of cases in order to see patterns. The information security experts with around ten years of experience have been chosen for the research.

2.1.4 Design as an Artifact

Design as an Artifact is a guideline that describes that design research should produce an artifact in the form of a construct, a model, a method or an instantiation.

The artifact of this research is an information security maturity model with the possibility of adjusting it and therefore making it applicable for organizations with different organizational characteristics. Figure 4 shows an example of a solution towards a maturity model with the use a rule-based system, a system that uses the rules to solve problems. When organizations select the characteristics of their organization, such as sector, a rule-based system will be used to configure and generate the information security maturity model.



	0	1	2	3	4	5
Focus Areas						
Focus Area 1			A		B	C
Focus Area 2		A		B		
Focus Area 3				A	B	
Focus Area 4				A		B

	0	1	2	3	4	5
Focus Areas						
Focus Area 1		A	B			C
Focus Area 2		A			B	
Focus Area 3				A		B

Figure 4 - ***Artifact solution***

According to Becker et al. (2009), a research artifact may be an improvement of an already existing artifact. One of the information security maturity tools that exist to help SMEs mature their level of information security is ISFAM (Spruit & Roeling, 2014). ISFAM will serve as the base maturity model that will be improved.

2.1.5 Design Evaluation

Design Evaluation describes that the artifact should be evaluated based on rigorous evaluation methods (Hevner et al., 2004). The artifact must be evaluated iteratively (Becker et al., 2009).

As stated, finding an effective solution can be done by evaluating the artifact and adjusting it after each evaluation. The artifact is evaluated by means of an evaluative survey research using expert interviews and a single case study. Three different evaluation points will be covered. The first evaluation point is the evaluation of possible additional focus areas in the information security maturity model, which is evaluated by conducting a survey research using the same information security experts as stated in the Design as a Search Process section in order to validate the improvements made to the model.

The second point of evaluation is the evaluation of the updated ISFAM model with possible additional focus areas. The evaluation is done at a case organization in order to research whether the information security maturity model can be used in another sector than the telecom, media and technology organization as stated by Spruit and Roeling (2014).

Lastly, in order to study the rule-based approach in combination with a focus area maturity model, the updated ISFAM model will be developed as a prototype together with the rule-based approach. This evaluation is done in order to see whether the ISFAM model, and therefore any focus area maturity model, can be adjusted based on the organizational characteristics using the rule-based technology.

2.1.6 Research Contributions

Research Contributions specifies that design-science research must provide clear and verifiable contributions.

The research is relevant from a scientific point of view due to the further development and re-evaluation of the ISFAM model. A second scientific contribution is the research of the effects of organizational characteristics on an information security maturity model. Although previous research showed that the organizational characteristics have an effect on focus area level of the ISFAM model, it is not clear how the characteristics affect the capability level of the ISFAM model. Lastly, the use of rule-based technology in combination with the information security focus area maturity model will be valuable for future research. It is for example interesting if the rule-based approach can be used for other focus area maturity models.

The research is relevant from a social point of view due to the support that it gives to SMEs in having a better overview of handling information security by means of a maturity tool that is generated based on each organization's characteristics in order to create a more fitting model. Information security officers, consultants, and auditors will be able to give organizations a more customized advice when using the final artifact.

2.1.7 Research Communications

Research Communication outlines the way design-science research should be communicated.

According to Hevner et al. (2004), the research needs to be communicated not only for the technology-oriented audience, but to the management-oriented audience as well. The research is written keeping this guideline in mind. Next to that, the research is written in the form of a scientific paper, which can be found in the appendices. The paper is, however, focused on a specific subject of the thesis, focusing on the ISFAM model.

2.2 Research Schedule and Deliverables

Based on the method engineering of Weerd and Brinkkemper (2008), a Process-Deliverable-Diagram (PDD), as depicted in Figure 5(a, b, c), is created in order to get a structured overview of the processes and deliverables of the research. The processes are positioned on the left side, while the deliverables are positioned on the right side of the figure. The description of the activities and deliverables can be found in the appendices.

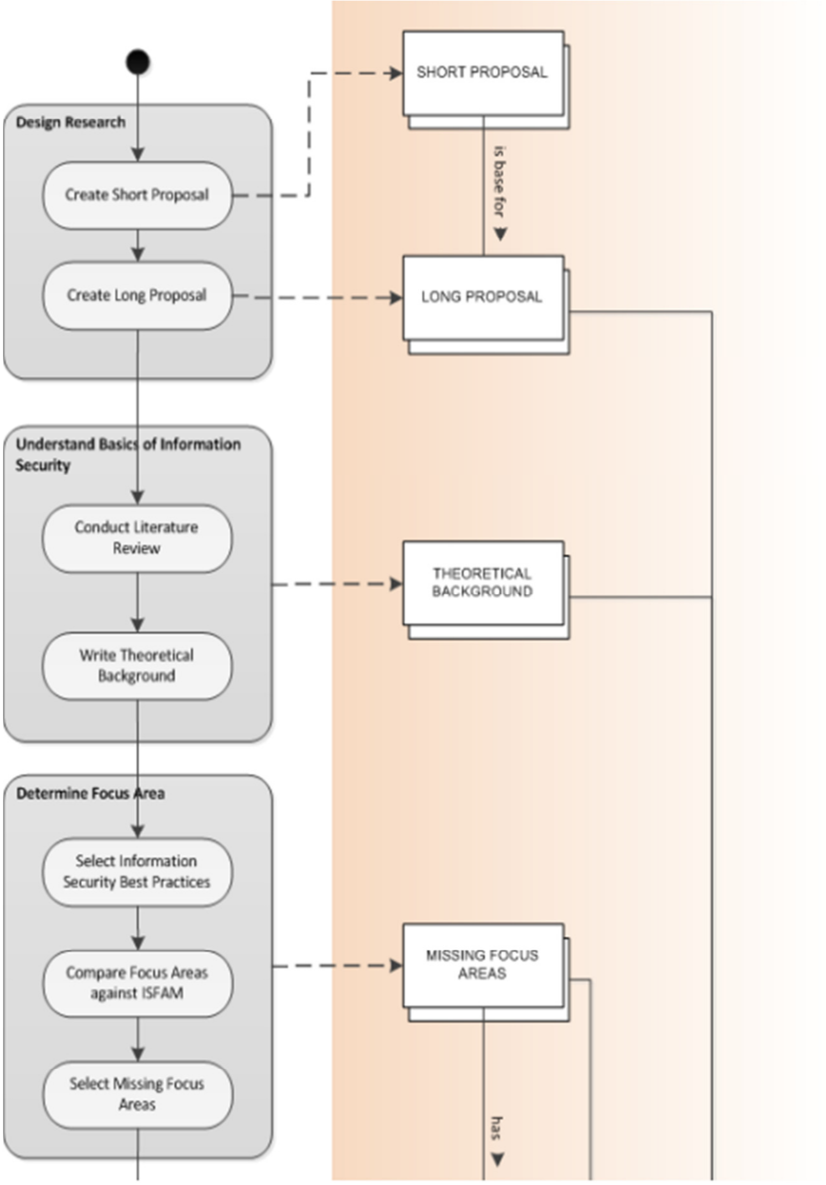

Design Research
Create Short Proposal
Create Long Proposal
SHORT PROPOSAL
is base for
LONG PROPOSAL
Understand Basics of Information Security
Conduct Literature Review
Write Theoretical Background
THEORETICAL BACKGROUND
Determine Focus Area
Select Information Security Best Practices
Compare Focus Areas against ISFAM
Select Missing Focus Areas
MISSING FOCUS AREAS
has

Figure 5a - ***PDD showing the research's activities and deliverables***

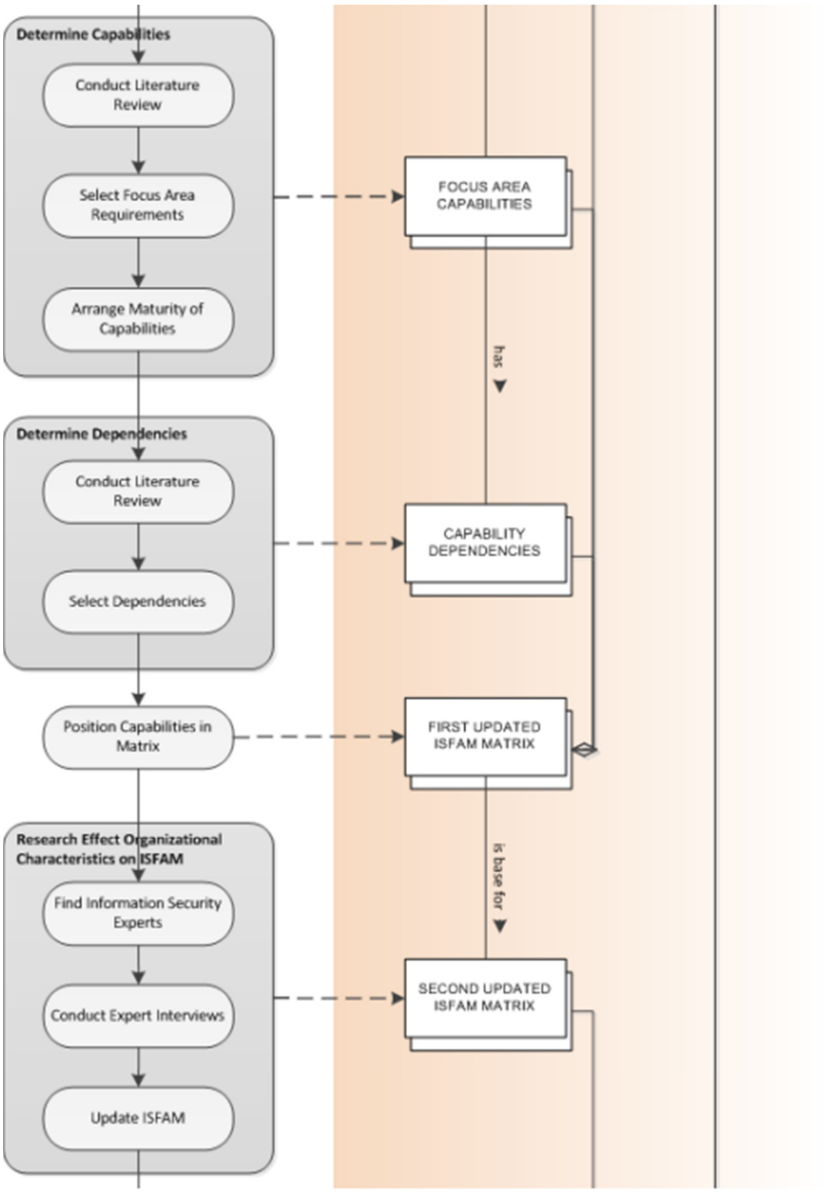

Determine Capabilities
Conduct Literature Review
Select Focus Area Requirements
Arrange Maturity of Capabilities
Determine Dependencies
Conduct Literature Review
Select Dependencies
Position Capabilities in Matrix
Research Effect Organizational Characteristics on ISFAM
Find Information Security Experts
Conduct Expert Interviews
Update ISFAM
FOCUS AREA CAPABILITIES
has
CAPABILITY DEPENDENCIES
FIRST UPDATED ISFAM MATRIX
is base for
SECOND UPDATED ISFAM MATRIX

Figure 5b - ***PDD showing the research's activities and deliverables***

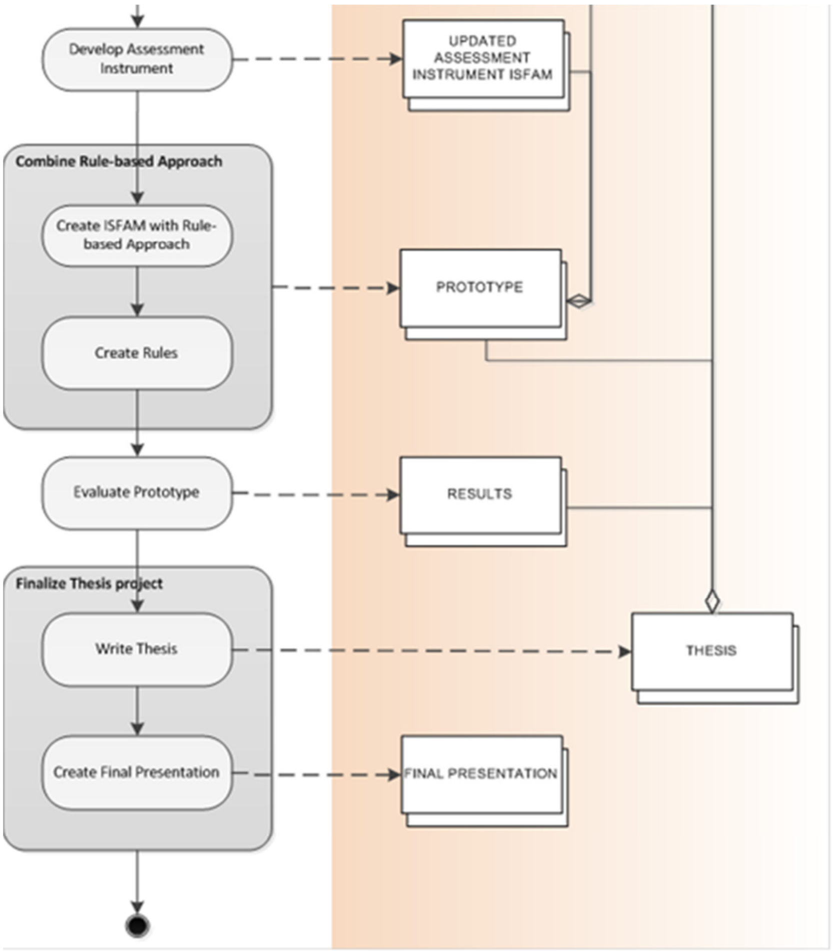

Develop Assessment Instrument
UPDATED ASSESSMENT INSTRUMENT ISFAM
Combine Rule-based Approach
Create ISFAM with Rule-based Approach
Create Rules
PROTOTYPE
Evaluate Prototype
RESULTS
Finalize Thesis project
Write Thesis
THESIS
Create Final Presentation
FINAL PRESENTATION

Figure 5c - ***PDD showing the research's activities and deliverables***

2.3 Research Challenges

The research will come across some challenges. The following challenges have been identified prior to the research.

Information security standards - It is challenging to consider which information security standards can be used to extend an information security maturity model, due to the high proliferation of existing and newly created information security standards.

Sector specific information security standards - Information security standards for general purposes and information security standards specifically designed for certain sectors have been found. However, it is not clear whether the differences between these two types of information security standards are significantly different from one another.

Existing model - Working with existing models can be challenging when not all rationale is documented. In order to use an existing model as a base, in this case the ISFAM model, it is necessary to know how parts of model were found and implemented. Next to that, it is important to understand what and why certain choices were made.

Simplicity - ISFAM was originally created as being a simple tool for SMEs. Keeping the information security maturity tool simple will be a challenge for this research. Adding additional focus areas, capabilities, or dependencies based on the organizational characteristics of an organization will lead to a bigger assessment and will therefore be less usable for these SMEs.

This page intentionally left blank

3 Literature Study

Based on literature study, following the PRISMA method, to identify the body of knowledge as mentioned in the research approach, the four pillars of this research, information security, focus area maturity model, organizational characteristics, and the rule-based approach, are discussed in this section.

3.1 Data Gathering

As explained in the research approach, the literature has been found following the PRISMA process. The literature study was conducted in the second half of 2014. Due to the very specific research area, information security focus area maturity in combination with the rule-based approach, the different research pillars have been split up in the literature study. Preselected terms, such as "“Ontology Information Security” OR “Information Security Taxonomy””, “Maturity Models”, or “Information Security Maturity”, were inserted in the Google scholar (http://scholar.google.com) search engine using the university’s UBULink. Google scholar was chosen because the given keywords are searched through numerous literature vendors such as Elsevier and IEEE. After selecting the appropriate filter, the accessible scientific literature found through this process will be used. The following table shows the total amount of literature using the PRISMA process. For readability reasons, the funnel towards the actual results of the literature study is placed in the appendices.

Key words	Information security: • Ontology Information Security; • Information Security Taxonomy; • Fundamental Information Security; • Comparison Information Security Standards ; • Comparative Study Information Security Standards. Maturity models: • Maturity Models; • Information Security Maturity. Rule-based approach with information security application: • Information Security Expert System. Additional focus area Supply Chain Management: • Supply Chain Management; • Supply Chain Risks Mitigation.
Search engine	Google Scholar
# of records before applied filter	348.210
# of records after filter (such as: excluding patents and citations, keywords only in title, or >1000 citations)	359
# of unique records used after screening	22

Table 1 - ***Overview of the total amount literature using the PRISMA process***

3.2 Information security

This section focuses on the first pillar on which the research is built, information security domain.

3.2.1 *Ontology of Information Security*

In order to share and reuse the body of knowledge, ontologies are often used to represent the concepts and relationships of a particular domain (Gruber, 1993). Fenz and Ekelhart (2009) studied the different concepts in the information security domain and the relationship between those concepts. Figure 6 depicts the concepts and relationships of information security as modeled by Fenz and Ekelhart (2009). The description of the concepts can be found in Table 2 following the information security model.

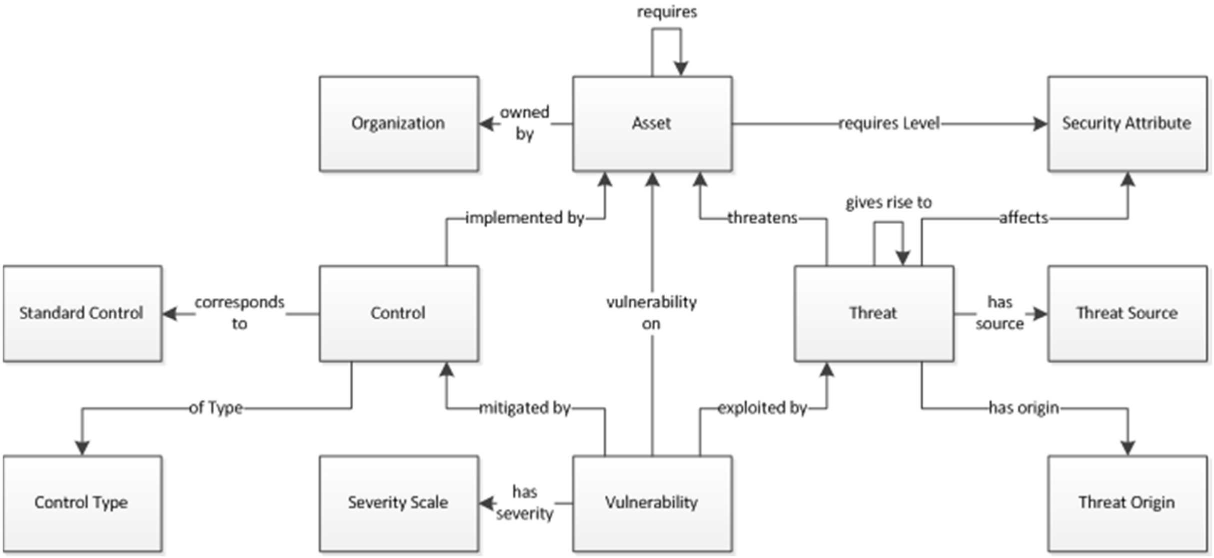


Figure 6 - ***The concepts and relationships of information security as studied by Fenz and Ekelhart (2009)***

Concept	**Description**
Organization	A single person or group that achieves its objectives by using its own functions, responsibilities, authorities, and relationships. It can be a company, corporation, enterprise, firm, partnership, charity, or institution and can be either incorporated or unincorporated and can be either privately or publicly owned. It can also be a single operating unit that is part of a larger entity. (ISO 27000, 2014)
Asset	Any tangible or intangible thing or characteristic that has value to an organization (ISO 27000, 2014).
Security Attribute	Confidentiality, integrity, and availability, also known as the CIA-triangle.
Vulnerability	A weakness of an asset or control that could potentially be exploited by one or more threats (ISO 27000, 2014).
Severity Scale	A scale in order to categorize the severity level of a vulnerability.
Threat	A potential danger to the organization's assets and affects specific security attributes as soon as it exploits a vulnerability in the form of a physical, technical, or administrative weakness, and it causes damage to certain assets. A threat can give rise to follow-up threats.
Threat Source	A threat is done either accidentally or deliberately.
Threat Origin	A threat can either come from a human or natural origin.
Control	A measure in order to mitigate an identified vulnerability and to protect the respective assets.

Standard Control	Controls are derived from and correspond to best-practice and information security standard controls.
Control Type	Preventive, corrective, deterrent, recovery, or detective measures.

Table 2 - ***Concepts of the information security model as studied by Fenz and Ekelhart (2009)***

The main goal of information security is to protect the assets of the organization against rising threats, i.e. theft of hardware or information, but natural threats such as flooding as well. The assets are in danger when vulnerabilities of the assets are exploited by the threats. In order to mitigate the threats from happening, controls or measures should be implemented. An information security control, a measure in order to mitigate an identified vulnerability and to protect the respective assets, is a critical element for successful information security (Menkus, 1991). These controls can vary from monitoring system logs to having full commitment of top management and are placed in information security best practices and information security standards focusing on supporting the organization and the employees.

3.2.2 Information Security Standards

Frangopoulos and Eloff (2004, June) did a comparative study on information security standards, which shows a comparison between the information security standards ISO 17799 (predecessor of ISO 27K which was changed in 2005), CERT Practices, and GASSP/GAISP. According to their study, many information security focus areas covered in the ISO 17799 standard do not exist in the other standards. A more recent comparative study done by Susanto, Almunawar, and Tuan (2011), benchmarking ISO 27K against other information security standards: BS7799, PCIDSS, ITIL, and COBIT. The subjects covered in the latter information security standards are checked against each section stated in the ISO 27K standard. The result of the study is shown in Table 3.

Focus areas	**ISO27K**	**BS7799**	**PCIDSS**	**ITIL**	**COBIT**
Information Security Policy	√	√	√	√	√
Communications and Operations Management	√	√	√	•	√
Access Control	√	√	√	√	√
Information Systems Acquisition, Development and Management	√	√	√	•	√
Organization of Information Security	√	√	√	√	√
Asset Management	√	√	√	√	√
Information Security Incident Management	√	•	√	√	√
Business Continuity Management	√	√	√	√	√
Human Resource Security	√	√	√	•	√
Physical and Environmental Security	√	√	√	•	√
Compliance	√	√	√	√	√

Table 3 - ***Comparative study of information security standards by Susanto et al. (2011)***

As can be seen in the paper of Susanto et al. (2011), ISO 27K is the most widely accepted information security standard next to standards as COBIT, BS 7799, PCIDSS, and ITIL. Therefore, this research looks at the focus areas of the ISO 27K standard.

3.2.3 Information Security Focus Areas

The comparison made in the paper of Susanto et al. focused on the ISO 27K:2005 version, while ISO 27K:2013 is the current version. In the latest ISO 27K version, some changes have been made as opposed to the ISO 27K:2005 version. The Communications and Operations Management section of the 2005 version have been separated in two different sections: Communication Security and Operations Security. The Cryptographic section is derived from the Information Systems Acquisition Development and Maintenance section and is a section of its own. Lastly, the Supplier Relationships section has been added as a new section (Praxiom Research Group Limited, 2014c). The following 14 sections are covered in the ISO 27K:2013 version (International Standards Organization 27002:2013):

1. **Information Security Policies** - According to the definition list of ISO 27000 (Praxiom Research Group Limited, 2014b), a policy defines “a general commitment, direction, or intention.” An information security policy should “express management’s formal commitment to the implementation and improvement of its information security management system and should include information security objectives or facilitate their development.”;
2. **Organization of Information Security** - The organization of information security entails measurements for the internal organization, i.e. the roles and responsibilities of information security, and the mobile devices and teleworking, i.e. policies for ICT devices, smartphones, USB gadgets, and working-from home.;
3. **Human Resources Security** - Human resource security is the security focused on the employees, from recruiting, to during the employment, and even after employment. Before employment a screening needs to be done. Employees during employment need to be aware of the information security policies that are defined within the organizations. After employment, the employees need to be reminded of ongoing obligations under privacy laws.;
4. **Asset Management** - Managing the assets of an organization, such as hardware, software, but also information, is important in order to keep track of critical assets. Without it, critical assets can become missing more easily. It is the responsibility of the assigned owner of the asset to keep the asset safe.;
5. **Access Control** - Access control focuses on the identification of users and defining their access to information in order to keep track of the users that have access to sensitive information. According to ISO, “the allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights”.;
6. **Cryptography -** This section that focuses on the security controls that involve the use of cryptographic controls and keys.;
7. **Physical and Environmental Security** - Physical and environmental security is a perfect example of information security no longer focusing on technical aspect alone. This section focuses on the building and perimeter of organizations and considers risks such as fires, floods, earthquakes, bombs, etc. Defining which rooms do not allow unauthorized access should be included in the policy as well.;
8. **Operations Security -** Operations security dictates that the operational procedures should be documented. Next to that, the operational systems should be backed up, logged and monitored, and audited in order to prevent incidents from happening.;
9. **Communications Security -** In communication security, controls for the security of network security and transfer for information are defined.;
10. **Systems Acquisition, Development and Maintenance** - This section comprises controls to ensure the security of the development life-cycle products.;

11. **Supplier Relationships -** According to the ISO (Praxiom Research Group Limited, 2014c), supplier relationships focuses on the policies, procedures, awareness, etc. to protect the organization's information that is accessible to IT outsources and other external suppliers. The service delivery by external suppliers should be monitored and reviewed. Next to that, changes in the service should be controlled.;
12. **Information Security Incident Management** - According to the definition list of ISO 27000 (Praxiom Research Group Limited, 2014b), information security incidents can occur during an information security event. An information security event is "a system, service, or network state, condition, or occurrence that indicates that information security may have been breached or compromised or that a security policy may have been violated or a control may have failed." In the list of definitions, an information security incident is "made up of one or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair business operations." The information security incidents should be management in order to prevent the incidents from happening again. This can be done by means of a set of processes, which include "a detection process, a reporting process, an assessment process, a response process, and a learning process.";
13. **Information Security Aspects of Business Continuity Management** - According to the ISO22301 – Business Continuity Management Systems (Praxiom Research Group Limited, 2014a), business continuity management is used in order to "ensure that operations continue and that products and services are delivered at predefined levels, that brands and value-creating activities are protected, and that the reputations and interests of key stakeholders are safeguarded whenever disruptive incidents occur. This is achieved by identifying potential threats, by analyzing possible impacts, and by taking steps to build organizational resilience.";
14. **Compliance** - Compliance focuses on the identification of the obligations towards external authorities. It includes intellectual property, business records, and cryptography.

Looking closely at the information security ontology by Fenz and Ekelhart (2009), the supply chain is not being discussed as being part of the information security domain. As an extra argument for the additional Supplier Relationships section, according to the papers of Li and Chandra (2008) and Li, Chandra, and Shiau (2009), supply chain security is an important concept of information security. To understand the basics of supply chain management and the importance of supply chain security in information security, the literature study focuses on supply chain management as well.

According to Mentzer, DeWitt, Keebler, Min, Nix, Smith, and Zacharia (2001), a supply chain is defined as "a set of three or more entities (organizations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer." Mentzer et al. (2001) present three types of supply chains as shown in Figure 7.

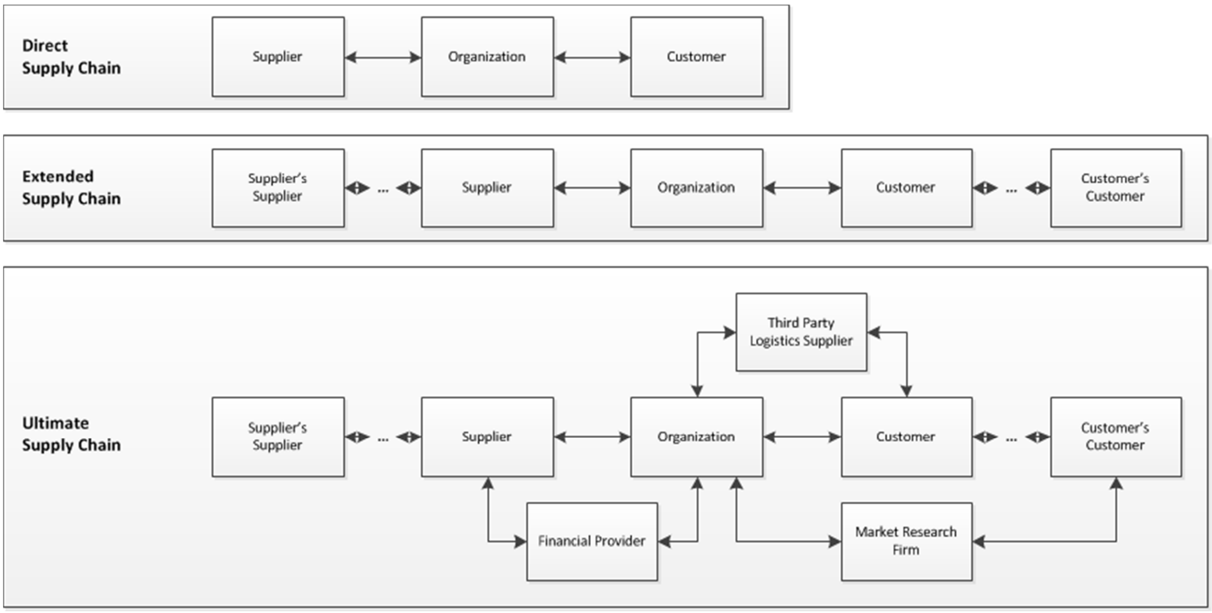


Figure 7 - ***Three types of supply chain management (Mentzer et al., 2001)***

In the paper, Mentzer et al. (2001) make a distinction between a supply chain and supply chain management. The latter is the actual management of the distribution channels of products, services, finances, and information. As can be seen in their paper, Manuj and Mentzer (2008) continued the research by Mentzer et al. (2001) by showing the places risks can occur in the extended supply chain (Figure 8).

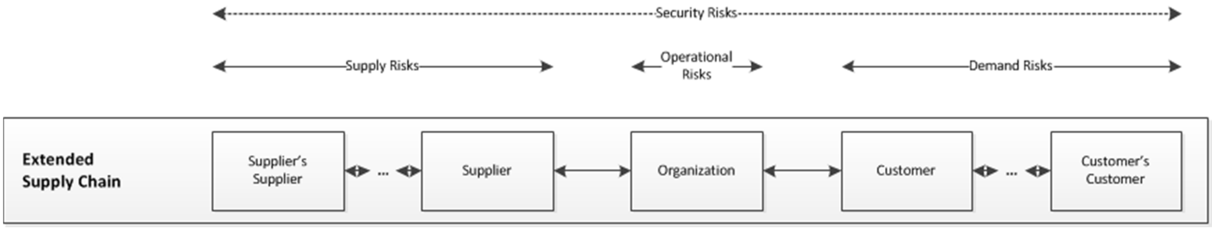


Figure 8 - ***Possible risk occurrence in the extended supply chain***

The following sources of the identified risks have been presented (Manuj & Mentzer, 2008):

- **Supply Risks -** Disruption of supply, inventory, schedules, and technology access; price escalation; quality issues; technology uncertainty; product complexity; frequency of material design changes.
- **Operational Risks -** Breakdown of operations; inadequate manufacturing or processing capability; high levels of process variations; changes in technology; changes in operating exposure.
- **Demand Risks -** New product introductions; variations in demand; chaos in the system.
- **Security Risks -** Information systems security; infrastructure security; freight breaches from terrorism, vandalism, crime, and sabotage.

On the risks involving information security, Manuj and Mentzer (2008) state that these risks come from threats from an unknown third party who may or may not be a member of the supply chain and whose motivation is to steal proprietary data or knowledge and/or destroy, upset, or disable an organization's operations. For example, if an organization is using a third party's application to process or store confidential information without knowing how the application works or how the information is stored, it can become dangerous to use the application as the application might be full of weaknesses and vulnerabilities that can be exploited. Although it is the third party's application that can be targeted by criminals, it will be hard to determine whether the stored information is untouched. In this light, it is therefore important to identify the risks that can occur in the supply chain, in this case the application that is used from a third party. Measures, as defined in the ISO 27K information security standard, such as conducting a supplier evaluation, can be implemented in order to mitigate the risks in the supply chain.

Looking at the findings on the supply chain it is necessary to add this concept to the ontology of information security as suggested by Fenz and Ekelhart (2009). An organization can be part of a supply chain and the supply chain can be targeted by certain threats (Manuj & Mentzer, 2008). Figure 9 shows the ontology of information security with the additional Supply Chain concept.

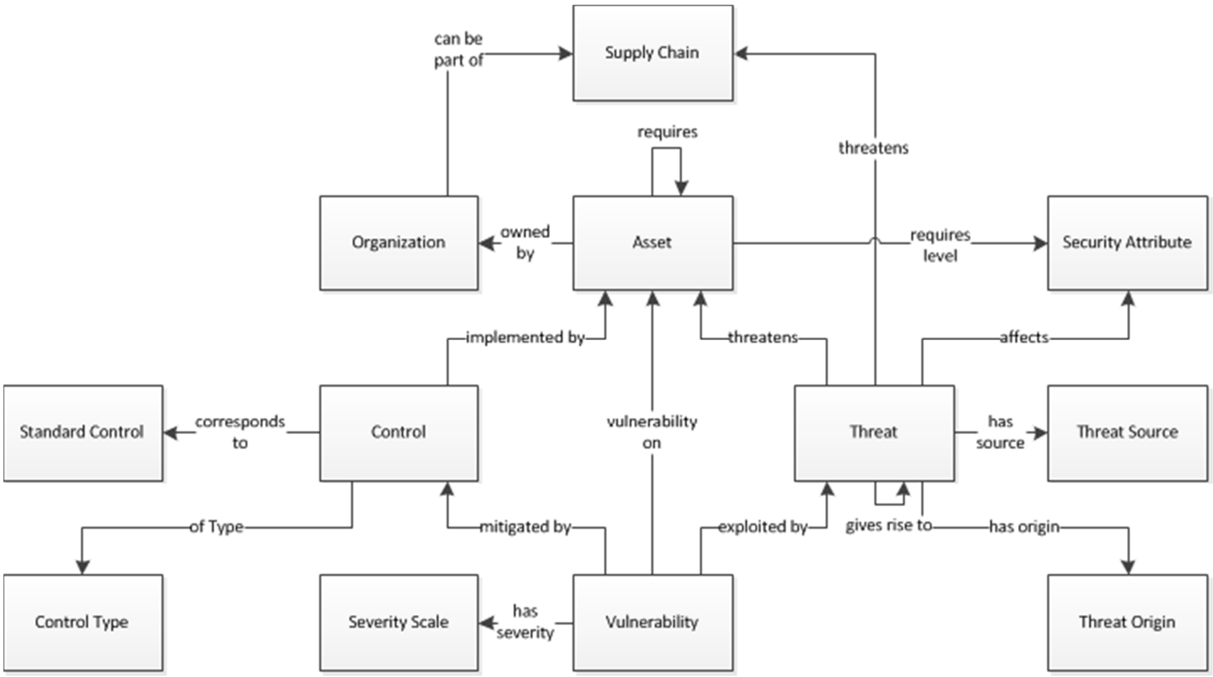


Figure 9 - ***Information security model (Fenz & Ekelhart, 2009) with additional Supply Chain concept***

3.3 Information Security Focus Area Maturity Models

The second pillar of this research is the focus area maturity model specifically focused in the information security domain. In order to understand the context of focus area maturity models, maturity models in general are discussed first. This is followed by information security maturity models, and finally by the information security focus area maturity model.

3.3.1 Maturity Models

Maturity is considered to be a measurement in order to evaluate an organization's capabilities within a certain area (Bruin & Rosemann, 2005). Maturity is measured by means of so called stages, where a stage represents a higher level as opposed to the previous stage (Rao, Metts, & Mora Monge, 2003). Based on the descriptors or variables that characterize a certain stage of a maturity model, it is possible to determine an organization's level of progress (Dekleva & Drehmer, 1997; Fraser, Moultrie, & Gregory, 2002; Gottschalk, 2009; Holland & Light, 2001; Rao et al., 2003).

As can be seen as a result of the literature analysis of Poeppelbuss, Niehaves, Simons, and Becker (2011) on maturity models in information systems research, maturity models are widely adopted in practice. The maturity models are constantly growing in numbers; 35 out of 76 papers that were analyzed by the researchers of Poeppelbuss et al. (2011), propose new maturity models and lead to the existence of similar maturity models in the same domains. Users are able to choose from an increasing multitude of potentially appropriate maturity models and are left with the challenge of identifying the most reliable, fitting, and ready-to-use model.

Most maturity models are so-called fixed-level maturity models and are less suited to incremental improvements, as they cannot express interdependencies between maturity stages (Steenbergen et al., 2010). A type of maturity model that allows incremental improvements is the focus area maturity model. Advantages of using such a maturity model are that it:

- Allows a fine-grained approach;
- Is possible to distinguish more than five overall stages of maturity. This results in smaller steps between the stages, providing more detailed guidance to setting priorities;
- Is flexible in defining both focus areas and interdependencies between focus areas (Steenbergen et al., 2010).

Focus areas form the core concepts of the focus area maturity models. By positioning the capabilities of the focus areas in the model, while considering the dependencies between each other, the focus area maturity model presents the order in which the focus areas need to be addressed and implemented. A focus area is defined by as an aspect of a functional domain covering the whole activities, responsibilities, and actors involved (Steenbergen et al., 2010). For example; risk management is a focus area in the information security functional domain (Spruit & Roeling, 2014) as well as the development of architecture in the enterprise architecture functional domain (Steenbergen et al., 2010). Focus areas can be divided into a number of capabilities, depicted in the matrix by capital letters. Capabilities are ways to achieve a predefined goal, which is defined by improvement actions, which is linked to a certain maturity level (Steenbergen et al., 2010). For example; capability A is a capability in the risk management focus area on the third maturity level. In order to reach this capability an organization must ensure that the following improvement actions are covered within their organization: There is an informal risk management program; individual are aware of potential risks; and individuals should be supporting risk management. When these actions have been met, that particular capability has been reached. The position of the capabilities of a focus area indicates the order in which the capabilities should be reached: capability B of focus area 1 should be done when the improvement actions of capability A of focus area 1 have met. This is called intra-process dependencies. There are also inter-process dependencies: capability A of focus area 1 should be done when capability A of focus area 2 is reached.

Steenbergen et al. (2010) studied the steps that need to be followed in order to create a focus area maturity model. De following PDD diagram shows these steps.

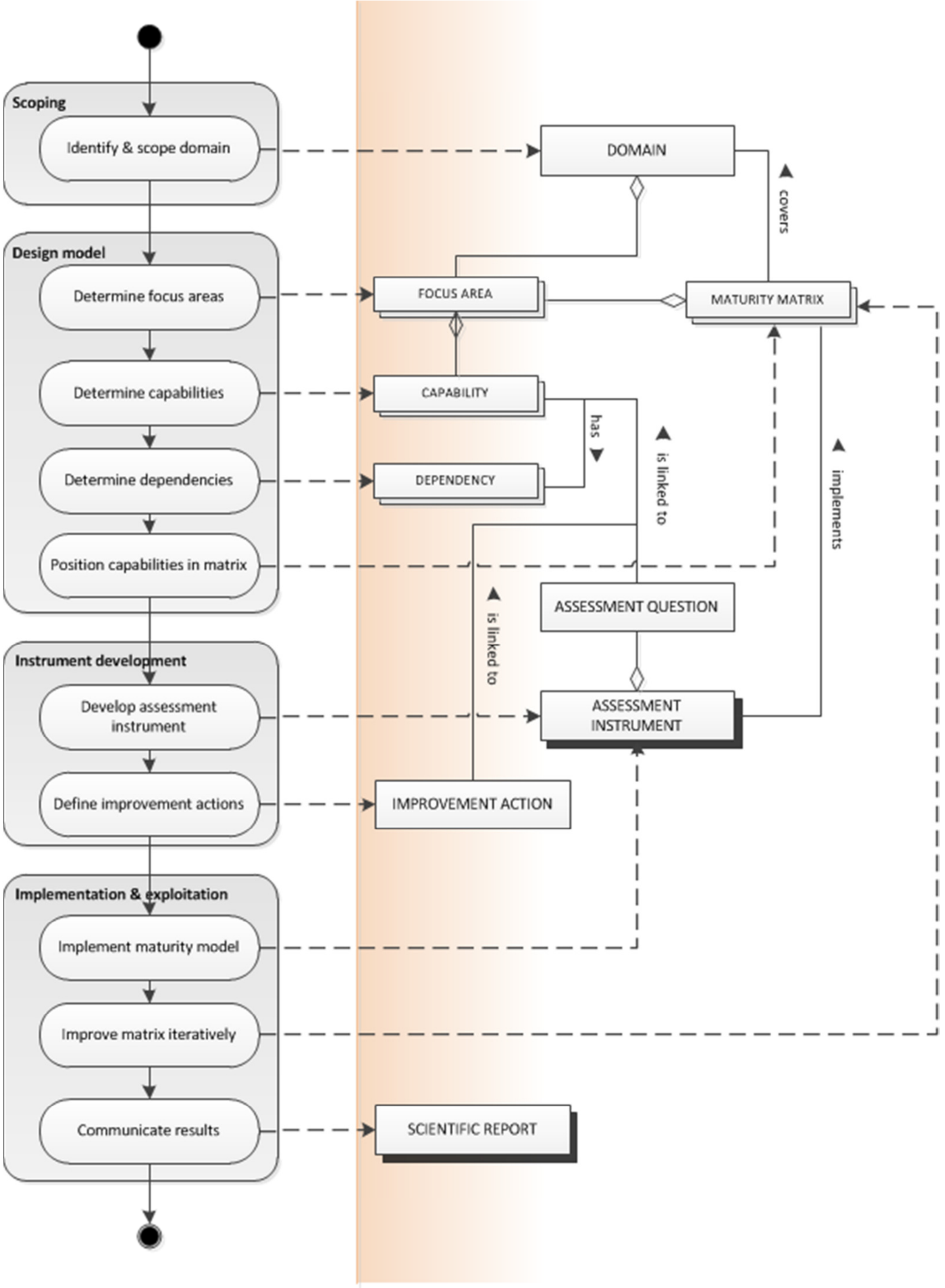


Figure 10 - ***PDD of the design of focus area maturity models (Steenbergen et al., 2010)***

3.3.2 Information Security Maturity Models

According to Lessing (2008), maturity in the field of security indicates the degree of development and the strength of the organization's security measures. The use of a security model is that it:

- generates reproducible and valid measurements;
- establish actual progress in the security environment;
- rank themselves against other organizations;
- determine the order in which security controls should be applied; and
- determine the resources needed to apply to in the security program.

Another important advantage of using a maturity model is an improvement of the stakeholder's trust in the organization (Lessing, 2008). As explained, maturity models exist of maturity stages. The maturity stages in the information security domain describe different levels in order for organizations to easily identify and understand existing security gaps; monitor the process of security implementation, practices, policies, and quality; and monitor security investment, management, and organizational audit (Karokola, Kowalski, & Yngström, 2011). An organization with full information security maturity, continuous assessment of maturity concerning information security, is able to respond to any information security related circumstances in an appropriate manner (Lessing, 2008).

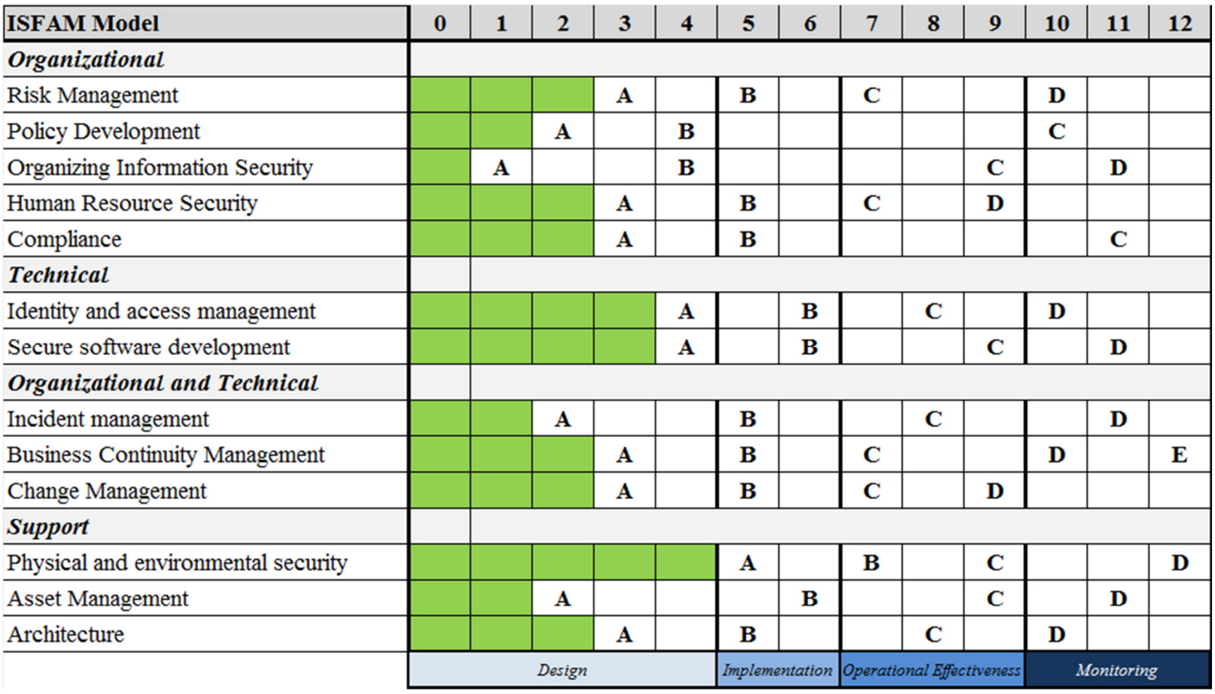
Most information security models are a poor fit for an SME due to the vast information security frameworks (Sanchez, Villafranca, & Piattini, 2007). The maturity models have been created based on information security frameworks that follow large organizations. The structures of the large organizations are mostly strict, complex, and costly, which does not fit the SME's profile. Looking at information security maturity models for SMEs, Sanchez et al. (2007) developed a model for SMEs called the Maturity Model for Security Management in SMEs (MMISS-SME). The MMISS-SME characterized itself by having three security levels (1 to 3) instead of the 5-6 levels proposed by the classical models; by the certification possibility of each level; and by associating the model with the characteristics of an organization. Another information security maturity model for SME is described in the paper of Cholez and Girard (2014). This model uses the widely used ISO standard and, like the MMISS-SME, considers the organizational characteristics by adjusting the amount of information security levels.

As explained, focus area maturity models allow a more suitable incremental improvement path due to the interdependencies between maturity stages. In the field of information security, the Information Security Focus Area Maturity model (ISFAM) exists. This model follows the focus area design as presented by Steenbergen et al. (2010) and focuses on the information security for SMEs.

3.3.3 Information Security Focus Area Maturity Model

The information security focus area maturity model (Spruit & Roeling, 2014) is a focus area maturity model that has its scope in the information security domain and focuses on SMEs. The model consists of four focus area categories (organizational, technical, organizational and technical, and support) which cluster 13 different aspects, or focus areas, and distribute 51 capabilities (A-E) over 12 maturity levels. The maturity levels are grouped into four maturity stages: Design, Implementation, Operational Effectiveness, and Monitoring. The assessment of the maturity model consists of a list of 162 close-ended (yes/no) statements. The focus areas and capabilities of the ISFAM model were determined by comparing five information security standards: ISO 27K, Information Security

Framework (based on ISO), Standard of Good practice (ISF), and IBM security framework, and was evaluated by information security experts. The result of the research is shown in Figure 11.



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management	🟩	🟩	🟩	**A**		**B**		**C**			**D**		
Policy Development	🟩	🟩	**A**		**B**						**C**		
Organizing Information Security	🟩	**A**			**B**					**C**		**D**	
Human Resource Security	🟩	🟩	🟩	**A**		**B**		**C**		**D**			
Compliance	🟩	🟩	🟩	**A**		**B**						**C**	
Technical													
Identity and access management	🟩	🟩	🟩	🟩	**A**		**B**		**C**		**D**		
Secure software development	🟩	🟩	🟩	🟩	**A**		**B**			**C**		**D**	
Organizational and Technical													
Incident management	🟩	🟩	**A**			**B**			**C**			**D**	
Business Continuity Management	🟩	🟩	🟩	**A**		**B**		**C**			**D**		**E**
Change Management	🟩	🟩	🟩	**A**		**B**		**C**		**D**			
Support													
Physical and environmental security	🟩	🟩	🟩	🟩	🟩	**A**		**B**		**C**			**D**
Asset Management	🟩	🟩	**A**				**B**			**C**		**D**	
Architecture	🟩	🟩	🟩	**A**		**B**			**C**		**D**		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Figure 11 - ***The information security focus area maturity model (Spruit & Roeling, 2014)***

3.4 Organizational Characteristics

An often heard criticism (Bollinger and McGowan, 1991) is that having a static maturity model that applies for every organization is oversimplifying reality and results in a poor model fit, because every organization has its own organizational characteristics that are different from other organizations. Organizations that use maturity models should critically analyze the available and existing models and interpret the maturity assessment results against their own characteristics (Poeppelbuss et al., 2011). As stated by Mettler and Rohner (2009), most prescribed improvement activities in a maturity model are inefficient for SMEs due to the level of bureaucracy or missing financial basis for the realization of improvement actions. Mettler and Rohner (2009) mention that the following factors need to be taken into account: economic orientation (financial revenue), organization size, coordination form, decision making, departmentalization, communication, and automation level.

According to the study by Mijnhardt et al. (In Press), eleven organizational characteristics affect the information security and therefore affect the information security maturity model. An example characteristic is the sector of an organization. Organizations in different sectors have different requirements of information security and therefore require different information security. A good example of differences of information security per sector can be found in the health sector. Due to the sensitive information of patients, medical institutions in the health sector demand a more elaborate level of security of the supportive applications and services provided by a software development organization. The available information security frameworks, of which organizations can choose from, underline the differences of information security per sector (Esra & Soysal, 2012; ISO27002:2013):

- ISO 27799: Health informatics - Information security management in health;
- NEN7510: Medische informatica - Informatiebeveiliging in de zorg (Health informatics - Information security management in health), especially focused on the Dutch health sector;
- The financial sector: ISO/IEC TR 27015: Information technology - Security techniques - Information security management guidelines for financial services;
- The telecoms sector: ISO 27011: Security techniques - Information security management for telecommunications;
- And the energy sector: ISO 27019: Security techniques - Information security management based on ISO27K for process control systems specific to the energy industry.

Mijnhardt et al. (In Press) concluded that ten other organizational characteristics, next to the sector of an organization, affect the information security. Their research was carried out by conducting a literature review comprising 71 papers, book chapters, and white papers of which the organizational characteristics were derived. The found characteristics were then evaluated by five information security experts. According to the study by Mijnhardt et al. (In Press), the four themes comprising 11 organizational characteristics as presented in Table 4 are considered to be the characteristics that have an effect on the information security and therefore on the information security maturity model.

(A) General	(B) Outsourcing	(C) IT Dependency	(D) IT Complexity
Number of Employees	Percentage of Outsourced versus Insourced Software Development	Importance of Critical Data	Number of Employees supporting IT Environment
Revenue	Percentage of Outsourced versus Insourced Software Hosting/IT Services	Importance of Confidentiality of Critical Data	Annual Expenditure on IT over Revenues
Sector		Importance of Availability of Critical Data	
		Possible Time without IT Support	

Table 4 - ***Organizational characteristics that have an effect on information security (Mijnhardt et al., In Press)***

A statistical survey study done by Baars et al. (2014) followed up on the research of Mijnhardt et al. (In Press). Mijnhardt et al. (In Press) did not investigate the effects on existing information security models and Baars et al. (2014) therefore further evaluated the organizational characteristics and their measurement levels, and how the organizational characteristics pertain to the ISFAM model in order to understand the influence of the organizational characteristics on the focus areas within the ISFAM model. According to the research done by Baars et al. (2014), organizational characteristics influence both the maturity model as well as the focus areas that it comprises.

Based on the above findings, next to the additional *Supply Chain* concept, the concept *Organizational Characteristic* is part of the information security model. Figure 12 depicts the information security model of Fenz and Ekelhart (2009), together with the previously added supply chain concept and the organizational characteristics concept (Mijnhardt et al., In Press).

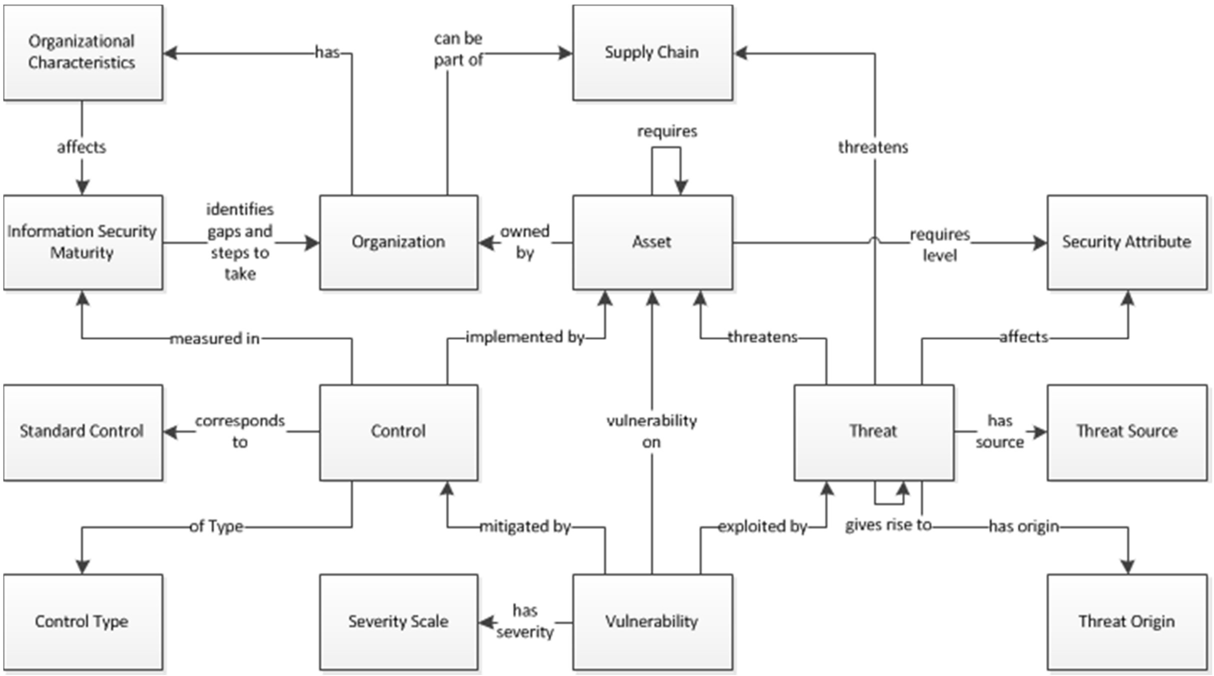


Figure 12 - ***Information security model (Fenz & Ekelhart, 2009) with additional concepts***

3.5 Rule-based Approach

Rule-based systems, rule-based expert systems, or just simple expert systems, are systems that use rules and are often represented in the form of "if-then" rules or as data within the computer which can be recalled to find a solution to real-world problems that normally would require human interference (Abraham, 2005). Abraham (2005) and Liao (2005) mentioned that the rule-based approach has been used in modern intelligent systems, as for example in strategic goal setting, planning, design, and scheduling.

As explained in the introduction, there are some advantages in using the rule-based approach. Using the rule-based approach makes it easier to implement changes as opposed to for example an Excel form (Spruit & Roeling, 2014), the maintenance and development time are low, and adjustments can be done not only by programmers, but by business people (consultants) as well (Graham, 2007).

3.5.1 Architecture

Hayes-Roth (1985) identifies two components of rule-based systems: a knowledge base and an inference engine. The knowledge base or rule base is the component that holds the rules which will be explained in the next section. These rules can be defined by the business expert. The inference engine component calculates the output based on the input of the user and the rules defined in the knowledge base. The engine follows three steps: (**1**) match facts against rules, (**2**) select a rule, and (**3**) execute the rule.

Masood and Soo (2002) also included the user interface component because the system needs an in and output. The interface component is the frond-end of the system through which the user communicates. Figure 13 depicts the components of a simple rule-based system as explained by Hayes-Roth (1985) and Masood and Soo (2002).

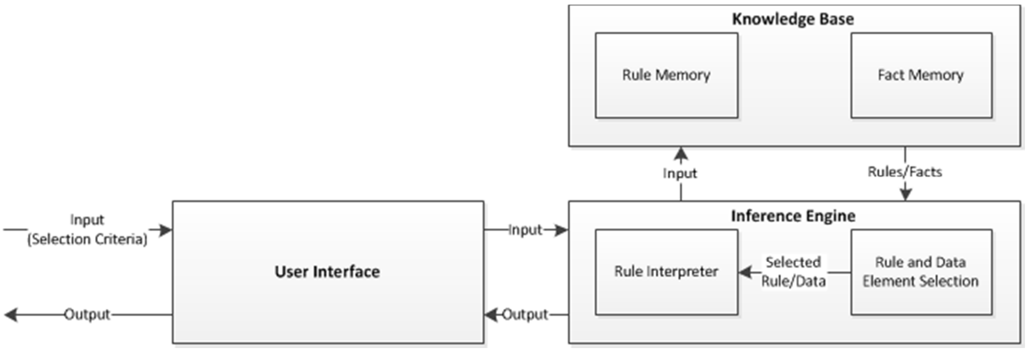


Figure 13 - ***Rule-based system components as explained by Hayes-Roth (1985) and Masood and Soo (2002)***

3.5.2 Rules

According to Browne (2009), a business rule is "any bit of knowledge that can be expressed in the following format: **When** 'something' is true, **Then** do 'this'". The business rules, action rules or just simple rules (Graham, 2007) always follow the basic form (Ligeza, 2006):

rule: <precondition> → <conclusion>

The "precondition" part is called condition, premise, antecedent, or Left Hand Side (LHS). The basic form is expressed as follows (Ligeza, 2006):

LHS(rule) = <precondition>,

The "conclusion" part is called conclusion, action, consequent, or Right Hand Side (RHS). The basic form is expressed as follows (Ligeza, 2006):

RHS(rule) = <conclusion>.

Having multiple preconditions (p_1, p_2… p_n) in a rule towards one conclusion (h) is a common way of using rules and is expressed as follows:

$$p_1 \text{ AND } p_2 \text{ AND} \ldots \text{AND } p_n \rightarrow h$$

The following example shows in a less abstract way how a rule works in a rule-based system:

Rule **"Do I need sunscreen?"**
When [the sun] = "burning"
And [sunscreen] = "false"
Then [the recommended action] = "apply sunscreen"

The name of this particular rule is [Do I need sunscreen?]. The preconditions of the rules are: the sun that needs to burn and the sunscreen that has not been applied yet. When the preconditions are met, applying sunscreen is the conclusion that follows.

3.5.3 Rules Matching

There are two types of matching to find a solution for the problem given by the user: forward chaining or data driven and backward chaining or goal driven (Figure 14) (Buchanan & Shortliffe, 1984).

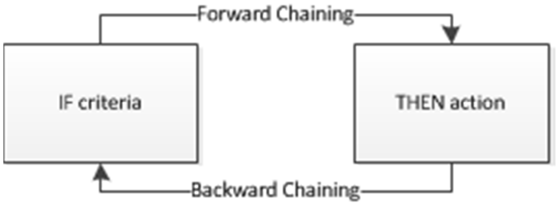


Figure 14 - ***Forward and backward chaining (Buchanan & Shortliffe, 1984)***

In the case of forward chaining, the system looks through the rule-based system to find the "if" rules and determine which actions should be triggered in order to solve a specific problem. When the "if" (condition) part of the rule matches a fact, the rule is fired and its "then" (action) part is executed and can trigger another rule. The following (Buchanan & Shortliffe, 1984) shows forward chaining.

If A, then B (Rule 1)
If B, then C (Rule 2)
A (Input)
C (Conclusion)

Using the sunscreen rule to explain forward chaining:

Rule 1 **Rule** **"Does the sun shine?"**
When [time] = ">11AM"
And [time] = "<3PM"
And [Season] = "summer"
Then [the sun] = "burning"

Rule 2 **Rule** **“Do I need sunscreen?”**
When [the sun] = “burning”
Then [the recommended action] = “apply sunscreen”

Looking at the rules, when the input is “it is 1PM in summer”, the outcome of the first rule will be that [the sun] is “burning”, triggering the second rule leading to the conclusion of [apply sunscreen].

With backward chaining, the system is given a certain goal and needs to look through the knowledge base to find the corresponding actions. The following example (Buchanan & Shortliffe, 1984) explains backward chaining.

Find out C (Goal)
If B, then C (Rule 1)
If A, then B (Rule 2)
If A, then C (Implicit rule)
Question: Is A true?

Using the sunscreen rule to explain backward chaining:
Looking at the rules, when the goal is given the conclusion “apply sunscreen”, the system will check which rule produces this outcome, which is rule 2. The system then checks which rule produces the input of rule 2, [the sun] is “burning”, which will lead to rule 1. The implicit rule is then: “if it is between 11AM and 3PM in summer, then apply sunscreen”.

These two ways, in order to find the right outcome, are defined and handled in the inference engine.

3.5.4 Application of Rules in Information Security

Using rules to change an information security maturity model for organizations with different organizational characteristics fits the list of modern day usage of rule-based systems (Abraham, 2005; Liao, 2005) due to the strategic planning nature of a maturity model. Using the rule-based approach in combination with information security can be beneficial; when the information security changes and there are situational maturity models for each type of organization, updating each of these models would take a lot of time, whereas updating the rules in a centralized rule-based system will be much easier. Multiple researches have combined the rule-based approach with information security. Walek, Bartos, and Zacek (2013), Atymtayeva, Kozhakhmet, and Bortsova (2014), and Bartoš, Walek, Klimeš, and Farana (2014) used the rules to identify the relevant countermeasure based on the vulnerabilities of the assets of an organization and the risks that can occur. The following rule to classify the risk factor of an asset is used by Walek et al. (2013):

IF asset_value==medium
AND threat (medium, medium)
AND weight==high
THEN risk=high

Close to the research at hand is the study of Tae-Nyeon and Hovav, who created a prototype in an expert system which helps SMEs in their information security. Their prototype considered the organizational characteristics of the SME, and based on an assessment, the prototype was able to rate the information security of the human resource part of the SME. Based on this security rate, the prototype could give potential improvements and recommendations, much like the information security focus area maturity model of Spruit and Roeling (2014). It is however not clear how the rules within the expert system in this particular project have been applied.

This page intentionally left blank

4 Information Security Focus Area Maturity Model

This section focuses on the second pillar, the focus area maturity model. The ISFAM model that is used in the research is explained here.

4.1 ISFAM 2.0

The information security focus area maturity model (Spruit & Roeling, 2014) is a focus area maturity model that has its scope in the information security domain. In order to update the model, the steps in order to create a focus area maturity model as stated by Steenbergen et al. (2010) have been followed and are presented next.

4.1.1 Identify and Scope the Functional Domain

The first step of designing focus area maturity models is determining the functional domain scope of the focus area maturity model, which in this case follows the scope of the initial ISFAM model of Spruit and Roeling (2014), the information security domain.

4.1.2 Determine Focus Areas

The next step is determining the focus areas of the maturity model for the functional domain. Spruit and Roeling (2014) initially compared the ISO 27K:2005, the CISSP, the information security framework (based on ISO), Standard of Good practice (ISF), and the IBM security framework and concluded a total of 13 focus areas, which were found by comparing the focus areas of the five different information security standards and then validated by expert interviews. The 13 information security focus areas are as follows:

1. Risk Management;
2. Policy Development;
3. Organizing Information Security;
4. Human Resource Security;
5. Compliance;
6. Identity and Access Management;
7. Secure Software Development;
8. Incident Management;
9. Business Continuity Management;
10. Change Management;
11. Physical and Environmental Security;
12. Asset Management;
13. Architecture.

As can be seen in the literature study, a new version of the ISO 27K standard has been released introducing the additional section Supplier Relationships. Second, according to the papers of Li and Chandra (2008) and Li, Chandra, and Shiau (2009), supply chain security is an important concept of information security.

Next to that, the Cloud Security Alliance (CSA) developed the so-called Cloud Control Matrix (CCM) in 2013 which is a matrix that includes controls from 20 different security best practices and standards (Cloud Security Alliance, 2013). Although the title of the matrix suggests that the matrix focuses on information security in the cloud alone, the matrix actually focuses on more aspects of information security than just the cloud. As an example of the broader focus in information security, the Human Resources section states: "Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period." Another example: "Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems." In these examples it can be seen that the information security stated in the CCM is not focused on information security in the cloud alone.

The following table shows the 13 focus areas found by Spruit and Roeling (2014) and the 16 focus areas that have been found by the CSA in their CCM.

ISFAM's focus areas **(Spruit and Roeling, 2014)**	**CCM's focus areas** **(Cloud Security Alliance, 2013)**
Architecture	Application & Interface Security;
Asset Management	Audit Assurance & Compliance;
Business Continuity Management	Business Continuity Management & Operational Resilience;
Change Management	Change Control & Configuration Management;
Compliance	Data Security & Information Lifecycle Management;
Human Resource Security	Datacenter Security;
Identity and Access Management	Encryption & Key Management;
Incident Management	Governance and Risk Management;
Organizing Information Security	Human Resources;
Physical and Environmental Security	Identity & Access Management;
Policy Development	Infrastructure & Virtualization Security;
Risk Management	Interoperability & Portability;
Secure Software Development	Mobile Security;
	Security Incident Management, E-Discovery & Cloud Forensics;
	Supply Chain Management, Transparency and Accountability;
	Threat and Vulnerability Management.

Table 5 - ***Focus areas of both ISFAM and the CCM***

It is clear that the focus areas of the CCM are more elaborate than the focus areas of ISFAM. A comparison, as can be seen in the next table, between the focus areas of both the CCM and the ISFAM model is done in order to see whether there are focus areas missing in the maturity model.

CCM's focus areas **(Cloud Security Alliance, 2013)**	**Present**	**Rationale to in or exclude focus areas defined by CSA in the ISFAM model**
Application & Interface Security;	√	Covered in Secure Software Development
Audit Assurance & Compliance;	√	Covered in Compliance
Business Continuity Management & Operational Resilience;	√	Covered in Business Continuity Management
Change Control & Configuration Management;	√	Covered in Secure Software Development and Change Management

Data Security & Information Lifecycle Management;	√	Covered in Organizing Information Security
Datacenter Security;	√	Covered in Asset Management
Encryption & Key Management;	√	Covered in Change Management
Governance and Risk Management;	√	Covered in Risk Management
Human Resources;	√	Covered in Human Resource Security
Identity & Access Management;	√	Covered in Identity and Access Management
Infrastructure & Virtualization Security;	√	Covered in Physical and Environmental Security
Interoperability & Portability;	√	Covered in Architecture
Mobile Security;	√	Covered in Architecture
Security Incident Management, E-Discovery & Cloud Forensics;	√	Covered in Incident Management
Supply Chain Management, Transparency and Accountability;	X	Not included in the focus areas of ISFAM
Threat and Vulnerability Management.	√	Covered in Risk Management

Table 6 - ***The rationale of including or excluding focus areas in the ISFAM model***

As can be seen in the comparison above and based on the findings of the literature study, Supply Chain Management or Supply Chain Security is not part of the focus areas of the ISFAM model (Spruit & Roeling, 2014) and needs to be added.

4.1.3 Determine Capabilities

For time constrain reasons, only the capabilities of the missing focus area, the Supply Chain Management, will be determined. Supply chain management should focus on the mitigation of the risks in the supply chain. The only place in the ISFAM model that takes suppliers into account is one requirement of capability D of the Risk Management focus area: *Risk management program involves customers and suppliers*. However, supply chain management covers more than only involving the customers and suppliers in the risk management program. In the Supply Chain Risk Mitigation paper of Faisal, Banwet, and Shankar (2006), risks are mitigated by means of 11 enablers. The enablers are categorized, in order to fit them in capabilities:

- Focus on information
    - Information sharing;
    - Information security;
    - Risk sharing in supply chain;
    - Knowledge about risks in a supply chain.
- Focus on supply chain partners
    - Agility in the supply chain;
    - Trust among supply chain partners;
    - Collaborative relationships among supply chain partners;
    - Corporate social responsibility.
- Focus on policies
    - Aligning incentives and revenue sharing policies in supply chain;
    - Strategic risk planning;
    - Continual risk analysis and assessment.

Although risk management focuses on the operational risks of the organization and supply chain management focuses on the supply and demand management, risk management is in line with supply chain management because both aspects focus on mitigating risks that can possibly occur. According to Spruit and Roeling (2014), the risk maturity has four levels of maturity. Supply chain management follows the same four levels of risk management (Table 7).

Maturity level	**Description**
0 – None	No consideration of third parties in the supply chain. Information is being shared, but the consequences of risks are not known or managed.
A - Naïve	Awareness of the consequences of possible risks in the supply chain.
B – Novice	Conceptual policies are made in order to mitigate the risks.
C – Normalized	Policies, including risk planning and risk analysis in the supply chain are in place.
D – Natural	Continual risk analysis of the supply chain.

Table 7 - ***Maturity levels of the Supply Chain Management focus area***

Table 8 presents the capabilities of the Supply Chain Management focus area determined based on the enablers of Faisal et al. (2006).

Supply Chain Management	**Capability description**
A - Naïve	• Informal supply chain management policy; • Low monitoring of information flowing through the supply chain; • Low awareness and knowledge of risks in the supply chain; • Low support for supply chain management.
B - Novice	• Strategically defined supply chain risk management; • Growing awareness and knowledge of risks in the supply chain; • Proactive management support for supply chain management.
C - Normalized	• Investment in selecting and maintaining collaborative relationship of supply chain participants; • Knowledge of risks and risks are shared with participants in the supply chain; • Formalized Supply Chain Management is shared with participants in the supply chain; • Formalized supply chain management policy.
D - Natural	• Maintaining awareness of risks in the supply chain; • Monitoring of information flow; • Continual risk analysis; • Continual risk assessments.

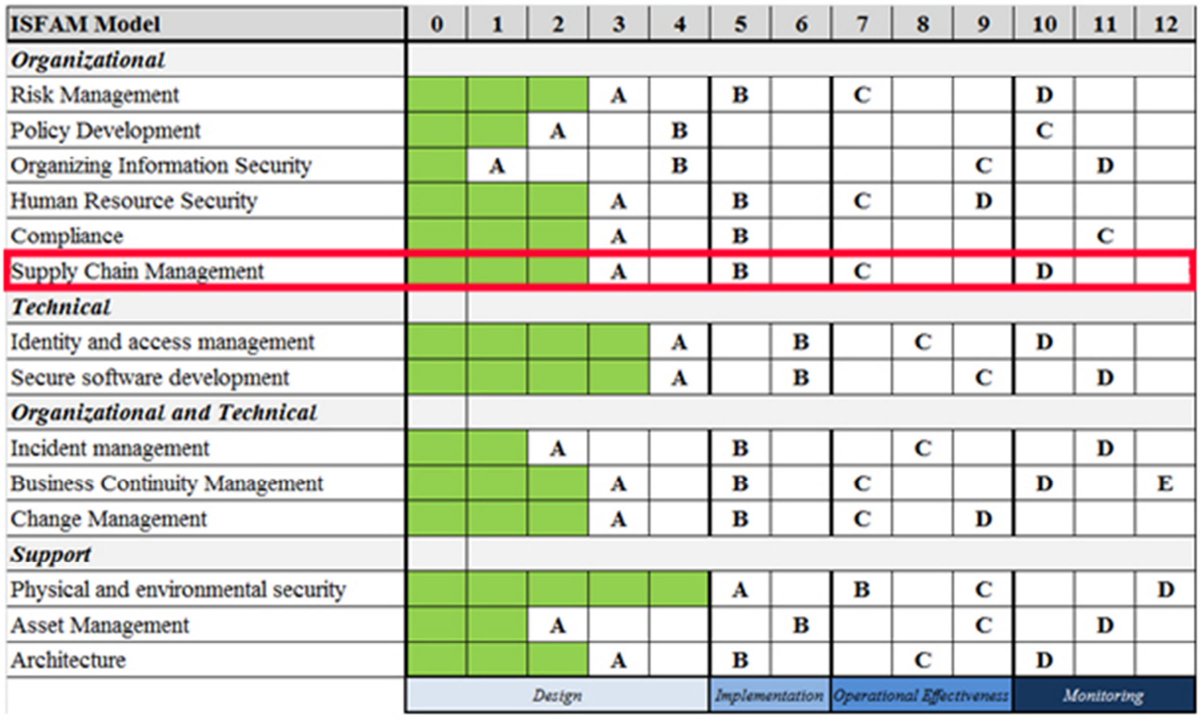
Table 8 - ***Capabilities of the Supply Chain Management focus area***

As explained, the only place risks within the supply chain are covered is in capability D in the risk management focus area. Because of the extra supply chain focus area, the supply chain requirement in the risk management focus area has been omitted.

4.1.4 Determine Dependencies and position capabilities

No dependencies between other focus areas have been found as a result of the literature study. However, it can be argued that the policy of the supply chain management, just like the policies that are needed in other focus areas, can only be created once the first level of policy development has been reached. The first capability is therefore placed on the third maturity level of the ISFAM model. The other capabilities of the supply chain management focus area are placed at the beginning of each of the three maturity stages, due to their implementation, operational effectiveness, and monitoring nature. For example, a statement in the last capability describes that the organization should monitor the information flow, which follows the monitoring maturity stage of the model. The last capability is therefore placed at the tenth maturity level. The capabilities are set at the maturity levels three, five, seven, and ten.

Based on the added focus area with the defined capabilities, the following matrix presents the updated version of the ISFAM model with the additional focus area Supply Chain Management. The Supply Chain Management focus area can be found at the sixth place in the ISFAM model, because of the organizational oriented capabilities of the focus area.



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management	🟩	🟩	🟩	A		B		C			D		
Policy Development	🟩	🟩	A		B						C		
Organizing Information Security	🟩	A			B					C		D	
Human Resource Security	🟩	🟩	🟩	A		B		C		D			
Compliance	🟩	🟩	🟩	A		B						C	
Supply Chain Management	🟩	🟩	🟩	A		B		C			D		
Technical													
Identity and access management	🟩	🟩	🟩	🟩	A		B		C		D		
Secure software development	🟩	🟩	🟩	🟩	A		B			C		D	
Organizational and Technical													
Incident management	🟩	🟩	A			B			C			D	
Business Continuity Management	🟩	🟩	🟩	A		B		C			D		E
Change Management	🟩	🟩	🟩	A		B		C		D			
Support													
Physical and environmental security	🟩	🟩	🟩	🟩	🟩	A		B		C			D
Asset Management	🟩	🟩	A				B			C		D	
Architecture	🟩	🟩	🟩	A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Figure 15 - ***Updated ISFAM model with the additional focus area Supply Chain Management***

4.1.6 Develop Assessment Instrument

The assessment of the initial information security maturity model as defined by Spruit and Roeling (2014) in order to get the current information security maturity of an organization consists of a list of 162 close-ended (yes/no) statements. The assessment will be expanded with 15 yes/no questions of the Supply Chain Management focus area as shown below.

- Capability A
    - Is there an informal supply chain management policy?
    - Is the information flowing through the supply chain being monitored at all?
    - Is there any awareness and knowledge of risks in the supply chain?
    - Is there support for supply chain management?

- Capability B
    - Is the supply chain risk management strategically defined?
    - Is awareness and knowledge of risks in the supply chain growing?
    - Is there a proactive management support for supply chain management?

- Capability C
    - Is there any investment in the selection and maintaining of collaborative relationship of supply chain participants?
    - Is knowledge of risks and risks being shared with participants in the supply chain?
    - Is there a formalized Supply Chain Management which is shared with participants in the supply chain?
    - Is there a formalized supply chain management policy?

- Capability D
    - Is the awareness of risks in the supply chain being maintained?
    - Is there a continual monitoring of the information flow?
    - Are risks continual being analyzed?
    - Are risk assessments continual being conducted?

4.2 ISFAM 2.0 Evaluation

As explained in the research approach, the artifact will be evaluated on three points. The first two points, the evaluation of additional focus areas and the evaluation of the updated ISFAM at a case organization, will be discussed next.

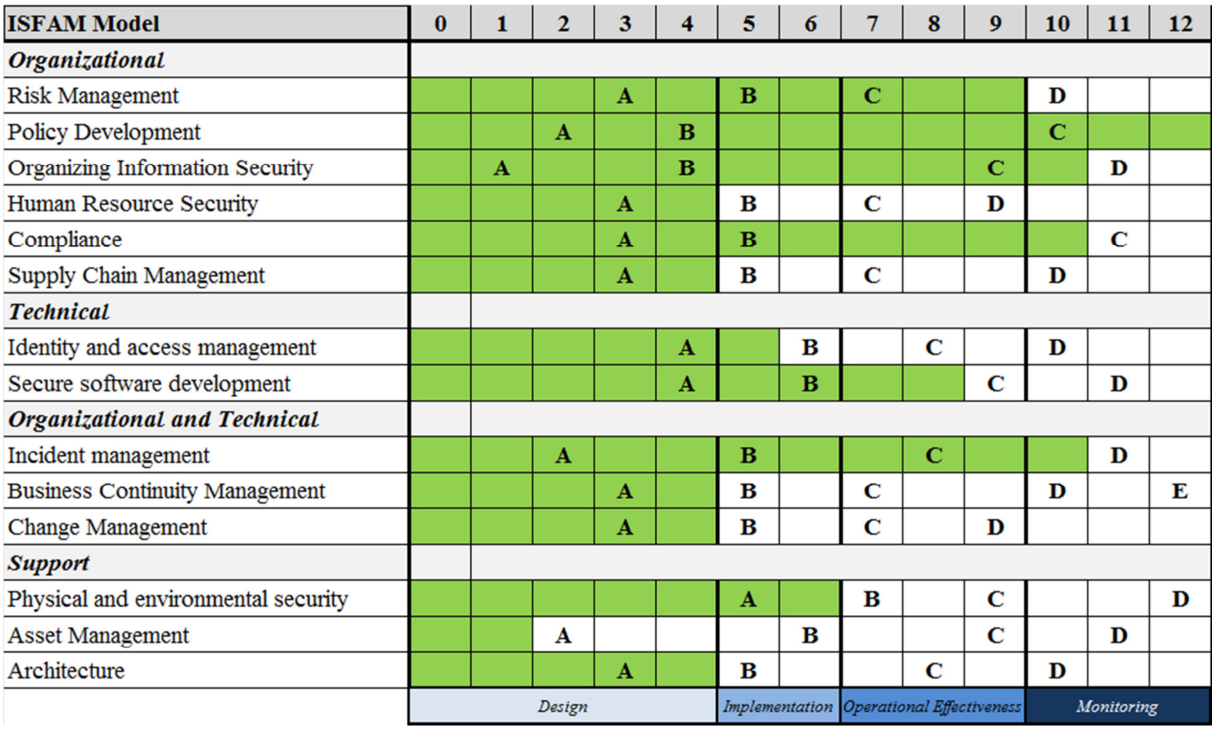
4.2.1 Information Security Experts

The first evaluation point in this research is the evaluation of possible additional focus areas in the information security maturity model. This includes the capabilities of the focus area as well and is done in order to validate the improvements made to the model. The updated model is evaluated by the same information security experts as were selected in order to study the effects of organizational characteristics. The information security experts will be introduced in the next section, as the expert were selected based on criteria to find organizational characteristics.

According to the information security experts, the Supply Chain Management focus area is one of the most important focus areas within the information security maturity matrix for SMEs. SMEs are more dependent on third parties than larger organizations, because larger organizations have the means of developing their products entirely by themselves as opposed to the smaller organizations. On the capabilities of the focus area, according to the experts, the capabilities have been well defined so that an organization can mature in a gradual manner and do not need further adjustment.

4.2.2 Single Case Study

The original ISFAM model was initially evaluated using a single case study at a small/medium sized telecom, media and technology organization. According to the researchers, it was uncertain whether the model was applicable for other organizations as well. The ISFAM model with the additional Supply Chain Management focus area is now evaluated by means of a single case study (Yin, 2003) using a software developing SME as the case organization in order to prove that the ISFAM model, in its updated form, can be assessed in this sector as well. The case organization is an SME in the range of 10-50 Number of Employees, has a revenue in the category 0-2 million and creates applications and stores client data for the health sector. Together with the information security officer of the organization, the case organization's information security has been assessed using the updated ISFAM model. The differences between the initial ISFAM model and the updated ISFAM model are discussed with information security experts of the case organization in order to study the added value of the updated ISFAM model. The following figure shows the assessment of the information security of the case organization with the use of the ISFAM model, which was conducted in the second half of 2014.



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management	🟩	🟩	🟩	🟩 A	🟩	🟩 B	🟩	🟩 C	🟩	🟩	D		
Policy Development	🟩	🟩	🟩 A	🟩	🟩 B	🟩	🟩	🟩	🟩	🟩	🟩 C	🟩	🟩
Organizing Information Security	🟩	🟩 A	🟩	🟩	🟩 B	🟩	🟩	🟩	🟩	🟩 C	🟩	D	
Human Resource Security	🟩	🟩	🟩	🟩 A	🟩	B		C		D			
Compliance	🟩	🟩	🟩	🟩 A	🟩	🟩 B	🟩	🟩	🟩	🟩	🟩	C	
Supply Chain Management	🟩	🟩	🟩	🟩 A	🟩	B		C			D		
Technical													
Identity and access management	🟩	🟩	🟩	🟩	🟩 A	🟩	B		C		D		
Secure software development	🟩	🟩	🟩	🟩	🟩 A	🟩	🟩 B	🟩	🟩	C		D	
Organizational and Technical													
Incident management	🟩	🟩	🟩 A	🟩	🟩	🟩 B	🟩	🟩	🟩 C	🟩	🟩	D	
Business Continuity Management	🟩	🟩	🟩	🟩 A	🟩	B		C			D		E
Change Management	🟩	🟩	🟩	🟩 A	🟩	B		C		D			
Support													
Physical and environmental security	🟩	🟩	🟩	🟩	🟩	🟩 A	🟩	B		C			D
Asset Management	🟩	🟩	A				B			C		D	
Architecture	🟩	🟩	🟩	🟩 A	🟩	B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Figure 16 - ***ISFAM assessment at case organization***

As can be seen in the assessment of the case organization, some information security focus areas are set at a high maturity level, such as Risk Management and Policy Development, while others remain very low, such as Human Resource Security and Supply Chain Management. The results of the assessment were discussed with the information security officer. According to the information security officer, the case organization is preparing to get the ISO 27K for information security certificate. This explains the high levels in Risk management, Policy Development, Compliance, and Incident Management. On the other hand, looking at the focus areas with a low maturity level, human resource security is not considered important for the clients of the organization and is therefore not focused on, explaining the low maturity. Next to that, the organization just recently started to work with third parties and is therefore not experienced in defining the risks that can occur in the supply chain. Lastly, the assets of the organization are not up to date and some are missing in their list of assets. In order to reach the first maturity level in this section, management has to be made responsible for the asset management within departments.

As can be derived from the model, the case organization should first focus on reaching the first level of the Asset Management focus area. As explained, this can be done by making the senior managers responsible for the assets of the organization and making them aware of the importance of asset management.

According to the information security officer and members of the information security team of the case organization, the information security maturity model is a valuable tool in order to see which steps need to be taken, especially when the organization is at the starting phase of implementing information security. The visual representation makes the maturity of information security very clear and understandable. Next to that, the additional focus area Supply Chain Management is added just at the right moment, since the organization started working with third parties.

This page intentionally left blank

5 Effects of Organizational Characteristics on ISFAM

This section focuses on the third pillar of the research, the organizational characteristics. The results of the study of organizational characteristics affecting the ISFAM model are presented in this section.

5.1 Organizational Characteristics

Due to time restriction, only the effects of a sub-set of organizational characteristics on the ISFAM model have been researched. The first theme of organizational characteristics, the general theme including Number of Employees (NoE), Revenue, and Sector, is studied in this research. According to Mijnhardt et al. (In Press), this theme affects the information security maturity model. However, it is not clear how the organizational characteristics have an effect on the capability level of the ISFAM model.

Number of Employees

According to the experts interviewed by the researchers of Mijnhardt et al. (In Press), the number of employees is a crucial indicator of both size and complexity of the organization. The scale of this factor is defined based on the number of employees in the SME category:

1. 0 - 10;
2. 10 - 50;
3. 50 - 250.

Revenue

Next to the number of employees, the organization’s revenue is another crucial indicator of the size and complexity of the organization. The parameters were defined based on the ECB and World Bank:

1. 0 - 2 million;
2. 2 million - 10 million;
3. 10 million - 50 million.

Sector

Sectors have been identified as being an organizational characteristic affecting information security. The following ten sectors have been identified (Mijnhardt et al., In Press):

1. Aerospace and Defense;
2. Professional Services and Finance;
3. Energy and Utilities;
4. ICT;
5. Public and Education;
6. Consumer, Retail, Leisure, Travel, Entertainment, and Media;
7. Health;
8. Transport, Logistics, and Packaging;
9. Agriculture, Forest, and Mining;
10. Industrial Manufacturing, Engineering, and Construction.

5.2 Data Gathering

The effects of organizational characteristics are studied by means of survey research where information security experts are interviewed. As explained in the research approach, the experts were selected based on three criteria: (**1**) the experts were selected from information security consultants due to their extensive knowledge of and experience with information security in different organizations. (**2**) The information security consults should not be working in the same organization. (**3**) The last criterion is years of experience. The information security experts with around ten years of experience have been chosen for the research and resulted in a total of 54 years of information security experience. The experts have been found using LinkedIn, searching for "Information Security Consultant". The following experts have been interviewed.

Expert	Function	Years of Experience
# 1	Information Security Consultant	10
# 2	Information Security Consultant	10
# 3	Information Security Consultant	14
# 4	Information Security Consultant	8
# 5	Information Security Consultant	12
		54

Table 9 - ***Information security experts***

The interviews were held in the second half of 2014. Each interview lasted around two hours where the interviewed information security experts discussed whether the organizational characteristics Number of Employees, Revenue, and Sector affect the capabilities as defined in the ISFAM model of Spruit and Roeling (2014).

Each capability of each focus area residing in the ISFAM model has been held against the different organizational characteristics. The next table shows the template that is used to find the effects. An example question during the interview was: "*Considering capability A of the first focus area Risk Management, 'there is an informal risk management program in place', what are the differences between an organization with 0-10 employees and an organization with 50-250 employees?*"

Focus Area	Number of Employees			Revenue*			Sector
	0-10	10-50	50-250	0-2	2-10	10-50	
A							
B							
C							
D							

Table 10 - ***Template that is used in order to find the effect of organizational characteristics on the information security maturity model (* = in millions)***

The interview template and the interview transcripts have been included in the appendices. The capabilities of each focus area of the maturity model will be discussed next.

5.3 Effects Organizational Characteristics

The findings of effects of organizational characteristics as discussed with the information security experts are presented here. An analysis of the findings can be found after the findings. For readability reasons, the findings of the effects of the organizational characteristics have not been put into the template as shown above, but do follow the same structure: effects of number of employees, effects of revenue, and effects of sector.

5.3.1 *Effects on Risk Management*

According to the ISO31K – Risk Management, a risk is "the effect of uncertainty on objectives and an effect is a positive or negative deviation from what is expected." Risks in information security emerge because potential security threats are identified that could exploit vulnerabilities in an asset and therefore cause harm to an organization. In order to cope with the risks of directly or indirectly losing money (Blakley, McDermott, & Geer, 2001), an organization must have a risk management program. The use of risk management is to protect the organization's values. ISO31K has been set up in order to reduce the uncertainty as much as possible. The following table shows the capabilities of the focus area.

Risk Management	Capability description
A	• Informal risk management program; • Individual awareness of risk management; • Individuals supporting risk management.
B	• Strategically defined risk management; • Individual has been formally made responsible for risk management; • Organizational awareness of risk management; • Proactive management support risk management.
C	• Standard-based detailed risk management program; • Organization wide defined risk management roles; • Risk management is measured using defined metrics; • Formalized risk management processes.
D	• Maintaining awareness of risk management; • Risk management processes are continuously improved; • Risk management is part of the decision making process.

Table 11 - ***Risk Management capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Risk Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

SMEs are able to reach full maturity in this focus area. For example, capability D suggests that risk management processes should be continuously improved. According to the experts, these improvements can be done on every level in any possible way. Next to that, risk management as small as a text written on one page can be considered risk management. Organizations of all categories should therefore be able to reach the last capability. In practice however, risks are not managed or risks are managed using a simple spreadsheet. SMEs do not invest in risk management. Risk management is mainly done informally and most SMEs can therefore be found on capability B of the focus area maturity model.

The only difference between a larger category (50-250 NoE) organization and a smaller category (0-10 and 10-50 NoE) organization is that it is easier for the smaller organization to have a risk management program because it can be done faster.

On the revenue characteristic, an organization with a larger revenue has more to protect, but the organization is also able to spend more on risk management. It is for example possible to hire an information security consultant that focuses on the risk management of an organization. An SME with a revenue in the smallest category (0-2million) will possibly not have the money to hire such an expert.

Risk management is often being done in the sectors finance and health because of the confidence level of data. The organizations in these sectors are more experienced with risk management and are therefore found on a higher maturity level than other organizations. Next to that, not the sector but rather the framework affects the capabilities. The sector gives a selection of frameworks, but the frameworks define the requirements that mitigate risks. These requirements differ per framework.

5.3.2 Effects on Policy Development

According to the definition list of ISO 27000, a policy defines "a general commitment, direction, or intention." An information security policy should "express management's formal commitment to the implementation and improvement of its information security management system and should include information security objectives or facilitate their development." The following table shows the capabilities of the focus area.

Policy Development	**Capability description**
A	• Laws and regulations as part of the information security policy; • Management supports the development of information security policy.
B	• Every policy should address a set of standard subjects; • Policies have to consider the organization's culture and strategy; • Defining all roles and tasks of information security; • Formal writing style information security policies.
C	• Frequently reviewing the information security policies; • Organization wide understanding of the content of the policies; • Policies are based on standards; • Policies are stored on a document management system.

Table 12 - ***Policy Development capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Policy Development focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

Most of the organizations focus on the Policy Development focus area as the first step in information security.

SMEs are able to reach full maturity in this focus area. In practice however, an organization with 0-10 NoE will reside on capability A, due to the fact that the policies do not exist or policies are not written in a formal way. The other organizations are able to reach full maturity. There is a difference between the largest category (50-250 NoE) and the smaller category (0-10 and 10-50 NoE); it is easier for the smaller organization to develop policies because it can be done faster and more simplistic.

The sector of an organization has no effect on the capabilities of the Policy Development focus area, although sectors that handle sensitive information will have a larger, in terms of pages, policy. Next to that, the financial sector has a lot of rules and legislations to comply with and is therefore more experienced in developing policies. The framework that is being used tells whether an organization should focus on the development of policies.

5.3.3 Effects on Organizing Information Security

The organization of information security entails the internal organization, i.e. the roles and responsibilities of information security, and the mobile devices and teleworking, i.e. policies for ICT devices, smartphones, USB gadgets, and working-from home. The following table shows the capabilities of the focus area.

Organizing Information Security	**Capability description**
A	• Management commitment to information security; • Management allocates resources to address information security; • Management is formally responsible for information security policies.
B	• Coordination of information security aspects throughout the organization; • High-level definitions of information security roles and responsibilities; • Confidentiality agreement signed by all employees.
C	• Available authorization process for information processing; • Contact with authorities about law and regulations; • Knowledge gaining through passively participating in special interest groups.
D	• Knowledge gaining through actively participating in special interest groups; • Regular review of information security status; • Risks related to external parties are identified and updated regularly.

Table 13 - *Organizing Information Security capabilities (Spruit & Roeling, 2014)*

With the above stated capabilities of the Organizing Information Security focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

The awareness of information security is of great importance in this focus area. When the awareness can be seen amongst the management and employees, it is much easier to organize information security. The information security should be initiated by the management; however, in most organizations information security is done by some IT-guy, who focuses mainly on information security in the IT. Each organization should have assigned someone as information security officer. However, organizations still need the resources to do so.

In practice, organizations with 0-10 and 10-50 NoE reside on capability B, due to the knowledge gaining requirement which suggests that an expert needs to be hired. However, it is possible for an organization to reach full maturity in this focus area if it is the ambition of the organization.

On the revenue characteristic, an organization with a larger revenue will be able to spend more resources on organizing information security.

The sector of an organization has no effect on the capabilities of the Organizing Information Security focus area, although sectors that handle sensitive information will have a larger list of requirements when organizing information security. These organizations are more experienced and are therefore able to reach higher maturity in this focus area.

5.3.4 Effects on Human Resource Security

Human resource security is the security focused on the employees, from recruiting, to during the employment, and even after employment. Before employment a screening needs to be done. Employees during employment need to be aware of the information security policies that are defined within the organizations. After employment, the employees need to be reminded of ongoing obligations under privacy laws. The following table shows the capabilities of the focus area.

Human Resource Security	**Capability description**
A	• Human Resource Security policies are in place; • Roles and responsibilities related to Human Resource Security are defined.
B	• Human Resource Security policies are known by the employees; • Human Resource Security processes are defined; • Employees have signed the document containing their roles and responsibilities.
C	• Screening before employment; • Human Resource Security policies are fully implemented; • Human Resource Security processes are fully implemented; • Post-employment restrictions are part of the contract.
D	• Regular review of Human Resource Security policies; • Continuous optimization of Human Resource Security processes.

Table 14 - ***Human Resource Security capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Human Resource Security focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

Human resource security should be covered by the smaller SMEs. In practice however, most organizations have no or an ad hoc way of handling human resource security.

On average an organization with 0-10 NoE reside on capability B and 10-50 reside on capability C. However, it is possible for an organization to reach full maturity in this focus area if it is the ambition of the organization.

The sector of an organization demands whether or not it is necessary to implement a screening process before hiring an employee. One sector might demand for every employee to fill in a certificate of conduct (Dutch: “verklaring omtrent gedrag”) because of the sensitive information that is used within that field, while it is not demanded in another sector.

Next to that, sectors that handle sensitive information will have a larger list of requirements when focusing on human resource security. These organizations are more experienced and are therefore able to reach higher maturity in this focus area.

5.3.5 Effects on Compliance

Compliance focuses on the identification of the obligations towards external authorities. It includes intellectual property, business records, and cryptography. The following table shows the capabilities of the focus area.

Compliance	Capability description
A	• The organization complies with the applicable laws and regulations; • Management complies with the organization's policy.
B	• Employees are aware of their roles and responsibilities; • Formal writing style information security policies.
C	• The organization complies with/is certified based on applicable standards; • Employees comply with the policies of the organization; • Employees are timely informed about changes in the policies.

Table 15 - ***Compliance capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Compliance focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

In general, organizations do not focus on this focus area. SMEs do not know much about the legislations. Compliance is not really practiced in the Netherlands or Europe as opposed to the USA. However, the level of compliance as practiced in the USA will eventually be the same in the European countries.

In practice, unless organizations are going to get a certificate, each organization can be found on capability A. However, an organization with a larger revenue will be able to hire a legal advisor in order to help the organization with the compliance requirements.

The focus area is very depended on the sector. However, the current capabilities have been formulated in a generic way and are therefore not affected by the sector.

5.3.6 Effects on Identity and Access Management

Identity and access management focuses on the identification of users and defining their access to information in order to keep track of the users that have access to sensitive information. According to ISO, "the allocation of access rights to users should be controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights". The following table shows the capabilities of the focus area.

Identity and Access Management (IAM)	Capability description
A	• Formal IAM policy; • Ad hoc user management; • Individuals take responsibility for IAM; • IT-oriented IAM that does not support the business.

B	• Logging of access of applications and buildings; • Formal IAM program and process; • IAM policy contains a password policy which is business unit oriented; • Roles and responsibilities related to IAM are defined.
C	• Vision and strategy of the organization is supported in the IAM policy; • Periodic processing of user management; • IAM policy contains password policy; • Senior management is responsible for IAM; • Logging and periodically review of access of applications and buildings.
D	• IAM policy contains advanced password policy defined per system/role; • IAM improves the business and generates new opportunities; • Periodic review and update of IAM policy and processes; • User management is a continuous process supported by an IT system.

Table 16 - ***Identity and Access Management capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Identity and Access Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

The Identity and Access Management focus area is a topic that is being neglected by the organizations. Most of the time, identity and access management is done by the help desk or IT department.

In practice, identity and access management is not applicable for SMEs smaller than 5 NoE. However, there is no difference between the SMEs. As stated by an expert: *"An organization with two employees will have a policy that can be written on one page, either employee A or employee B will have access to assets. An organization with 238 employees will have a policy that can be more than ten pages. In both cases the organization has a formal identity and access management policy."*

On the revenue characteristic, identity and access management is a costly project which requires heavy investment.

The sector of an organization has no effect on the capabilities of the Identity and Access Management focus area, although sectors that handle sensitive information will have a larger list of requirements when focusing on identity and access management. It is for example demanded in the financial and health sector to have an authorization policy stating the profiles that have access to confidential information. Next to that, logging and periodically review of access of applications and buildings (capability C) in these sectors are required due to the sensitive information that is being used, processed or stored.

5.3.7 Effects on Secure Software Development

Secure software development is the technical part of information security that entails the operational IT procedures and responsibilities, the security of system files, the security in development and support processes, and eventually the technical vulnerability management. The following table shows the capabilities of the focus area.

Secure Software Development	**Capability description**
A	• Formal System Development Lifecycle consisting at least of: requirements gathering, development, testing, and migrating to production. • Formal system development policy; • Separate development, testing and production environments.
B	• Formal deployment plan for migrating changes or new systems to production; • Identified roles and responsibilities throughout the System Development Lifecycle; • Business requirements are based on standards, policies, and procedures; • Identifying risks for every project.
C	• Test results are documented; • Quality review is done as one of the last steps of the System Development Lifecycle; • Trained staff in using the System Development Lifecycle; • Formal sign off procedure at the end of every phase of the System Development Lifecycle.
D	• A post implementation review is done on every change or new system; • Quality review is a continuous process in the System Development Lifecycle; • Business requirements are reviewed at each step of the System Development Lifecycle.

Table 17 - ***Secure Software Development capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Secure Software Development focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

In order to see the effects of organizational characteristics on the Secure Software Development focus area, establishing whether developing software is the organization’s core business is the first step. If developing software is not the core business of an organization the Secure Software Development focus area would not be applicable for that organization. In practice, most SMEs with a core business of developing software will be placed at capability A.

A lot is been written in literature on this subject, however, it is not being done in practice. There are a handful of organizations that develop software in a secure way. These organizations mainly reside in the health sector. Developers often need to choose between developing secure software or deliver functionality as fast as possible.

It should be noted that when an organization develops software for a client, the sector of that client is affecting the development of secure software.

5.3.8 Effects on Incident Management

According to the definition list of ISO 27000, information security incidents can occur during an information security event. An information security event is "a system, service, or network state, condition, or occurrence that indicates that information security may have been breached or compromised or that a security policy may have been violated or a control may have failed." In the list of definitions, an information security incident is "made up of one or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair business operations." The information security incidents should be management in order to prevent the incidents from happening again. This can be done by means of a set of processes, which include "a detection process, a reporting process, an assessment process, a response process, and a learning process." The following table shows the capabilities of the focus area.

Incident Management	**Capability description**
A	• Formally defined Incident Management policy and process; • Formal process in order to assess and classify systems based on the critical level.
B	• Formal Incident Management process implemented; • Defined roles and responsibilities in order to respond to incidents.
C	• Audit trail of the system to trace back the incident; • Incident Management process is tested using a walkthrough in order to validate the process; • Incident Management is supported by tooling.
D	• Incidents are documented and logged; • Learning from previous incidents and act accordingly; • Incident Management process is periodically tested for operational effectiveness.

Table 18 - *Incident Management capabilities (Spruit & Roeling, 2014)*

With the above stated capabilities of the Incident Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

Most of the SMEs do not recognize information security incidents as actual incidents. Next to that, it is difficult for the smaller SMEs to do incident management in a formal way. There has to be enough capacity in order to handle incident management formally. However, incident management is easier for the smaller SMEs as opposed to larger SMEs, because the larger SMEs have a more complex incident management program.

In practice, SMEs with 0-10 and 10-50 NoE are placed at the first capability. SMEs with 50-250 NoE are mostly found on capability B. Most of the time this is due to the fact that there is no formal plan as stated in capability B.

The larger SMEs are able to afford more and will therefore have a more advanced system in place to handle incidents, where smaller SMEs will have to do with a basic system. However, the main idea of handling incident management remains the same.

5.3.9 Effects on Business Continuity Management

According to the ISO22301 – Business Continuity Management Systems, business continuity management is used in order to "ensure that operations continue and that products and services are delivered at predefined levels, that brands and value-creating activities are protected, and that the reputations and interests of key stakeholders are safeguarded whenever disruptive incidents occur. This is achieved by identifying potential threats, by analyzing possible impacts, and by taking steps to build organizational resilience." The following table shows the capabilities of the focus area.

Business Continuity Management (BCM)	Capability description
A	• BCM is performed by IT; • Senior management is responsible for BCM; • Formally defined BCM policy.
B	• Defined roles and responsibilities regarding BCM; • BCM process is performed; • Regularly performed Business Impact Analysis.
C	• Formal Business Continuity Plan is designed; • BCM process and procedures are based on available standards; • Testing Business Continuity Plan by performing a walkthrough test.
D	• Regular testing of Business Continuity Plan by simulating real events; • Internal testing of BCM; • Formally implemented Business Continuity Plan.
E	• Regular review by third party and update of Business Continuity Plan; • Regular review and update of BCM policy.

Table 19 - ***Business Continuity Management capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Business Continuity Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

In practice, a growing number of organizations focus on this focus area. Especially technical organizations focus on business continuity management and are mostly done in an informal way. Small SMEs often do not test their evacuation and communication plan in order to keep their availability and most of the time, they just talk about it during their coffee break.

As previous focus areas, business continuity management is easier for the smaller SMEs. The larger SMEs have a more complex business continuity management program. However, most of the time there is no formal plan as stated in capability C.

A larger revenue of an organization makes it possible to invest more in business continuity. As stated by an expert: *"organizations with the resources will have an ad hoc mirror environment in order to back-up their data. Organizations that do not have the resources will store their data on a USB-stick, which is updated every month. Both organizations have a design for a business continuity plan. Testing the USB-stick business continuity plan is much easier than to test an ad hoc mirror environment."*

The sector of an organization determines the level of business continuity that is necessary. Some sectors work with sensitive information and require a very complex back-up solution. In such cases, the business continuity plan and therefore the business continuity management can become complex as well. Especially the financial and health sector need a strict business continuity program, because of the data that needs to stay available.

5.3.10 Effects on Change Management

Change management should be implemented in order to control changes to all critical information resources of the organization, such as hardware, software, system documentation and operating procedures. Without change management, it is possible that critical assets are exposed to unforeseen vulnerabilities. The following table shows the capabilities of the focus area.

Change Management	**Capability description**
A	• Management awareness of the importance of Change Management; • Change Management is used in large projects; • Change Management is used to react on negative events.
B	• Formally defined roles and responsibilities regarding Change Management; • Change Management is used in all projects; • Structured Change Management process.
C	• Formally designed Change Management procedure; • Change Management is standardized and changes are documented; • Change Management is used to track mutations of the IT environment; • Senior Management is responsible for Change Management.
D	• Change Management as an organization wide integrated process; • Formally implemented Change Management procedure; • Change Management procedure is supported by information systems; • Emergency change procedures are part of Change Management.

Table 20 - ***Change Management capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Change Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

In practice, almost every organization does change management, but on an ad hoc base. Change management is difficult for the smaller SMEs to do in a formal way. There has to be enough capacity in order to handle change management in a formal way. When incident management is not correctly implemented, it will have its effect on change management as well. Change management can be done a lot faster at smaller organizations, because the communication lines are a lot tighter.

Organizations with 0-10 and 10-50 NoE reach capability B. Organizations with 50-250 NoE reach capability C.

5.3.11 Effects on Physical and Environmental Security

Physical and environmental security is a perfect example of information security no longer focusing on technical aspect alone. The focus area focuses on the building and perimeter of organizations and considers risks such as fires, floods, earthquakes, bombs, etc. Defining which rooms do not allow unauthorized access should be included in the policy as well. The following table shows the capabilities of the focus area.

Physical and Environmental Security	**Capability description**
A	• Formally defined Physical and Environmental Security policy; • Limited access to key facilities.
B	• Defined roles and responsibilities regarding Physical and Environmental Security; • Use of multiple security zones; • Key facilities are protected from theft; • Logging of access to key facilities.
C	• IT assets with business information are stored in secure areas; • Monitoring of access to key facilities; • Measures to sustain Physical and Environmental Security are regularly tested and audited; • Employees receive training in preventing physical breaches.
D	• Periodically reviewing and updating Physical and Environmental Security policies and procedures; • All facilities are protected from theft and weather.

Table 21 - ***Physical and Environmental Security capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Physical and Environmental Security focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings
As stated by an expert: *"organizations with the necessary resources are able to buy a secure room that is locked with identity cards and is monitored with a motion detector in order to secure their assets. Organizations that do not have the resources will store their assets in a vault in a room that can be locked with regular keys. Both organizations fulfill the same capability requirement of having multiple security zones."*

In practice, SMEs with 0-10 and 10-50 NoE reach capability B, while organizations with 50-250 reach capability C.

Physical and environmental security is applicable for every organization. However, having the means to physically protect an organization is important in this focus area. As previous focus areas, the revenue of an organization determines how much can be spend on physical and environmental security.

5.3.12 Effects on Asset Management

Managing the assets of an organization, such as hardware, software, but also information, is important in order to keep track of critical assets. Without it, critical assets can become missing more easily. It is the responsibility of the owner of the asset to keep the asset safe. The following table shows the capabilities of the focus area.

Asset Management	Capability description
A	• Management awareness of the importance of Asset Management; • Senior management is responsible for Asset Management.
B	• Formal Asset Management policy taken into account the phases of the asset management lifecycle; • Defined roles and responsibilities regarding Asset Management; • Asset inventory is established including status, connectivity, classification, and proximity.
C	• All assets have been assigned to an owner; • All stakeholders are familiar with the procedures of Asset Management; • Asset inventory is updated periodically; • Safe disposal, handled, processed, stored in line with the classification.
D	• Periodic reviewing of Asset Management policies; • Continuous review and update of the Asset Management process; • Asset Management is supported by a system; • Classification is based on the asset's lifecycle.

Table 22 - ***Asset Management capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Asset Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

Asset management is applicable for every organization and is a focus area that is covered by the IT department. However, only a few organizations have an actual up-to-date asset management.

In practice, most organizations can be found on capability B. An SME does not need more in the Asset Management focus area.

Organizations with a larger revenue and therefore having more assets will have a more complex asset management program than the organization with a smaller revenue.

5.3.13 Effects on Architecture

According to Spruit and Roeling (2014), the Architecture focus area addresses the construction and design of computers, communication networks and the distributed business systems that are implemented for information security technologies. The aim of information security architecture is to increase the effectiveness with which these computers, networks, etc. are implemented. The following table shows the capabilities of the focus area.

Architecture	Capability description
A	• At least one employee is responsible for the architecture, although that employee might not be familiar with security.
B	• Formal information security architect role; • Formal policy regarding information security architecture; • IT security and the usage of hardware and software to protect sensitive data have been put in a defense-in-depth concept.
C	• Architectural development is based on a standard; • The effectiveness of the architecture are monitored; • Implemented defense-in-depth concept;

	• Regular audit/penetration test in order to test the architecture.
D	• Business is supported by the architecture; • Continuous update of architecture; • Building blocks are used to set up the architecture.

Table 23 - ***Architecture capabilities (Spruit & Roeling, 2014)***

With the above stated capabilities of the Architecture focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

Most of the organizations focus on the architecture in some way, but it is mainly done informally by the information security officer.

In practice, most organizations can be found on capability A. For SMEs smaller than 50 NoE, focusing on the architecture seems like an overkill. It is important to determine the risks, which can be done by mapping the information flows. In practice, the larger organizations will write these information flows down.

5.3.14 Effects on Supply Chain Management

Supply chain management is the management in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer. The following table shows the capabilities of the focus area.

Supply Chain Management	Capability description
A	• Informal supply chain management policy; • Low monitoring of information flowing through the supply chain; • Low awareness and knowledge of risks; • Low support for supply chain management.
B	• Strategically defined supply chain risk management; • Monitoring of information flow; • Growing awareness and knowledge of risks in the supply chain; • Proactive management support for supply chain management.
C	• Investment in selecting and maintaining collaborative relationship of supply chain participants; • Knowledge of risks and risks are shared with participants in the supply chain; • Formalized Supply Chain Management.
D	• Maintaining awareness of risks in the supply chain; • Formalized Supply Chain Management is shared with participants in the supply chain; • Continual risk analysis; • Continual risk assessments.

Table 24 - ***Supply Chain Management capabilities***

With the above stated capabilities of the Supply Chain Management focus area, expert interviews were conducted in order to study the effect of organizational characteristics on this particular focus area.

Expert findings

Supply Chain Management is getting more important because of the specialization of organizations. The number of third party organizations that process data is growing. The need for supply chain management or supplier management is therefore growing as well. The Supply Chain Management focus area is especially important for SMEs. Due to the limited resources, the smaller organizations are largely dependent on third parties and should therefore strive for the highest possible maturity level. SMEs need to know what assets come from third parties as they are risks for their own business. Every aspect of the supplier needs to be written down and signed in a contract.

In practice however, most of the organizations reach capability A, even though supply chain management is an important subject.

5.4 Effects of Organizational Characteristics Analysis

The following analysis is done based on the findings of the interviews with the information security experts.

5.4.1 Reaching Maturity

In practice, most SMEs can be found at the first two capability levels of the information security focus area maturity model. However, that does not mean these organizations are not able to reach full maturity. Whenever it is the SME's ambition or goal to reach full maturity in order to get a stronger market position by presenting themselves as being a serious protector of information, or whenever it is demanded by the clients of the SME, they are able to. This can be seen in the case study results, where SMEs are able to reach the highest levels. Omitting the highest maturity levels is therefore not possible.

5.4.2 Additional Organizational Characteristics

During the expert interviews, it became clear that other organizational characteristics have an effect on the information security as well and should therefore be considered in the maturity model.

First, information security is subjected to the *national or international business orientation of the organization*. International organizations are bound to the legislations of the country in which they operate. For example, the Health Insurance Portability and Accountability Act (HIPAA) of the USA enforces organizations in the health sector to work with a different spectrum of information security controls in order to mitigate risks that could harm medical information. Organizations only working in the health sector in Europe do not have to work according to the HIPAA.

Next to that, according to Mijnhardt et al. (In Press), the sector in which the organization is operating is an organizational characteristic that affects the information security. However, according to the experts, the *information security framework* which is chosen by the organization has an even bigger effect. For example, for the financial sector different frameworks like Sarbanes-Oxley act (SOx), COBIT, and PCIDS exist. Although each of these frameworks focuses on the information security aspect, they do so in different ways, with different controls. An organization that works according to SOx will have their focus on other information security controls than an organization working with the COBIT framework even though both organizations work in the financial sector.

5.4.3 Generic Capabilities

According to the interviewed information security experts, the improvement actions, in order to reach the capabilities that are stated in the information security maturity matrix, have been set up in a generic way and showed no differences between organizations with different organizational characteristics. According to the experts, this is not strange because the capabilities have been defined based on the ISO framework. The ISO framework is one of most widely used information security frameworks which is applicable for every organization. Defining the improvement actions of the capabilities based on the information security standard can lead to capabilities that are applicable for every organization as well. Although the organizations are different from one another, the fundamental principle of the defined capabilities remains the same. According to the information security experts, multiple examples explain this statement. One of these examples to emphasize the statement: "*Focus area Identity and Access Management, capability A, 'The organization has a formal IAM policy in place'; an organization with two employees will have a policy that can be written* *on one page, either employee A or employee B will have access to assets. An organization with 238 employees will have a policy that can be more than ten pages. In both cases the organization has a formal IAM policy."* As can be seen, both organizations will be able to reach the capability and show not much of a difference.

Another example can be seen in the Policy focus area, stating: "Laws and regulations are part of the information security policy." Although each sector has different laws and regulations, the current definition of the improvement action makes the capability applicable for organizations with different organizational characteristics.

The given examples of generically defined improvement actions are backed up by the fact that the ISFAM model has been successfully evaluated at multiple SMEs of different organizational profiles, which suggests that the ISFAM model is indeed applicable for different kinds of SMEs.

5.4.4 Discrepancy in Results

As explained, the interviewed information security experts in this research concluded, based on their experience, that there is no real effect in the capabilities of the ISFAM model between SMEs with different organizational characteristics. Next to that, the model proved to be working for multiple cases of different profiles. However, it is impossible to ignore the extensive literature study of organizational characteristics affecting the information security model (Mijnhardt et al., In Press), backed up by the statistical analysis done by Baars et al. (2014), the existence of sector specific information security standards (Esra & Soysal, 2012; ISO27002:2013), and multiple information security maturity models considering organizational characteristics (Sanchez et al., 2007; Cholez & Girard, 2014).

In order to understand the different results, a discussion with the researchers of Baars et al. (2014) was initiated. According to the researchers, the difference in scope is a possible explanation for the discrepancy in results. As stated by the researchers: *"We researched the effect of organizational characteristics on the focus area level and reported those results. I do not know what happens on the capability level."* While the researchers of Baars et al. (2014) focused on the focus area level of the ISFAM model, this research focused on the capability level of the model as defined by Spruit and Roeling (2014). The improvement actions, in order to reach the capabilities, have been created in a very generic way, but were not taken into account in the previous research.

The information security focus area maturity model (Spruit & Roeling, 2014) is indeed applicable for different organizations, but it is also possible that the model is oversimplifying reality and is too simplistic as is often is the case with maturity models (Bollinger & McGowan, 1991). In order to overcome developing simplistic maturity models, it is necessary to consider the organizational characteristics. This has been done in other information security maturity models (Sanchez et al., 2007; Cholez and Girard, 2014) and should be done in focus area maturity models, such as ISFAM, as well. A fragment considering the organization's characteristics needs to be added to the design of focus area maturity models. In the design of focus area maturity models (Steenbergen et al., 2010), a model should be scoped following the domain, such as information security, for which the model is designed in order to decide what should be included or excluded and making it a useful model. Next to the identification of the functional domain, a fragment considering the organization's characteristics needs to be added as can be seen in the following figure.

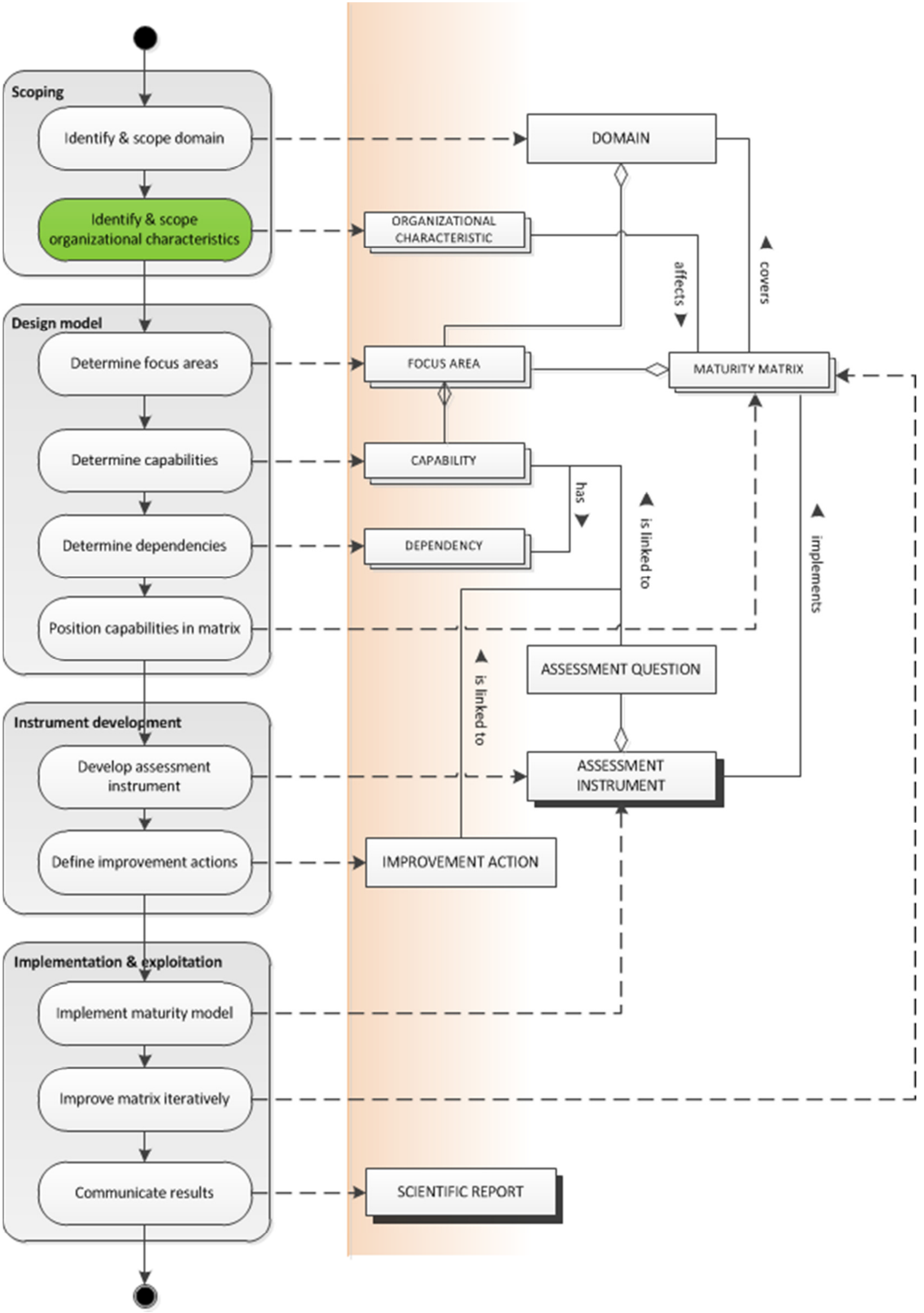


Figure 17 - ***PDD of the design of focus area maturity models (Steenbergen et al., 2010) with additional method fragment to consider organizational characteristics***

This page intentionally left blank

6 Rule-based Focus Area Maturity Model

This section covers the focus area maturity model in combination with the rule-based approach. The combination has been put together as a prototype application for the information security domain in order to identify the applicability of the rule-based approach.

6.1 Rule-based Engines

Rule-based engines are applications in which rules can be created and managed. The following shows a short list of some open source rule-based engines (Java Source, 2014):

- Drools;
- OpenRules;
- JRuleEngine;
- Zilonis;
- DTRules;
- OpenL Tablets;
- Roolie.

Based on the advice of a rule-based approach expert, the prototype application is created using the rule-based system Drools, because of the large community behind the system. Drools is an advanced open source business rule management system (BRMS) created by Red Hat and allows the user to develop applications where rules can be used to solve problems (Browne, 2009).

6.2 Prototype in Drools

The base and core of the prototype application is written in Java due to its platform independent nature and is created using the client-server architecture. This allows an easier access from any place and any time. Next to that, the prototype follows the same rule-based architecture, comprising the knowledge base, inference engine and user interface, as described earlier. The knowledge base and the inference engine of the rule-base architecture are found on the server side, while the user interface resides on the client side. The knowledge base and the user interface will be discussed next. The inference engine is not included because this component is part of the Drools system itself.

6.2.1 Fact Memory in the Knowledge Base

Initially, the server, on which the prototype application runs, creates an array which consists of the focus area objects of the information security domain with references to their capability objects (Figure 18). Ideally, the focus areas and capabilities should be placed in a database forming the facts of the knowledge base, but for simplicity reasons they are hardcoded in the prototype. Each capability within the array has a “Name” (A, B, C, D, or E), a “MaturityLevel” (1-12), and an “Achieved” value (true or false to indicate whether the capability has been reached).

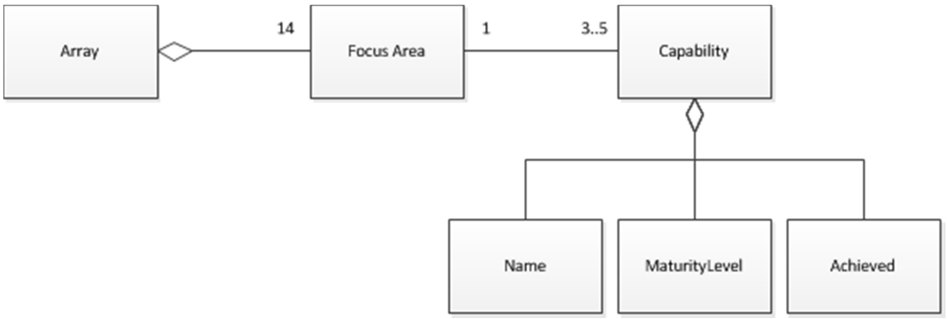


Figure 18 - ***The array of focus areas that is used in the prototype application***

For this prototype, the array has been filled with the 14 focus areas and their capabilities of the information security domain as stated in the ISFAM model. The output has been corrected to the JSON standard, as the array needs to be sent to the HTML pages on the client-side. The output of the array, written in JSON syntax, will look as follows.

```
Array [
        Risk Management [
                {Name:          A,
                MaturityLevel:  3,
                Achieved:       false.},
                {Name:          B,
                MaturityLevel:  5,
                Achieved:       false.},
                Etc.
        ],
        Policy Development [
        ],
        Etc.
]
```

The default values of the capabilities are derived from the initial ISFAM model, but can be changed based on predefined rules, as will be explained in the next section. When all rules have been fired, the server sends the array of focus areas and capabilities as a JSON string, as shown above, to the HTML pages on the client-side. The client will generate the model in HTML using JavaScript.

6.2.2 Rules in the Knowledge Base

All the rules are placed in a specific file forming the knowledge base of the prototype application. As explained in the literature study, the condition of the rule is written in the Left Hand Side, while the action is written in the Right Hand Side. The rules in Drools need to be written following the syntax:

```
Rule    "Name"
   When
        Left Hand Side;
   Then
        Right Hand Side;
End
```

The rules can be defined for specific purposes. The first one is to assess whether the capability's improvement actions have been met, similar to the prototype as described in the study of Tae-Nyeon and Hovav. An example rule for changing a capability to "achieved":

```
Rule    "Change RMA to achieved"
   When
        RMA1 == 1 && RMA2 == 1 && RMA3 == 1;
        //this line will check whether the capability's improvement actions, in this case the
        actions for capability A of the Risk Management focus area (RMA1-3), filled out in the
        assessment have been met.
   Then
        changeAchieved("Risk Management", "A", true);
        //this line will call upon the changeAchieved() function. The function will crawl
        through the array of focus areas and changes the "achieved" value of capability A of
        the Risk Management focus area to true.
End
```

As explained, due to the intra-process dependencies of a focus area maturity model, capability B can only be reached when capability A of a focus area has been completed. The rule to change capability B to "achieved" will therefore have an additional Left Hand Side argument to check the conclusion of the rule of the previous capability.

```
Rule    "Change RMB to achieved"
   When
        RMA == true && RMB1 == 1 && RMB2 == 1 && RMB3 == 1 && RMB4 == 1;
   Then
        changeAchieved("Risk Management", "B", true);
End
```

The rules for capability C and D of the Risk Management focus area are followed in a similar way, checking the conclusion of the capabilities before them. This shows the forward chaining architecture of the rule-based approach. This type of rule has been used for all the focus areas, because checking the capabilities as "achieved" is done the same in the entire model. Therefore, only the "achieved" rules for the risk management focus area have been put in the appendices.

The second type of rule is the rule for changing the maturity levels of the capabilities in order to change the inter-process dependencies (capabilities with dependent on capabilities in other focus areas) of the model. The dependencies in the focus area maturity model are defined by the maturity level of the capabilities. As an example, capability A of focus area Policy Development, which is at maturity level 2, should be reached only when capability A of focus area Organizing Information Security, which is at maturity level 1, has been met. A rule in order to deal with the inter-process dependencies will look as follows:

```
Rule    “OISA dependency PDA”
   When
        getMaturityLevel(“OIS”, “A”) !< getMaturityLevel(“PD”, “A”);
        //this line will check if the maturity level of capability A of focus area Organizing
        Information Security is smaller than capability A of focus area Policy Development.
   Then
        changeMaturityLevel(“PD”, “A”, getMaturityLevel(“OIS”, “A”)+1);
        //this line will call upon the changeMaturityLevel() function. The function will crawl
        through the array of focus areas and changes the “maturity level” value of capability
        A of the Policy Development focus area to a higher level maturity level than that of
        capability A of the Organizing Information Security focus area.
End
```

Although this is a valid way to use rules in order to change the inter-process dependencies, it is better to change the maturity level in the base array rather than to create rules to change the dependencies every time the model is generated, which makes the application unnecessary slower.

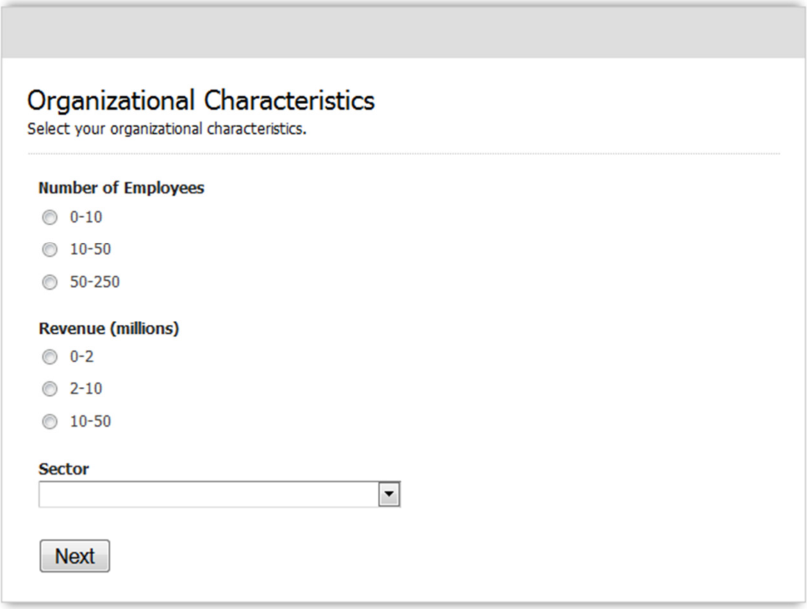
Due to the fact that no effects of the organizational characteristics have been found, the rules in order to change the model based on organizational characteristics cannot be defined. However, it is possible that future research will find effects by, for example, researching the other organizational characteristics than studied in this research or by redefining the capabilities of information security for each organizational profile. Next to that, focus area maturity models in other domains are able to use this kind of rule. For these reasons, a fictive rule has been created in order to understand how the rule-based approach can be used to change the entire order of the focus area maturity model for different organizational profiles. An example of a fictive rule for changing the maturity level will look as follows:

```
Rule    “Change maturity levels for health”
   When
        OrganizationalCharacteristics.getSector().equals(“Health”);
        //this line will check whether the selected sector is the same as “Health”.
   Then
        changeMaturityLevel(“RM”, “A”, 2);
        //this line will change the maturity level of a capability to the defined maturity level.
        removeCapability(“RM”, “D”);
        //this line will remove capability D from the Risk Management focus area.
End
```

From the main file, all the rules that are defined in the knowledge base are triggered using the function fireAllRules(). When all the rules have been fired, the rules that have a positive Left Hand Side will be carried out. The focus area maturity model is changed based on the input the prototype application has gotten. Next, the array on the server side is sent to the client side, where it will be shown in the interface. Following these steps, the rules can change or complete remove the focus areas, capabilities, and dependencies of the maturity model.

6.2.3 Interface

The interface of the application prototype runs on the client side and shows three views in HTML: selection of organizational characteristics, the assessment, and the model. These views are explained next. The first step is the selection of organizational characteristics (Figure 19). The organizational characteristics that have been researched, number of employees, revenue, and sector, are shown. The values defined by Mijnhardt et al. (In Press) have been used. Not selecting organizational characteristics will lead to the basic ISFAM model. It is possible for future research to expand this step with additional organizational characteristics.



Organizational Characteristics

Select your organizational characteristics.

Number of Employees

○ 0-10

○ 10-50

○ 50-250

Revenue (millions)

○ 0-2

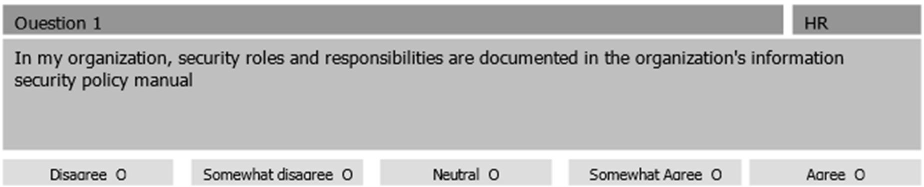
○ 2-10

○ 10-50

Sector

Figure 19 - ***Selection of organizational characteristics***

The next step is the assessment. Users are able to do the assessment in order to see the achievement of their information security. In the rule-based prototype as described by Tae-Nyeon and Hovav, the following question (Figure 20) was used in the assessment. Although the assessment question is in line with controls in information security frameworks, it is confusing for the user to select the right option. From a design point of view, it is unclear when a policy is at level "somewhat disagree", "neutral" or "somewhat agree".



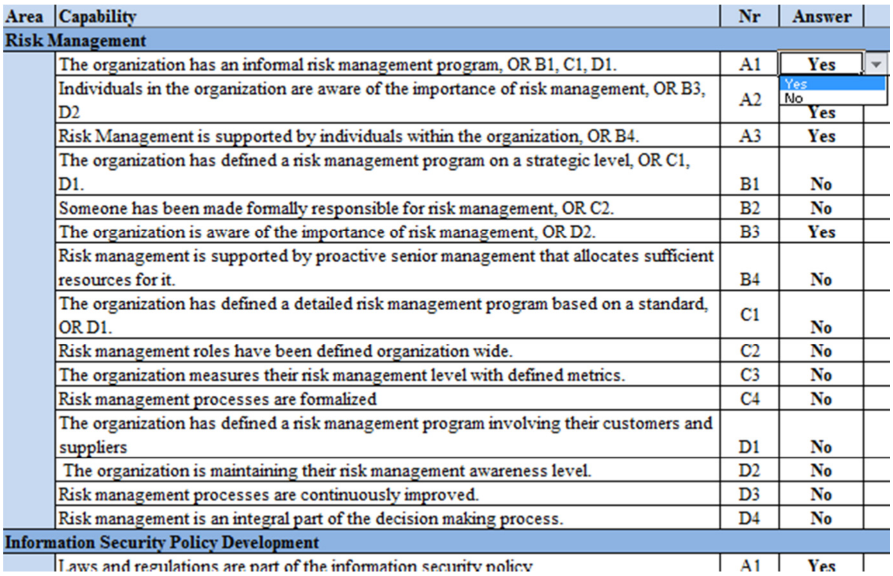
Question 1 HR

In my organization, security roles and responsibilities are documented in the organization's information security policy manual

Disagree ○ Somewhat disagree ○ Neutral ○ Somewhat Agree ○ Agree ○

Figure 20 - ***Rule-based assessment (Tae-Nyeon & Hovav)***

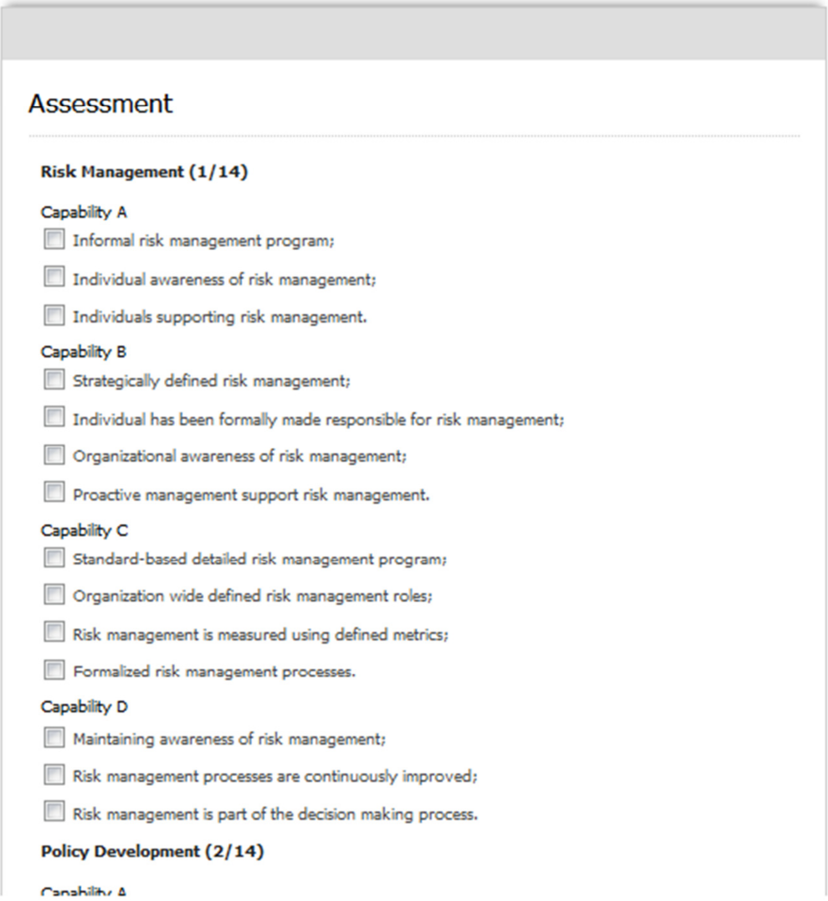
Looking at the assessment tool created in the ISFAM model (Spruit & Roeling, 2014), the user has to select the "Yes" option of a dropdown menu (Yes or No) in order to indicate whether the improvement action of the capability is reached, as shown in the following figure. The assessment of Spruit and Roeling is created in Excel where the result of the assessment is calculated in another view in Excel as well.



Area	Capability	Nr	Answer
Risk Management			
	The organization has an informal risk management program, OR B1, C1, D1.	A1	Yes
	Individuals in the organization are aware of the importance of risk management, OR B3, D2	A2	Yes
	Risk Management is supported by individuals within the organization, OR B4.	A3	Yes
	The organization has defined a risk management program on a strategic level, OR C1, D1.	B1	No
	Someone has been made formally responsible for risk management, OR C2.	B2	No
	The organization is aware of the importance of risk management, OR D2.	B3	Yes
	Risk management is supported by proactive senior management that allocates sufficient resources for it.	B4	No
	The organization has defined a detailed risk management program based on a standard, OR D1.	C1	No
	Risk management roles have been defined organization wide.	C2	No
	The organization measures their risk management level with defined metrics.	C3	No
	Risk management processes are formalized	C4	No
	The organization has defined a risk management program involving their customers and suppliers	D1	No
	The organization is maintaining their risk management awareness level.	D2	No
	Risk management processes are continuously improved.	D3	No
	Risk management is an integral part of the decision making process.	D4	No
Information Security Policy Development			
	Laws and regulations are part of the information security policy	A1	Yes

Figure 21 - ***ISFAM assessment (Spruit & Roeling, 2014)***

In the prototype of this research, as can be seen in the next figure, the user has to check a checkbox for the particular requirement of the capability. Not clicking twice (clicking the dropdown menu and clicking the "Yes" option) to check an improvement action (Spruit & Roeling, 2014) is an advantage of having a checkbox instead of a dropdown menu. Next to the usability improvement, the assessment with improvements actions has been updated according to the additional supply chain focus area as has been studied in this research.



Assessment

Risk Management (1/14)

Capability A

□ Informal risk management program;

□ Individual awareness of risk management;

□ Individuals supporting risk management.

Capability B

□ Strategically defined risk management;

□ Individual has been formally made responsible for risk management;

□ Organizational awareness of risk management;

□ Proactive management support risk management.

Capability C

□ Standard-based detailed risk management program;

□ Organization wide defined risk management roles;

□ Risk management is measured using defined metrics;

□ Formalized risk management processes.

Capability D

□ Maintaining awareness of risk management;

□ Risk management processes are continuously improved;

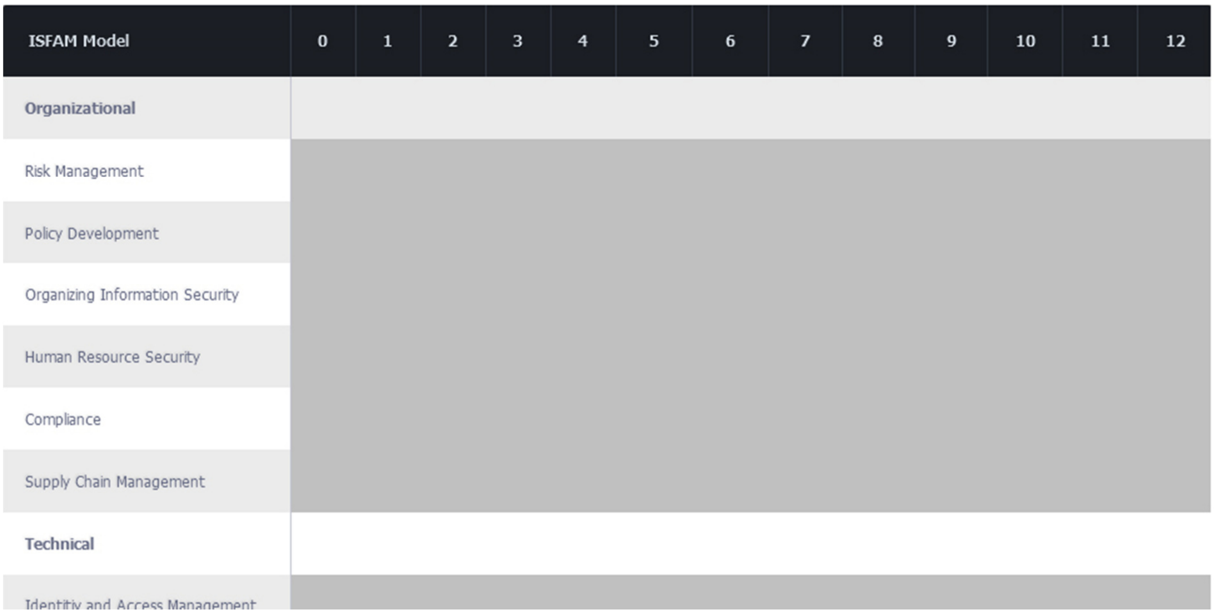
□ Risk management is part of the decision making process.

Policy Development (2/14)

Capability A

Figure 22 - ***The assessment***

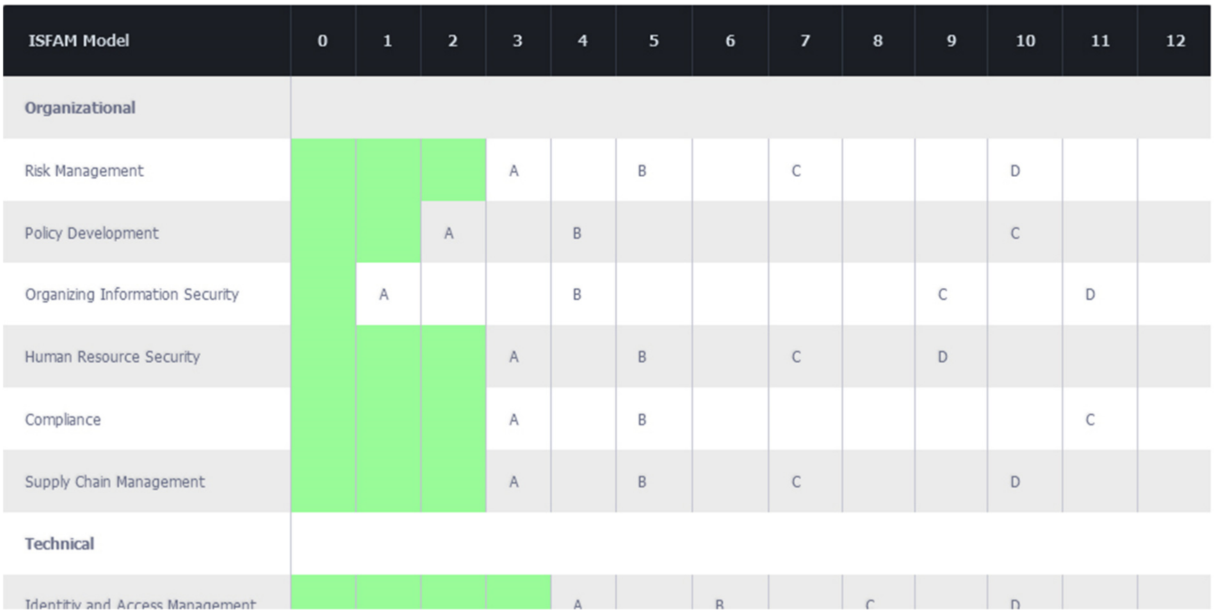
The last part of the interface is the model, showing the result based on the assessment. The capabilities are placed according to the array of focus areas and capabilities. Without the array of capabilities, the model will not generate the capabilities within the model as depicted in Figure 23.



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management													
Policy Development													
Organizing Information Security													
Human Resource Security													
Compliance													
Supply Chain Management													
Technical													
Identity and Access Management													

Figure 23 - ***ISFAM model without generated capabilities***

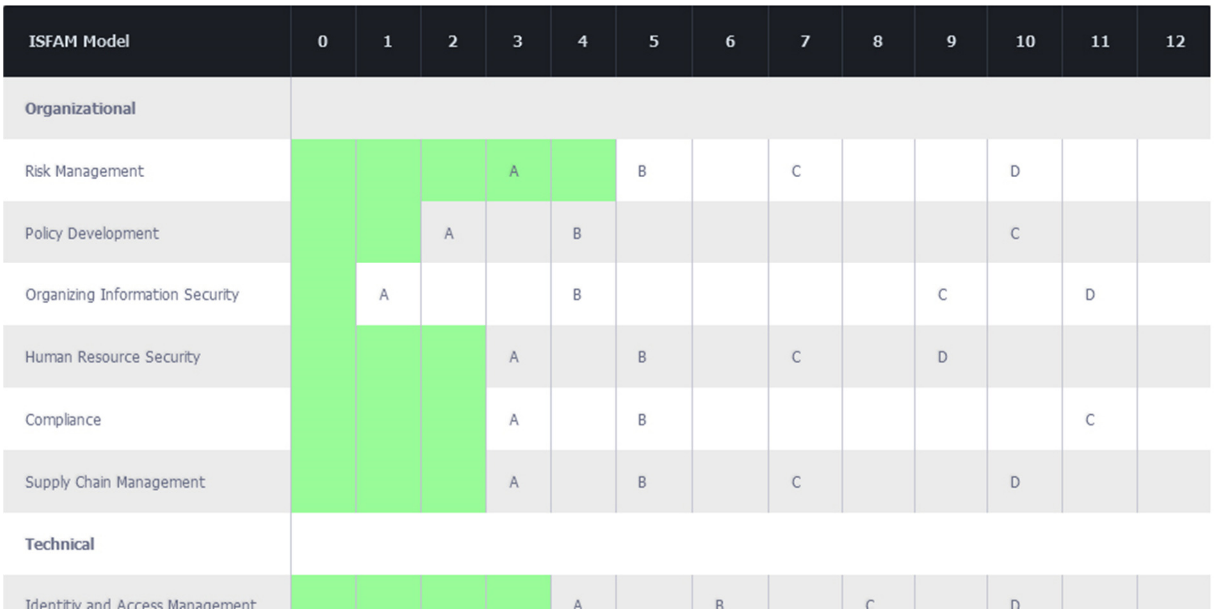
With the default capability values in the array of focus areas as defined in the initial ISFAM model and the additional Supply Chain Management focus area, the client will generate the model in HTML using JavaScript (Figure 24).



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management	🟩	🟩	🟩	A		B		C			D		
Policy Development	🟩	🟩	A		B						C		
Organizing Information Security	🟩	A			B					C		D	
Human Resource Security	🟩	🟩	🟩	A		B		C		D			
Compliance	🟩	🟩	🟩	A		B						C	
Supply Chain Management	🟩	🟩	🟩	A		B		C			D		
Technical													
Identity and Access Management	🟩	🟩	🟩	🟩	A		B		C		D		

Figure 24 - ***ISFAM model with generated capabilities as defined in the initial ISFAM model***

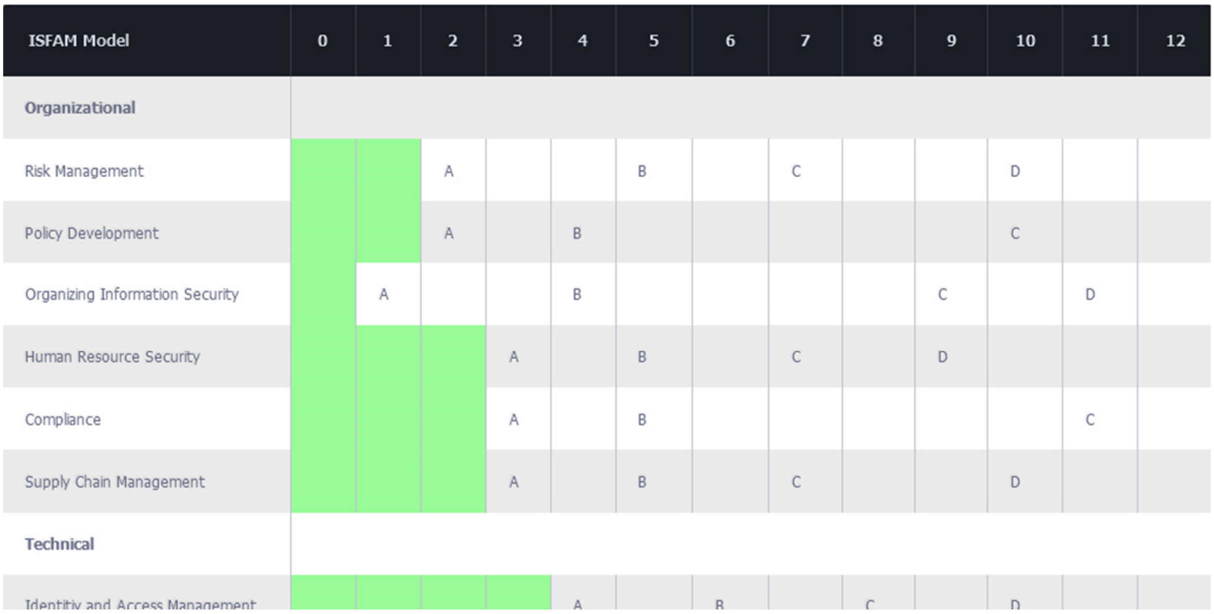
Following the defined rule, the capability background will turn green whenever a capability is reached. Figure 25 depicts capability A of the Risk Management focus area as achieved.



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management	🟩	🟩	🟩	🟩 A	🟩	B		C			D		
Policy Development	🟩	🟩	A		B						C		
Organizing Information Security	🟩	A			B					C		D	
Human Resource Security	🟩	🟩	🟩	A		B		C		D			
Compliance	🟩	🟩	🟩	A		B						C	
Supply Chain Management	🟩	🟩	🟩	A		B		C			D		
Technical													
Identity and Access Management	🟩	🟩	🟩	🟩	A		B		C		D		

Figure 25 - ***ISFAM model with the first capability of Risk Management reached***

As explained, based on the organizational characteristics given in the first view, it is possible to change the place of the capabilities in the matrix or even remove the capability using the defined rules. Figure 26 depicts the change of maturity level of capability A of the Risk Management focus area from level three to level two.



ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management	🟩	🟩	A			B		C			D		
Policy Development	🟩	🟩	A		B						C		
Organizing Information Security	🟩	A			B					C		D	
Human Resource Security	🟩	🟩	🟩	A		B		C		D			
Compliance	🟩	🟩	🟩	A		B						C	
Supply Chain Management	🟩	🟩	🟩	A		B		C			D		
Technical													
Identity and Access Management	🟩	🟩	🟩	🟩	A		B		C		D		

Figure 26 - ***ISFAM model with the change of maturity level of the first capability of Risk Management***

Next to the possibility to change the maturity level based on the organizational characteristics, it is possible to completely remove all dependencies. Although the dependencies give clear information of best practices on steps that need to be taken in order to mature towards a higher maturity level and therefore should be followed, organizations are able to choose not to follow the model, but rather follow their own priorities.

6.3 Extrapolate Prototype towards FAM Models

The development of the prototype artifact of this research proved that the rule-based approach can help an information security focus area maturity model in two ways: rules for changing a capability to "achieved" and rules for changing the focus areas, capabilities, and dependencies in the model based on the selected organizational characteristics. The prototype can be changed towards focus area maturity models in other domains, such as the enterprise architecture or the software product management domain (Steenbergen et al., 2010), as well. In order to change the prototype for a different domain, some parts in the prototype need to be changed. The model itself can be changed by altering the array of focus areas and capabilities for the selected domain, the assessment needs to be changed based on the determined capabilities, and the rules need to be defined for organizations with different organizational characteristics for that particular domain.

In order to apply the rule-based approach for FAM models, an optional method fragment in the design of focus area maturity models, the rule-based approach, needs to be added. Following the method fragment makes it possible for the designer of the focus area maturity model to rearrange the model based on the organizational characteristics, which makes it easy to change focus area maturity models to create a better fitting maturity model for different types of organizations. The first step in using the rule-based approach is filling the fact memory with facts: the organizational characteristics and the focus areas with its capabilities and dependencies. Next is defining the rules in the rule base that can actually change the maturity model based on the organizational characteristics in the fact memory. Last is the creation of the user interface. As can be seen in the prototype, the user interface should incorporate the organization characteristics, the assessment, and the maturity model itself. Following figure shows the method fragment needed for the implementation steps of the rule-based approach.

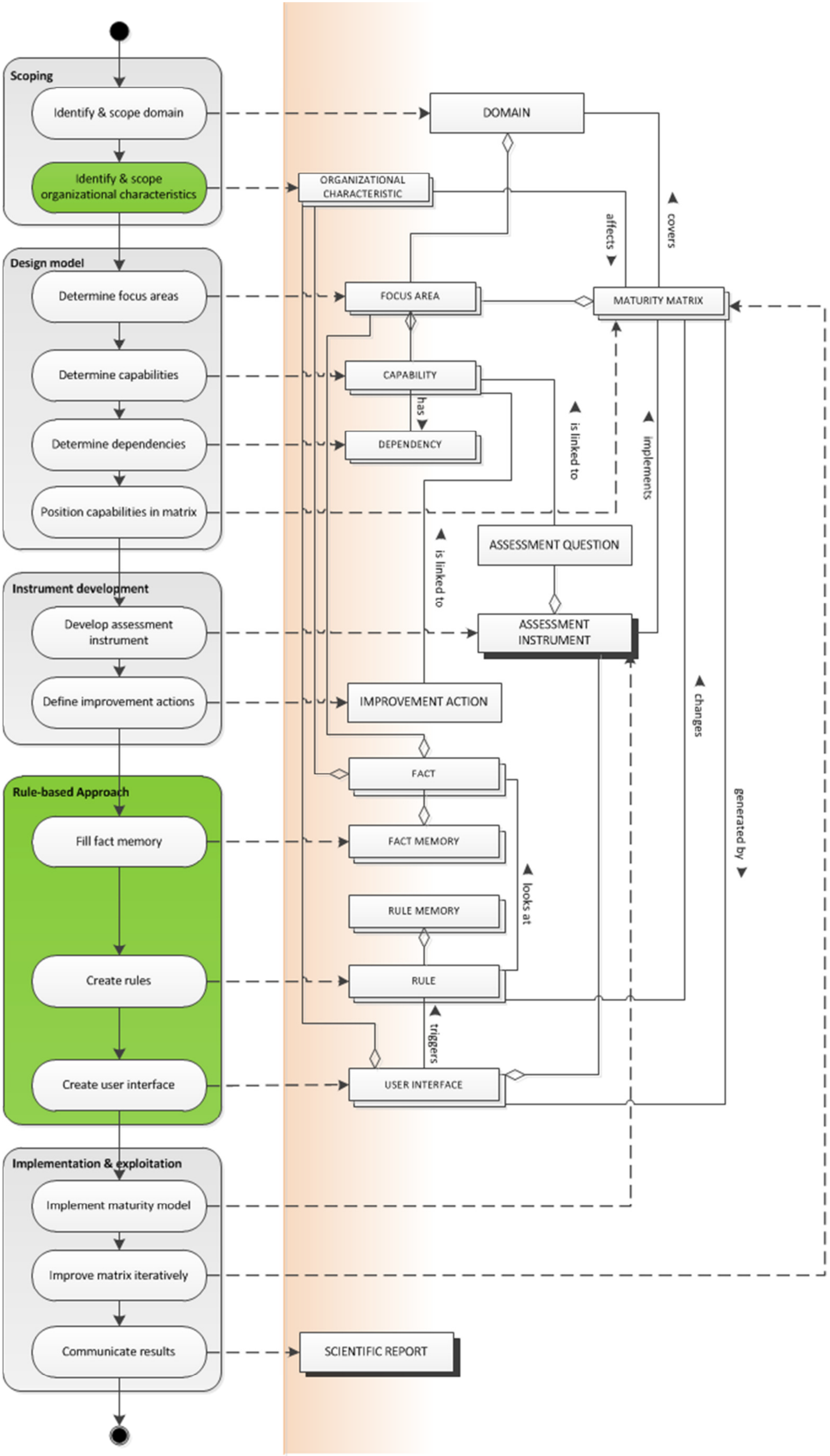


Figure 27 - ***PDD of the design of focus area maturity models (Steenbergen et al., 2010) with additional method fragments Organizational Characteristics and Rule-based Approach***

This page intentionally left blank

7 Conclusion, Discussion, and Future Research

This section presents the final conclusions, discusses the results of the research, and ends with topics for future research.

7.1 Conclusion

This research was set out to further develop the existing information security focus area maturity model in a rule-based system. The objectives of the research were to:

- Research and possibly update the ISFAM model based on current information security standards;
- Research the effect of the organizational characteristics affecting the ISFAM model;
- Research whether and in what way the rule-based approach can be used for an information security maturity model.

Based on the conducted research, the following conclusion can be made.

The ISFAM model has been updated with the found focus area Supply Chain Management. Based on literature research, the capabilities of the focus area were defined and evaluated by information security experts. According to the experts, this focus area is very valuable, especially to SMEs, because they are dependent on third parties due to the limited available resources. The updated ISFAM model was evaluated at the case organization and showed that the model is, next to the telecom, media and technology and the financial sector, applicable for an SME in the health sector as well.

Although this was not part of the research, the information security experts concluded that there are additional organizational characteristics affecting the information security maturity model, which should be added to the list of organizational characteristics of Mijnhardt et al. (In Press).The first organizational characteristics is the business scope of an organization. Due to the different legislation in different countries, it is important to know whether the organization works at a national or an international level. Different legislation leads to other information security requirements. The second organizational characteristic that influences the information security is the use of an information security framework. According to Mijnhardt et al. (In Press), the sector in which the organization is operating is an influencing organizational characteristic. However, the information security framework which is chosen by the organization has an even bigger effect. These two organizational characteristics need to be further researched as has been done with the other characteristics in order to understand how these characteristics affect the information security and the maturity of it.

As explained, no effects of organizational characteristics on the capability level of the information security model have been found. This is due to the fact that the capabilities were defined based on the ISO information security framework which is applicable for every organization. Defining the capabilities in such a way can lead to capabilities that are applicable for every organization as well. A discussion with the researcher of Baars et al. (In Press) showed that the difference in scope, focus area level versus capability level, might be the explanation of not finding the same effects (Baars et al., 2014) that were expected.

Not finding effects on the capability level of the model implies that the ISFAM model is applicable for organizations with different organizational characteristics. This is backed-up by the fact that the model has been successfully evaluated at different case organizations. However, it is also possible that the model is oversimplifying reality and is too simplistic. Adding an additional method fragment, identifying and scoping the organizational characteristics, to the design of focus area maturity models could diminish the chance of developing less fitting focus area maturity models. To verify the additional method fragment, the fragment needs to be tested first by, for example, developing a maturity model for a specific organizational profile.

The research presented the findings on the rule-based approach and how it can be implemented together with the information security focus area maturity model. Two ways of implementing rules for the maturity model were discussed: changing the capabilities to “achieved” and changing the model based on the inter-dependencies of the capabilities. Next to that, although it is possible to use the rule-based approach to change the model based on the organizational characteristics, as of now, the use of a rule-based approach is not implemented to the fullest, because the model does not need to be changed for different organizations as no effects were found. However, the prototype application is still valuable in a way that it gives insight on the possibilities of the rule-based approach in combination with the ISFAM model. The research sets a base for future research where the rule-based approach can be used for other focus area maturity models.

7.2 Discussion

There are some discussions points in this research that need some extra attention.

The first discussion point that needs to be addressed is that not all of the papers were found by means of the literature study. The most important papers, the paper about the organizational characteristics of Mijnhardt et al. (In Press) and the research by Baars et al. (2014), were not yet published at the time of the research. These papers were retrieved from the project supervisor. Next to that, the literature covering the body of knowledge for the rule-based approach was retrieved from a lecturer at the Utrecht University of Applied Sciences.

The second discussion point is the use of the Cloud Control Matrix (CCM). The CCM of the Cloud Security Alliance was not found by means of the literature study and according to the cloud security alliance the matrix focuses on the security in the cloud alone. It was however used in the research because of the extensive comparison of information security standards. As explained, the controls of the CCM did not only encompass security in the cloud, but also for example security of the physical facilities and was therefore used as a comparison against the focus areas of the original ISFAM model.

The next discussion point is the possibility of finding early indications of the generic capabilities of the ISFAM model. Following the steps of design of a focus area maturity model, and more specific the determination of the capabilities of the maturity model, could have shown the simplicity of the defined capabilities in the original ISFAM model. However, due to time constrains, only the capabilities of the additional focus area were determined. Next to that, the evaluation of the ISFAM model has been done at multiple case organizations with different organizational characteristics. This should have been an early indicator of the results of this research.

The evaluation of the additional focus area in the updated ISFAM model is another discussion point. The evaluation was done with the same information security experts as for the study of the effects of the organizational characteristics. These experts were used because of their extensive knowledge of information security. The same experts were used because it was less time consuming to evaluate the additional focus area and, at same time, question the effects of the organizational characteristics on the capabilities of the ISFAM model. Looking back, it might have been better to evaluate the additional focus area, supply chain security, with information security experts working in that particular domain.

Next, the first theme of organizational characteristics was selected as the scope of this research. Some organizational characteristics, like Percentage Hosting Services Outsourced and FTE Employed in the IT Department, affect the entire ISFAM model and showed more effect than others. It would have been better to study these organizational characteristics first. However, according to previous research, all the organizational characteristics affect the model and it was therefore expected that every organizational characteristic has an effect on the capability level as well. It was assumed that it did not matter which organizational characteristic was studied first. Starting with the first theme of organizational characteristics seemed the most logical step.

The research presented results based on five in-depth interviews with five different information security officers in order to validate the effects of organizational characteristics as identified by Mijnhardt et al. (In Press). During the interviews, it soon became clear that there were no effects of the organizational characteristics on the capability level of the ISFAM model because of the generically defined capabilities. Hearing the same results after each interview, each lasting two hours, it was decided not to continue with the interviews. Instead, a discussion with the researchers, who did find effects of organizational characteristics on the ISFAM model (Baars et al., 2014), was initiated in order to understand the differences in results.

The interview questions in order to find the effects of the organizational characteristics were set up and defined in the research method. However, during the interview with the information security experts, asking different questions could have led to a different result. Instead of asking “is there a difference between organization A in the range of 0-10 employees and organization B in the range of 50-250 employees for capability Z?”, asking “define capability Z for organization A, would capability Z be the same for organization B?” could result in a different outcome as the experts would have defined the capabilities themselves.

In a methodical discussion with the information security experts at the organization, finding the effects would indeed give an organization a more fitting and precise advice as opposed to the fixed ISFAM model. However, according to the information security experts, three points need to be taken into account.

- The first point can be seen when an organization uses the information security maturity model in order to assess the information security. It is possible that the organization wants different information security measures but resides in a category which has the information security measures filtered out by the rules based on the organizational profile of the organization. The organization would have to work with the information security improvement actions that work for the average organization of its category.
- A second point of consideration is the growth of an organization. The maturity model could be changed whenever the organizations grows from nine to ten employees and therefore from the 0-9 number of employees category to the 10-50 number of employees category. Adjusting the model is easy; however, when another employee leaves the same organization, the maturity model will be adjusted once again. It might be hard to keep track of what is the current maturity model.
- The last point is the business scope of the organization. The case organization develops software for the health sector and should therefore comply with the information security requirements that apply in this sector. However, it is not clear what happens to the maturity model when the organization widens its scope and develops software for example the educational or financial sector as well.

Next, creating rules in a rule-based system are simple to create, in such a way that even non-programmers can define rules. In the prototype however, the rules are still too much like coding. It is possible to create an extra interface to define the rules in a more simplistic way, but due to time restriction it was decided not to develop an extra interface to implement simplicity.

And lastly, initially, the prototype was supposed to be evaluated using multiple case studies because the artifact is created for multiple organizations with different organizational characteristics by adjusting the rules. However, due to the fact that no effects of the researched organizational characteristics on the matrix were found, it is not necessary to evaluate the rule-based prototype against different organizations.

7.3 Future Research

The research has been set up to find the effects of the organizational characteristics in the general theme, the number of employees, the revenue, and the sector, as stated by Mijnhardt et al. (In Press). However, Mijnhardt et al. (In Press) identified eight other organization characteristics of which the effects have yet to be researched. Next to that, two additional organizational characteristics, business scope of the organization and the used information security framework, need to be validated and their effect on the information security maturity model need to be researched.

In order to determine the capabilities, the design of focus area maturity models (Steenbergen et al., 2010) with the additional method fragment of identifying and scoping the organizational characteristics need to be followed and tested. As can be seen in this research, the capabilities as defined by Spruit and Roeling (2014), were defined in a way that they are applicable for organizations with different organizational profiles. Future study should focus on redefining the capabilities' improvement actions of the model, making them less simplistic and more useful for SMEs. For example, instead of defining an improvement action as: "laws and regulations are part of the information security policy", it should be defined as: "for organizations in the health sector, the following laws and regulations are part of the information security policy", because each sector has its own laws and regulation.

After redefining the capabilities in the ISFAM model, it will be possible to study the effects of organizational characteristics and eventually implement the rule-based approach so it can be used to change the model for different organizational profiles.

This page intentionally left blank

References

Abraham, A. (2005). Rule-Based Expert Systems. *Handbook of measuring system design*.

Atymtayeva, L., Kozhakhmet, K., & Bortsova, G. (2014). Building a Knowledge Base for Expert System in Information Security. In *Soft Computing in Artificial Intelligence* (pp. 57-76). Springer International Publishing.

Baars, T., Mijnhardt, A.F., Vlaanderen, K., & Spruit, M. (2014). An Argument for Dynamic Maturity Matrices (With an Application in Information Security).

Bartoš, J., Walek, B., Klimeš, C., & Farana, R. (2014). Fuzzy Application With Expert System for Conducting Information Security Risk Analysis. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece* (p. 33).

Becker, J., Knackstedt, R., & Pöppelbuß, D. W. I. J. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering*, *1*(3), 213-222.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Bollinger, T. B., & McGowan, C. (1991). A Critical Look at Software Capability Evaluations. In *IEEE Software, July,* 25-41.

Browne, P. (2009). *JBoss Drools Business Rules*. Packt Publishing.

Bruin, T. de, & Rosemann, M. (2005). Towards a business process management maturity model.

BS 7799 (1999). BS 7799: code of practice for information security management as a base for certification.

Buchanan, B. G., & Shortliffe, E. H. (Eds.). (1984). *Rule-based expert systems* (Vol. 3). Reading, MA: Addison-Wesley.

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. *Organizational, Legal, and Technological Dimensions of IS Administrator.* IGI Global Publishing.

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, *26*(5), 496-503.

Cloud Security Alliance (2013). *Cloud Control Matrix v3*. Retrieved on 30-04-2014, https://cloudsecurityalliance.org/research/ccm/#_version_3.

Dekleva, S., & Drehmer, D. (1997). Measuring software engineering evolution: A Rasch calibration. *Information Systems Research*, *8*(1), 95-104.

Esra, O., & Soysal, E. (2012). Security Standards for Electronic Health Records. *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,* (pp. 815-817). IEEE.

Faisal, M. N., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal*, *12*(4), 535-552.

Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*. ACM.

Frangopoulos, E. D., & Eloff, M. M. (2004, June). A Comparative Study Of Standards And Practices Related To Information Security Management. In *ISSA* (pp. 1-15).

Fraser, P., Moultrie, J., & Gregory, M. (2002, February). The use of maturity models/grids as a tool in assessing product development capability. In *Engineering Management Conference, 2002. IEMC'02. 2002 IEEE International* (pp. 244-249).

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly*, *26*(1), 75-81.

Graham, I. (2007). *Business rules management and service oriented architecture: a pattern language*. John Wiley & Sons.

Gruber, T. R. (1993). A Translation Approach to Portable Ontology Specifications. *Knowledge Acquisition*, 5(2), 199-220.

Hayes-Roth, F. (1985). Rule-based systems. *Communications of the ACM*, *28*(9), 921-932.

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

Holland, C. P., & Light, B. (2001). A stage maturity model for enterprise resource planning systems use. *ACM SIGMIS Database*, *32*(2), 34-45.

In Defense of Data (2014). *Data Breach Trends & Stats*. Retrieved on 21-01-2014, http://www.indefenseofdata.com/data-breach-trends-stats/.

International Standards Organization 27002:2013. *Information Security, Security Techniques.* Retrieved on 18-12-2014, http://www.iso27001security.com/html/27002.html.

International Standards Organization 27032. ISO, Guidelines for Cybersecurity. Retrieved on 11-03-2014, http://www.iso27001security.com/html/27032.html.

International Standards Organization 31000. ISO 31000 – Risk Management. Retrieved on 15-11-2014, http://www.iso.org/iso/home/standards/iso31000.htm.

Java Source (2014). *Open Rules Engines in Java.* Retrieved on 26-02-2014, http://java-source.net/open-source/rule-engines.

Karokola, G., Kowalski, S., & Yngström, L. (2011, August). Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. In *HAISA* (pp. 58-73).

Kissel, R. (2013). Glossary of key information security terms. *NIST Interagency Reports NIST IR*, *7298*, 3.

Lessing, M. M. (2008). Best practices show the way to Information Security Maturity.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline*, *9*(1), 181-212.

Liao, S. H. (2005). Expert system methodologies and applications - a decade review from 1995 to 2004. *Expert systems with applications*, *28*(1), 93-103.

Li, X., & Chandra, C. (2008). Toward a secure supply chain: A system's perspective. *Human Systems Management*, *27*(1), 73-86.

Li, X., Chandra, C., & Shiau, J. Y. (2009). Developing taxonomy and model for security centric supply chain management. *International Journal of Manufacturing Technology and Management*, *17*(1), 184-212.

Ligeza, A. (2006). *Logical Foundations for Rule-Based Systems.* Springer Science & Business Media.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management. *Journal of Business Logistics*, *29*(1), 133-155.

Masood, S. H., & Soo, A. (2002). A rule based expert system for rapid prototyping system selection. *Robotics and Computer-Integrated Manufacturing*, *18*(3), 267-274.

Menkus, B. (1991). “Control” is fundamental to successful information security. *Computers & Security*, *10*(4), 293-297.

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*, *22*(2), 1-25.

Mettler, T., & Rohner, P. (2009). Situational maturity models as instrumental artifacts for organizational design. In *Proceedings of the 4th international conference on design science research in information systems and technology* (p. 22). ACM.

Mijnhardt, A.F., Baars, T., & Spruit, M. (In Press). Organizational Characteristics Influencing Information Security Maturity. In *Journal of Computing and Information Science, 00*(00), 00.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine*, *151*(4), 264-269.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: literature search and analysis. *Communications of the Association for Information Systems*, *29*(27), 505-532.

Praxiom Research Group Limited, 2014a. *ISO, Business Continuity Management Standards*. Retrieved on 15-11-2014, http://www.praxiom.com/iso-22301.htm.

Praxiom Research Group Limited, 2014b. *ISO, Information Security Definitions.* Retrieved on 15-11-2014, http://www.praxiom.com/iso-27000-definitions.htm.

Praxiom Research Group Limited, 2014c. *ISO IEC 27002 Old versus New*. Retrieved on 30-01-2014, http://www.praxiom.com/iso-27002-old-new.htm.

Rao, S. S., Metts, G., & Mora Monge, C. A. (2003). Electronic commerce development in small and medium sized enterprises: A stage model and its implications. *Business Process Management Journal*, *9*(1), 11-32.

Sanchez, L. E., Villafranca, D., & Piattini, M. (2007). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. In *WOSIS* (pp. 233-244).

Spruit, M., & Roeling, M. (2014). ISFAM: the Information Security Focus Area Maturity model. *ECIS.*

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2010). The design of focus area maturity models. In *Global Perspectives on Design Science Research* (pp. 317-332). Springer Berlin Heidelberg.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*, *11*(5).

Tae-Nyeon, K., & Hovav, A. An Expert System for the Evaluation of Information Security Programs: A Helping Hand for SMEs.

Vacca, J. R. (2009). *Computer and information security handbook*. Morgan Kaufmann.

Walek, B., Bartos, J., & Zacek, J. (2013). Proposal of The Expert System for Conducting Information Security Risk Analysis. In *The International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2013)* (pp. 58-68). The Society of Digital Information and Wireless Communication.

Weerd, I.V., & Brinkkemper, S. (2008). Meta-Modeling for Situational Analysis and Design Methods. *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications* (pp. 35-54). Mankato: Minnesota State University.

Yin, R. (2003). Case Study Research: Design and Methods. Third edition. *London, UK: Sage publications.*

This page intentionally left blank

Appendices

Appendix A - Additional Information

Student

Name	Gabriël C.A. Slot, BSc
Student number	4005627
E-mail address	g.c.a.slot@students.uu.nl
Master program	Master of Business Informatics
Starting year	September, 2012
Title of thesis project	Towards Rule-based Information Security Maturity

Project supervisor

Name and title	dr. Marco R. Spruit
E-mail address	m.r.spruit@uu.nl
Faculty	Faculty of Science, Information and Computing Sciences
Research group	Software Systems: Organization and Information

Daily supervisor

Name and title	Tan Li
E-mail address	tan@regas.nl
Affiliation	Regas B.V. - Security officer
Address	Pelmolenlaan 18a, 3447 GW Woerden

Second examiner

Name and title	dr. Floris J. Bex
E-mail address	f.j.bex@uu.nl
Faculty	Faculty of Science, Information and Computing Sciences
Research group	Software Systems: Organization and Information

Appendix B - Description Project Activities and Deliverables

Activity	Sub Activity	Description
Design Research	Create Short Proposal	Initial set up of the research.
	Create Long Proposal	More elaborate set up of the research.
Understand Basics of Information Security	Conduct Literature Review	Literature review in order to understand what information security is about.
	Write Theoretical Background	The findings of the previous activity are put together as the theoretical background of the thesis.
Determine Focus Areas	Select Information Security Best Practices	In order to update the ISFAM model, information security standards need to be found.
	Compare Focus Areas against ISFAM	With the found information security standards, a comparison is made to study if focus areas are missing.
	Select Missing Focus Areas	After the comparison a list of missing focus areas can be found.
Determine Capabilities	Conduct Literature Review	A literature study is necessary in order to define the capabilities of the missing focus areas.
	Select Focus Area Requirements	Based on the literature study, the improvement actions of the capabilities need to be formed in applicable improvement actions.
	Arrange Maturity of Capabilities	The applicable capabilities need to be placed on different maturity levels.
Determine Dependencies	Conduct Literature Review	Determining the dependencies of a focus area is important in order to position the capabilities on the focus area maturity model.
	Select Dependencies	Based on the literature study, the applicable dependencies of the found focus areas needs to be selected.
Position Capabilities in		Based on the defined focus areas,

Matrix		capabilities, and dependencies, the capabilities will be placed on the maturity matrix.
Research Effect Organizational Characteristics on ISFAM	Find Information Security Experts	In order to research the effects of the organizational characteristics, it is necessary to find information security experts who can tell what kind of effect the organizational characteristics have. The information security experts will be selected based on three criteria.
	Conduct Expert Interviews	The information security experts will be asked whether there is an effect of the organizational characteristics on the matrix. The template as can be found in the appendices is used.
	Update ISFAM	The maturity model will be updated based on the found effects.
Develop Assessment Instrument		The assessment instrument is necessary in order to see at what maturity level an organization is. It is possible that the organizational characteristics have an effect on the assessment instrument, e.g. questions that are not applicable for a certain organization.
Combine Rule-based Approach	Create ISFAM with Rule-based Approach	The updated maturity model needs to be put into the rule-based context.
	Create Rules	Based on the effects, rules will be defined so that the maturity model will be changed for each organization based on their organizational characteristics.
Evaluate Prototype		The created rule-based prototype will be evaluated at the case organization.
Finalize Thesis Project	Write Thesis	Based on all the actions and findings of the research, the thesis will be written.
	Create Final Presentation	Lastly, the final presentation will be created. The presentation will hold the most important actions and

		findings that can be found in the research.

Concept	Description
SHORT PROPOSAL	First set up of the research and forerunner of the LONG PROPOSAL.
LONG PROPOSAL	More detailed set up of the research.
THEORETICAL BACKGROUND	The information that is necessary for the research.
MISSING FOCUS AREAS	Based on the literature study, a list of focus areas missing in the ISFAM model is created. This list will eventually be considered to be part of the updated ISFAM model.
FOCUS AREA CAPABILITIES	Based on the literature study, the capabilities of the missing focus areas are formed.
CAPABILITY DEPENDENCIES	Based on the literature study, the dependencies of the capabilities of the missing focus areas selected.
FIRST UPDATED ISFAM MATRIX	The original ISFAM model will be updated according to the missing focus areas, capabilities and dependencies.
SECOND UPDATED ISFAM MATRIX	The effects of the organizational characteristics will change the information security maturity model. All these changes will be packed together, so it can be placed in rule-based system.
UPDATED ASSESSMENT INSTRUMENT ISFAM	The effects of the organizational characteristics will change the assessment as well. All these changes will be packed together, so it can be placed in rule-based system.
PROTOTYPE	The FIRST UPDATED ISFAM MATRIX will be put in the rule-based system. Rules will be created to simulate the differences of information security based on the organizational characteristics.
RESULTS	The findings of the case study of the prototype.
THESIS	The final product of the research.
FINAL PRESENTATION	The presentation that will be given at the end of the project, holding the most important findings of the research.

Appendix C - Results Literature Study

Information security

Key word	“Ontology Information Security” OR “Information Security Taxonomy”
Search engine	Google Scholar
# of records before applied filter	47
Filter	Excluding patents and citations
# of unique records identified	46
# of records omitted (not accessible)	7
# of records screened	39
# of records excluded	36
# of records used	3
	Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. In *Proceedings of the 4th international Symposium on information, Computer, and Communications Security* (pp. 183-194). ACM. Li, X., & Chandra, C. (2008). Toward a secure supply chain: A system's perspective. *Human Systems Management*, *27*(1), 73-86. Li, X., Chandra, C., & Shiau, J. Y. (2009). Developing taxonomy and model for security centric supply chain management. *International Journal of Manufacturing Technology and Management*, *17*(1), 184-212.

Key word	Fundamental “Information Security”
Search engine	Google Scholar
# of records before applied filter	57.700
Filter	All in title, excluding patents and citations
# of unique records identified	7
# of records omitted (not accessible)	1
# of records screened	6
# of records excluded	3
# of records used	3
	Menkus, B. (1991). “Control” is fundamental to successful information security. *Computers & Security*, *10*(4), 293-297. Sample, R. (2004). *Fundamental Practices for Security of Information Assets In the Small to Medium Sized Organization* (Doctoral dissertation, University of Oregon). Bassey, E. B. E. (2010). The Fundamental Practice of Information System Security.

Key word	"Comparison Information Security Standards" OR "Comparative Study" "Information Security Standards"
Search engine	Google Scholar
# of records before applied filter	87
Filter	All in title, excluding patents and citations
# of unique records identified	2
# of records omitted (not accessible)	0
# of records screened	2
# of records excluded	0
# of records used	2
	Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. Frangopoulos, E. D., & Eloff, M. M. (2004, June). A Comparative Study Of Standards And Practices Related To Information Security Management. In *ISSA* (pp. 1-15).

Information Security Maturity Models

Key word	"Maturity Models"
Search engine	Google Scholar
# of records before applied filter	10.500
Filter	All in title, excluding patents and citations
# of unique records identified	229
# of records omitted (not accessible)	77
# of records screened	152
# of records excluded	149
# of records used	3
	Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: literature search and analysis. *Communications of the Association for Information Systems*, *29*(27), 505-532. Mettler, T., & Rohner, P. (2009). Situational maturity models as instrumental artifacts for organizational design. In *Proceedings of the 4th international conference on design science research in information systems and technology* (p. 22). ACM. van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I., & Bekkers, W. (2010). The design of focus area maturity models. In *Global perspectives on design science research* (pp. 317-332). Springer Berlin Heidelberg.

Key word	"Information Security Maturity"
Search engine	Google Scholar
# of records before applied filter	215
Filter	All in title, excluding patents and citations
# of unique records identified	28
# of records omitted (not accessible)	9
# of records screened	18
# of records excluded	13
# of records used	5
	Sanchez, L. E., Villafranca, D., & Piattini, M. (2007). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. In *WOSIS* (pp. 233-244). Lessing, M. M. (2008). Best practices show the way to Information Security Maturity. Karokola, G., Kowalski, S., & Yngström, L. (2011, August). Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. In *HAISA* (pp. 58-73). Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, *26*(5), 496-503. Spruit, M., & Röling, M. (2014). ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL.

Rule-based Information Security

Key word	"Information Security" "Expert System"
Search engine	Google Scholar
# of records before applied filter	5.150
Filter	All in title, excluding patents and citations
# of unique records identified	7
# of records omitted (not accessible)	3
# of records screened	4
# of records excluded	0
# of records used	4
	Walek, B., Bartos, J., & Zacek, J. (2013). Proposal of The Expert System for Conducting Information Security Risk Analysis. In *The International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2013)* (pp. 58-68). The Society of

	Digital Information and Wireless Communication. Tae-Nyeon, K., & Hovav, A. An Expert System for the Evaluation of Information Security Programs: A Helping Hand for SMEs. Atymtayeva, L., Kozhakhmet, K., & Bortsova, G. (2014). Building a Knowledge Base for Expert System in Information Security. In *Soft Computing in Artificial Intelligence* (pp. 57-76). Springer International Publishing. Bartoš, J., Walek, B., Klimeš, C., & Farana, R. (2014). Fuzzy Application With Expert System for Conducting Information Security Risk Analysis. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece* (p. 33).

Supply Chain Management

Key word	"Supply Chain Management"
Search engine	Google Scholar
# of records before applied filter	274.000
Filter	All in title, excluding patents and citations, >1.000 citations
# of unique records identified	16
# of records omitted (not accessible)	3
# of records screened	13
# of records excluded	12
# of records used	1
	Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*, *22*(2), 1-25.

Supply Chain Risks

Key word	"Supply Chain Risks Mitigation"
Search engine	Google Scholar
# of records before applied filter	469
Filter	All in title, excluding patents and citations
# of unique records identified	24
# of records omitted (not accessible)	5
# of records screened	19
# of records excluded	18
# of records used	1
	Faisal, M. N., Banwet, D. K., & Shankar, R. (2006). Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal*, *12*(4), 535-552.

Appendix D - Interview Information Security

Effect of organizational characteristics on focus areas

According to Mijnhardt et al. (In Press), organizational characteristics affect the information maturity model. However, it is not clear how the characteristics have an effect on the maturity model.

- *Is there a difference in measuring the maturity of the different information security focus areas and capabilities between organizations with different Number of Employees (0-10, 10-50, and 50-250), Revenues (0-2m, 2m-10m, and 10m-50m), and Sectors?*

Focus Area	**Number of Employees**			**Revenue***			**Sector**
	0-10	**10-50**	**50-250**	**0-2**	**2-10**	**10-50**	
A							
B							
C							
D							

*- in millions

We will look at the following focus areas:

- *Risk Management;*
- *Policy Development;*
- *Organizing Information Security;*
- *Human Resource Security;*
- *Compliance;*
- *Identity and Access Management;*
- *Secure Software Development;*
- *Incident Management;*
- *Business Continuity Management;*
- *Change Management;*
- *Physical and Environmental Security;*
- *Asset Management;*
- *Architecture;*
- *Supply Chain Management.*

Appendix E - Transcript Interviews

Overview

The following information security experts have been interviewed.

Expert	Organization	Function	Years of Information Security Experience (in 2014)
anonymized	*anonymized*	Information Security Consultant	10
anonymized	*anonymized*	Information Security Consultant	10
anonymized	*anonymized*	Information Security Consultant	14
anonymized	*anonymized*	Information Security Consultant	8
anonymized	*anonymized*	Information Security Consultant	12
			54

Interview 1

Name	*anonymized*
Organization	*anonymized*
Function	Information Security Consultant
Years of experience	8
Date	27th June

Information security is dependent on the used framework and the national or international business scope of the organization due to the differences in legislation. Most SMEs can be found at the first two maturity levels of information security. However, that does not mean these organizations are not able to reach full maturity.

Risk Management

SMEs are able to reach full maturity. In practice however, most organizations will not reach more than capability B. There is a difference between the larger category (50-250 NoE) and smaller category (0-10 and 10-50 NoE); it is easier for the smaller organization to have a risk management program because it can be done faster and more simplistic.

An organization with a larger revenue has more to protect, but the organization is also able to spend more on risk management. It is for example possible to hire an information security consultant that focuses on the risk management of an organization.

The sector of an organization tells whether an organization should have a risk management. It is for example not necessary for a bakery company to have a risk management program, while it is for a financial organization.

Policy Development

Most of the organizations focus on the Policy Development focus area as the first step in information security.

The effect of NoE on Policy Development is the same as the previous focus area.

The revenue of an organization has no effect on the capabilities of the development of policies.

The framework that is being used tells whether an organization should focus on the development of policies.

Organizing Information Security

The information security should be done by the management; however, in most companies information security is done by some IT-guy in the organization, who focuses mainly on IT.

In practice, organizations with 0-10 NoE reach capability B, 10-50 NoE reach capability C, and 50-250 NoE reach capability D.

An organization with a larger revenue will be able to spend more resources on organizing information security.

Human Resource Security

The effect of NoE on Human Resource Security is the same as the previous focus area.

The revenue of an organization has no effect on the capabilities of the Human Resource Security focus area.

The sector of an organization demands whether or not it is necessary to implement a screening process before hiring an employee.

Compliance

The effect of the organization characteristics depends on whether or not an organization is listed as a stock market. If an organization is listed, it is accountable and should focus on compliance.

Identity and Access Management

In practice, most of the SMEs do not reach more than capability B.

Identity and access management is a costly project which requires heavy investment.

Identity and access management is demanded in the financial and health sector.

Secure Software Development

The effect of organizational characteristic on the development of secure software depends on the core business of the organization. It should be noted that when an organization develops software for a client, the sector of that client is affecting the development of secure software.

In practice, most SMEs do not reach more than capability A.

The NoE of an organization has no effect on the capabilities of the Secure Software Development focus area.

Incident Management

As the focus area Risk Management, Incident Management is easier for the smaller SMEs. The larger SMEs have a more complex incident management program.

In practice, SMEs with 0-10 and 10-50 NoE do not reach more than capability A. SMEs with 50-250 NoE are mostly found on capability B.

The revenue of an organization has no effect on the capabilities of the Incident Management focus area.

The sector of an organization has no effect on the capabilities of the Incident Management focus area.

Business Continuity Management

As the previous focus area Incident Management, Business Continuity Management is easier for the smaller SMEs. The larger SMEs have a more complex business continuity management program.

The NoE of an organization has no effect on the capabilities of the Business Continuity Management focus area.

A larger revenue of an organization lets an organization have more room for facilitating business continuity. For example, having an ad hoc updated mirror environment to serve as a back-up is possible for organizations that have the resources to implement such a back-up.

The sector of an organization determines the level of business continuity that is necessary. Especially the financial and health sector need a strict business continuity program, because of the data that needs to stay available.

Change Management

When Incident Management is not correctly in place, it will have its effect on Change Management.

In practice, organizations with 0-10 and 10-50 NoE reach capability B. Organizations with 50-250 NoE reach capability C.

The revenue of an organization has no effect on the capabilities of the Change Management focus area.

The sector of an organization has no effect on the capabilities of the Change Management focus area.

Physical and Environmental Security

In practice, SMEs with 0-10 and 10-50 NoE reach capability B, while organizations with 50-250 reach capability C.

As previous focus areas, the revenue of an organization determines how much can be spend on physical and environmental security.

The sector of an organization determines the level of physical and environmental security that needs to be implemented.

Asset Management

In practice, most organizations do not reach capability C. An SME does not need more in the Asset Management focus area.

Organizations with a larger revenue and therefore having more assets will have a more complex asset management program than the organization with a smaller revenue.

The sector of an organization has no effect on the capabilities of the Asset Management focus area.

Architecture

A more technical part of information security, which is only applicable for IT organizations.

In practice, most organizations do not reach capability B.

Supply Chain Management

The Supply Chain Management focus area is especially important for SMEs. Due to the limited resources, the smaller organizations are largely dependent on third parties and should therefore strive for the highest possible maturity level.

The NoE of an organization has no effect on the capabilities of the Supply Chain Management focus area.

The revenue of an organization has no effect on the capabilities of the Supply Chain Management focus area.

The sector of an organization has no effect on the capabilities of the Supply Chain Management focus area.

Interview 2

Name	*anonymized*
Organization	*anonymized*
Function	Information Security Consultant
Years of experience	12
Date	12th August

*The capabilities that are stated in the information security maturity matrix have been set up in a generic way and are therefore applicable for all organizations. Next two examples will explain this statement. (**1**) Focus area Business Continuity Management, capability C "Formal Business Continuity Plan is designed"; organizations with the resources will have an ad hoc mirror environment in order to back-up their data. Organizations that do not have the resources will store their data on a USB-stick, which is updated every month. Both organizations have a design for a business continuity plan. (**2**) Focus area Identity and Access Management, capability A "Formal IAM policy"; an organization with two employees will have a policy that can be written on one page, either employee A or employee B will have access to assets. An organization with 238 employees will have a policy that can be more than ten pages. In both cases the organization has a formal IAM policy.*

Risk Management

SMEs are able to reach full maturity. For example, capability D suggests that Risk management processes should be continuously improved. These improvements can be done on every level.

The revenue of an organization has no effect on the capabilities of the Risk Management focus area.

Risk management is often being done in the sectors finance and health because of the confidence level of data. The organizations in these sectors are therefore known with risk management and are more often found on a higher maturity level than other organizations.

Policy Development

In practice, an organization with 0-10 NoE does not reach capability B, due to the fact that the policies are not written in a formal way. The other organizations are able to reach full maturity.

The sector of an organization has no effect on the capabilities of the Policy Development focus area, although sectors that handle sensitive information will have a larger policy.

Organizing Information Security

In practice, organizations with 0-10 and 10-50 NoE do not reach capability C, due to the knowledge gaining requirement which suggests that an expert needs to be hired.

In practice, organizations with a revenue of 0-2 or 2-5 million will not reach capability D.

The sector of an organization has no effect on the capabilities of the Organizing Information Security focus area, although sectors that handle sensitive information will have a larger list of requirements when organizing information security.

Human Resource Security

Human resource security should be covered by the smaller SMEs, in practice however, most organizations have no or an ad hoc way of handling human resource security.

The NoE of an organization has no effect on the capabilities of the Human Resource Security focus area.

The revenue of an organization has no effect on the capabilities of the Human Resource Security focus area.

The sector of an organization has no effect on the capabilities of the Human Resource Security focus area, although sectors that handle sensitive information will have a larger list of requirements when focusing on human resource security.

Compliance

In practice, most organizations have not heard about compliance. Compliance is not really practiced in the Netherlands or Europe as opposed to the USA. However, the level of compliance as practiced in the USA will eventually be the same in the European countries.

Identity and Access Management

The Identity and Access Management focus area is a topic that is being neglected by the organizations.

In practice, identity and access management is not applicable for SMEs smaller than 5 NoE. However, there is no difference between the SMEs. An organization with two employees will have a policy that can be written on one page, either employee A or employee B will have access to assets. An organization with 238 employees will have a policy that can be more than ten pages. In both cases the organization has a formal identity and access management policy.

The revenue of an organization has no effect on the capabilities of the Identity and Access Management focus area. However, it should be noted that organizations should have an interest in handling identity and access management.

The sector of an organization has no effect on the capabilities of the Identity and Access Management focus area, although sectors that handle sensitive information will have a larger list of requirements when focusing on identity and access management. It is for example more important to have an authentication policy.

Secure Software Development

The NoE of an organization has no effect on the capabilities of the Secure Software Development focus area.

The revenue of an organization has no effect on the capabilities of the Secure Software Development focus area.

The sector of an organization has no effect on the capabilities of the Secure Software Development focus area.

Incident Management

It is difficult for the smaller SMEs to do incident management in a formal way.

The NoE of an organization has no effect on the capabilities of the Incident Management focus area. Managing incidents is easily done by the smaller SMEs.

The revenue of an organization has no effect on the capabilities of the Incident Management focus area.

The sector of an organization has no effect on the capabilities of the Incident Management focus area.

Business Continuity Management

The NoE of an organization has no effect on the capabilities of the Business Continuity Management focus area.

The revenue of an organization has no effect on the capabilities of the Business Continuity Management focus area. Organizations with the resources will have an ad hoc mirror environment in order to back-up their data. Organizations that do not have the resources will store their data on a USB-stick, which is updated every month. Both organizations have a design for a business continuity plan. Testing the USB-stick business continuity plan is much easier than to test an ad hoc mirror environment.

The sector of an organization has no effect on the capabilities of the Business Continuity Management focus area.

Change Management

Change management is the same as the Incident Management focus area. It is difficult for the smaller SMEs to do change management in a formal way.

The NoE of an organization has no effect on the capabilities of the Change Management focus area. Managing changes is easily done by the smaller SMEs.

The revenue of an organization has no effect on the capabilities of the Change Management focus area.

The sector of an organization has no effect on the capabilities of the Change Management focus area.

Physical and Environmental Security

Physical and environmental security is applicable for every organization.

The NoE of an organization has no effect on the capabilities of the Physical and Environmental Security focus area.

The revenue of an organization has no effect on the capabilities of the Physical and Environmental Security focus area.

The sector of an organization has no effect on the capabilities of the Physical and Environmental Security focus area.

Asset Management

Asset management is applicable for every organization.

The NoE of an organization has no effect on the capabilities of the Asset Management focus area.

The revenue of an organization has no effect on the capabilities of the Asset Management focus area.

The sector of an organization has no effect on the capabilities of the Asset Management focus area.

Architecture

According to the expert, the Architecture focus area is a too ambiguous topic.

Supply Chain Management

Supply Chain Management is getting more important because of the specialization of organizations.

The NoE of an organization has no effect on the capabilities of the Supply Chain Management focus area.

The revenue of an organization has no effect on the capabilities of the Supply Chain Management focus area.

The sector of an organization has no effect on the capabilities of the Supply Chain Management focus area.

Interview 3

Name	*anonymized*
Organization	*anonymized*
Function	Information Security Consultant
Years of experience	10
Date	4th September

The capabilities that are stated in the information security maturity matrix have been set up in a generic way. This is not strange because the capabilities are derived from the ISO framework, which is applicable for every organization. Although the organizations are different from one another, the fundamental principle of the capabilities remains the same.

Risk Management

Risk management needs to be handled more formally when the organization will become larger.

Risk management becomes more important for the organization when it gets larger based on revenue.

The financial sector has a larger legislation and is therefore more experienced in handling risk management.

Policy Development

The development of policies has the same results as the previous focus area.

Policy development needs to be handled more formally when the organization will become larger.

Policy development becomes more important for the organization when it gets larger based on revenue.

The financial sector has a larger legislation and is therefore more experienced in developing policies.

Organizing Information Security

From the expert’s experience, the organization of information security is done well. The NoE of an organization does not matter; each organization should have assigned someone as information security officer.

Human Resource Security

Just like the first two focus areas, human resource security needs to be handled more formally when the organization will become larger.

Compliance

In general, organizations do not focus on this focus area. SMEs do not know much about the legislations.

Identity and Access Management

Most of the time, identity and access management is done by the help desk or IT department.

Secure Software Development

According to the expert, the Secure Software Development is not his expertise.

Incident Management

There has to be enough capacity in order to handle incident management in a formal way. In practice, SMEs with 0-10 NoE handle incidents informally. SMEs larger than that category do this in a formal way. Capabilities C and D, where organizations are supposed to do audits, are for the larger SMEs.

Business Continuity Management

Especially technical organizations focus on business continuity management and are mostly done informally. Carrying out the business continuity plan is mainly done by the larger organizations.

Change Management

Change management is done in the same way as incident management is being done. There has to be enough capacity in order to handle change management in a formal way. In practice, SMEs with 0-10 NoE handle changes informally. SMEs larger than that category do this in a formal way.

Physical and Environmental Security

Asset Management

Few organizations have an up-to-date asset management.

The NoE of an organization has no effect on the capabilities of the Asset Management focus area.

The revenue of an organization has no effect on the capabilities of the Asset Management focus area.

The sector of an organization has no effect on the capabilities of the Asset Management focus area.

Architecture

Most of the organizations focus on the architecture in some way, but it is mainly done informally by the information security officer.

For SMEs smaller than 50 NoE, focusing on the architecture seems like an overkill.

Supply Chain Management

The number of third party organizations that process data is growing. The need for supply chain management or supplier management is therefore growing as well.

Interview 4

Name	*anonymized*
Organization	*anonymized*
Function	Information Security Consultant
Years of experience	14
Date	24th October

Looking at capabilities of the maturity matrix, there is no difference in the requirements between organizations. For example, focus area Physical and Environmental Security, capability B "Use of multiple security zones"; organizations with the necessary resources are able to buy a secure room that is locked with identity cards and is monitored with a motion detector in order to secure their assets. Organizations that do not have the resources will store their assets in a vault in a room that can be locked with regular keys. Both organizations fulfill the same capability requirement of having multiple security zones.

Risk Management

In practice, risk management is done informally. Organizations in the financial sector do it in a formal way.

The NoE of an organization has no effect on the capabilities of the Risk Management focus area.

The revenue of an organization has no effect on the capabilities of the Risk Management focus area. The larger SMEs based on revenue have more resources in order to handle risks.

The sector of an organization has no effect on the capabilities of the Risk Management focus area. The organizations in the health care sector will be able to reach capability B, while the organizations in the financial sector are able to reach full maturity.

Policy Development

The NoE of an organization has no effect on the capabilities of the Policy Development focus area. In practice, most organizations reach capability B.

The revenue of an organization has no effect on the capabilities of the Policy Development focus area.

The sector of an organization has no effect on the capabilities of the Policy Development focus area.

Organizing Information Security

The NoE of an organization has no effect on the capabilities of the Organizing Information Security focus area.

The revenue of an organization has no effect on the capabilities of the Organizing Information Security focus area.

The sector of an organization has no effect on the capabilities of the Organizing Information Security focus area. Organizations in the financial sector are able to reach higher maturity in this focus area.

Human Resource Security

The NoE of an organization has no effect on the capabilities of the Human Resource Security focus area.

The revenue of an organization has no effect on the capabilities of the Human Resource Security focus area.

The sector of an organization has no effect on the capabilities of the Human Resource Security focus area.

Compliance

In practice, unless organizations are going to get a certificate, every organization reaches capability A.

Identity and Access Management

In practice, every organization reaches capability A.

The NoE of an organization has no effect on the capabilities of the Identity and Access Management focus area.

The revenue of an organization has no effect on the capabilities of the Identity and Access Management focus area.

The sector of an organization has no effect on the capabilities of the Identity and Access Management focus area.

Secure Software Development

A lot is been written in literature on this subject, however, it is not being done in practice. There are a handful of organizations that develop software in a secure way. These organizations mainly reside in the health care sector. Developers often need to choose between developing secure software or deliver functionality as fast as possible.

Incident Management

Most of the SMEs do not recognize information security incidents as actual incidents.

The NoE of an organization has no effect on the capabilities of the Incident Management focus area.

The revenue of an organization has no effect on the capabilities of the Incident Management focus area.

The sector of an organization has no effect on the capabilities of the Incident Management focus area.

Business Continuity Management

In practice, a growing number of organizations focus on this focus area. Most of the organizations reach capability C.

The sector of an organization has no effect on the capabilities of the Business Continuity Management focus area.

Change Management

In practice, almost every organization does change management, but on an ad hoc base. However, the larger organizations do change management in a more formal way.

Physical and Environmental Security

The NoE of an organization has no effect on the capabilities of the Physical and Environmental Security focus area.

The revenue of an organization has no effect on the capabilities of the Physical and Environmental Security focus area. Organizations with the necessary resources are able to buy a secure room that is locked with identity cards and is monitored with a motion detector in order to secure their assets. Organizations that do not have the resources will store their assets in a vault in a room that can be locked with regular keys. Both organizations fulfill the same capability requirement of having multiple security zones.

The sector of an organization has no effect on the capabilities of the Physical and Environmental Security focus area.

Asset Management

The same as change management, larger organizations do asset management in a more formal way.

Architecture

In practice, the focus area Architecture is mainly done by the larger SMEs. However, according to the expert, there are still some points of improvement for this focus area.

Supply Chain Management

In practice, most of the organizations reach capability A, even though supply chain management is an important subject.

Interview 5

Name	*anonymized*
Organization	*anonymized*
Function	Information Security Consultant
Years of experience	10
Date	11th November

The focus of the interview is on the health care sector. It does not matter whether an organization is large or small, and whether an organization has a large or small revenue. The basic principle of the information security capabilities remain the same.

Risk Management

In practice, SMEs do not have the time to focus on risk management. Risks are therefore not managed or by means of a small spreadsheet.

An organization with a larger revenue is able to accomplish more, hiring an expert for example.

Policy Development

Most of the general practitioners do not have an information security policy, but a document including their main vision.

Organizing Information Security

The awareness of information security is of great importance in this focus area. When the awareness can be seen amongst the employees it is much easier to organize information security. However, organizations still need the resources to do so.

Human Resource Security

Compliance

Again, an organization with a larger revenue will be able to hire a legal advisor in order to help the organization with the legislations.

Identity and Access Management

It is important, especially for organizations in the health care sector, to have an authorization policy stating the profiles that have access to confidential information. In practice, the smaller SMEs handle identity and access management in an informal way. Within the larger SMEs is handled in a more centralized way.

Secure Software Development

Incident Management

The larger SMEs are able to afford more and will therefore have a more advanced system in place, where smaller SMEs will have to do with a more basic license. However, the main idea of handling incident management remains the same.

Business Continuity Management

Small SMEs often do not test their evacuation and communication plan in order to keep their availability. Most of the time, they just talk about it during their coffee break.

Just like previous focus areas, organizations with a lot of resources will be able to spend more on business continuity.

Change Management

Change management can be done a lot faster at smaller organizations. Most of the time, change management is formally organized at the IT department.

Physical and Environmental Security

Having the means to physically protect an organization is important in this focus area. Organizations in the health care sector can maintain their security by using access passes. However, normal locks will suffice as well.

Asset Management

Asset management is a focus area that is covered by the IT department. Contracts needs to be signed whenever there are third parties involved.

Architecture

It is important to determine the risks, which can be done by mapping the information flows. In practice, the larger organizations will write these information flows down.

Supply Chain Management

SMEs need to know what assets are come from third parties as they are risks for their own business. Every aspect of the supplier needs to be written down and signed in a contract.

Appendix F - Rules in the Knowledge Base

```
//Risk management

Rule    “Change RMA to achieved”
    When
        RMA1 == 1 && RMA2 == 1 && RMA3;
    Then
        changeAchieved(“Risk Management”, “A”, true);
End


Rule    “Change RMB to achieved”
    When
        RMA == true && RMB1 == 1 && RMB2 == 1 && RMB3 == 1 && RMB4 == 1;
    Then
        changeAchieved(“Risk Management”, “B”, true);
End


Rule    “Change RMC to achieved”
    When
        RMB == true && RMC1 == 1 && RMC2 == 1 && RMC3 == 1 && RMC4 == 1;
    Then
        changeAchieved(“Risk Management”, “C”, true);
End


Rule    “Change RMD to achieved”
    When
        RMC == true && RMD1 == 1 && RMD2 == 1 && RMD3 == 1;
    Then
        changeAchieved(“Risk Management”, “D”, true);
End
```

Appendix G - Scientific Paper