Modelling adaptive information security for SMEs in a cluster

Bilge Yigit Ozkan, Marco Spruit, Roland Wondolleck and Verónica Burriel Coll
Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands

Received 31 May 2019
Revised 2 October 2019
Accepted 24 October 2019

Abstract

Purpose – This paper presents a method for adapting an Information Security Focus Area Maturity (ISFAM) model to the organizational characteristics (OCs) of a small- and medium-sized enterprise (SME) cluster. The purpose of this paper is to provide SMEs with a tailored maturity model enabling them to capture and improve their information security capabilities.
Design/methodology/approach – Design Science Research was followed to design and evaluate the method as a design artifact.
Findings – The method has successfully been used to adapt the ISFAM model to a group of SMEs within a regional cluster resulting in a model that is aligned with the OCs of the cluster. Areas for further investigation and improvements were identified.
Research limitations/implications – The study is based on applying the proposed method for the SMEs active in the transport, logistics and packaging sector in the Port of Rotterdam. Future research can focus on different sectors and regions. The method can be used for adapting other focus area maturity models.
Practical implications – The resulting adapted maturity model can facilitate the creation and further development of a base of common or shared knowledge in the cluster. The adapted maturity model can cut the cost of over implementation of information security capabilities for the SMEs with scarce resources.
Originality/value – The resulting adapted maturity model can facilitate the creation and further development of a base of common or shared knowledge in the cluster. The adapted maturity model can cut the cost of over implementation of information security capabilities for the SMEs with scarce resources.

Keywords Assessment, SME, Cybersecurity, Process improvement, Information security, Maturity model, Capabilities approach

Paper type Research paper

1. Introduction

Businesses and industries are at risk with increasing cyber threats. Protecting organizational information from these cyber threats is more important than ever. A survey in the Global Risks Report by the World Economic Forum (2018) has revealed that cyberattacks are in the top ten risks both in terms of likelihood and impact. Cyberattacks are now seen as the third most likely global risk for the world over the next ten years. According to this study, cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Cyberattacks have both short-term and long-term economic impacts on different economic agents in terms of loses and expenses (Gañán *et al.*, 2017).

Small- and medium-sized enterprises (SMEs) make up 99.8 per cent of European enterprises (Digital SME Alliance, 2017) and in the Organization for Economic Co-operation and Development (OECD, 2017) area, SMEs are the predominant form of enterprise, accounting for approximately 99 per cent of all firms, yet they are ill-prepared for cyberattacks.

Management of cybersecurity has many challenges both in technical and non-technical factors (Kayworth and Whitten, 2012). Many organizations struggle with cybersecurity not

Journal of Intellectual Capital
Vol. 21 No. 2, 2020
pp. 235-256
Emerald Publishing Limited
1469-1930
DOI 10.1108/JIC-05-2019-0128

only due to a lack of expertise or awareness but also due to the perception of cybersecurity implementation as a costly endeavour. Lack of funding is another barrier, to accessing external support, in particular for SMEs (Kertysova *et al.*, 2018).

One way of tackling with the challenges of managing and implementing cybersecurity is through the concept of maturity modelling. Originating from software engineering, maturity modelling is a method for representing domain specific knowledge in a structured way in order to provide organizations with an evolutionary process for assessment and improvement (Yigit Ozkan and Spruit, 2019; Becker *et al.*, 2009). A maturity model provides a structure for organizations to baseline current capabilities in a domain, establishing a foundation for consistent evaluation. It allows organizations to compare their capabilities to one another and enables leaders to make better, well-informed decisions about how to support progression and what investments to make in regard to domain specific initiatives (adapted from US Department of Homeland Security, 2014).

From an intellectual capital (IC) perspective, organizations assessing themselves utilizing a maturity model can capture their related IC in the form of capabilities in various domains such as information security and business process management. Usage of maturity models can give insights into their current state and facilitate the identification of the desired capabilities and the definition of improvement roadmaps.

Although there is a multitude of tools such as standards, frameworks and models available to measure, identify and improve the cybersecurity practices at organizations, many of these are not well suited for SMEs (Manso *et al.*, 2015). This is mainly because these tools are complex and require specialists to be hired in order to utilize them properly.

From the perspective of information security maturity models, there is a need to facilitate SMEs with tailor-made models that are more situation aware and that can adapt to their specific needs (Mijnhardt *et al.*, 2016). An adaptive maturity model yields a higher value, as the resulting capabilities and areas for improvement match the expectations and characteristics of the organizations, SMEs in this case (Cholez and Girard, 2014). Given these phenomena, utilization of maturity models for self-assessing information security or cybersecurity capabilities can be a remedy for SMEs.

Lawson and Lorenz (1999) reviewed key ideas in the firm capabilities literature and showed how they can be usefully extended to develop a conception of collective learning among regionally clustered enterprises. Smedlund and Pöyhönen (2005) defined an approach for understanding regional knowledge creation and the dynamics of creating IC in a complex collaboration of multiple actors. They argue that three main themes appear in the different theories of the intellectual resources of organizations. These themes are stated as: intangible assets, competencies and capabilities, and social relationships in which the knowledge processes occur. The capability approach views knowledge as an ongoing and emergent process, where the capability to leverage, develop and change intangible assets is important (Smedlund and Pöyhönen, 2005). The competencies and capabilities approach resonates with the maturity modelling paradigm which enables the assessment and improvement of capabilities in a specific domain. Maturity models that define the required capabilities in a domain can be used to capture these intellectual resources of organizations.

The focus of this paper is to propose a method for adaptive maturity modelling that facilitates collective and collaborative improvement of information security capabilities in a cluster of SMEs through regional learning. The proposed method enables SME managers in a specific cluster to adapt a comprehensive Information Security Focus Area Maturity (ISFAM) model) according to their differentiating sectoral organizational characteristics (OCs). A cluster is a geographically proximate group of interconnected companies and associated institutions in a particular field, linked by commonalities and complementarities (Porter, 2000).

We aim to facilitate SMEs with a maturity model to create and further develop a base of common or shared knowledge in the information security domain. The adapted maturity

model can be used as an evaluative and comparative basis for the improvement of organizational capabilities.

Therefore, this paper proposes a method for adaptive maturity modelling and presents the results of our empirical study of creating a tailored focus area information security maturity model for SMEs in a cluster (the SMEs active in transport, logistics and packaging sector in the Port of Rotterdam), taking into account their OCs' profile. By using the tailored maturity model, SMEs in this cluster can have personalized guidance on applying the maturity model and improving their capabilities.

The tailored model in our research is based on the ISFAM model (Spruit and Roeling, 2014), which is the only existing focus area maturity model (FAMM) for information security in the literature. Its broad scope covers all of the links in the systems chain, that is, technologies–policies–processes–people–society–economy–legislature, as discussed by Lowry *et al.* (2017). The ISFAM model's broad coverage comes from its 13 focus areas, 51 information security capabilities and 161 statements that are derived from well-known industry standards (Spruit and Roeling, 2014).

Limited resources, company size, limited support for practical tools and guidelines and flexibility concerns are among the important barriers of wide adoption of maturity models (Poeppelbuss *et al.*, 2011; Staples *et al.*, 2007). Providing an adaptive method that accounts for OCs, we aim to lower ISFAM model implementation barriers, by improving its practical qualities regarding SME awareness and cost of implementation.

Our research question is formulated as follows:

RQ1. How can the focus area maturity model in information security be methodologically adapted to the organisational characteristics profiles of an SME cluster for focussed process improvement?

We followed a design science research methodology to investigate our research question.

This paper is organized as follows. In Section 2, the background information on existing information and cybersecurity maturity models, FAMMs, the need for adaptive information security and situational awareness are discussed and the ISFAM model, the OCs that influence information security and an analytics approach to adaptive maturity models are introduced. In Section 3, the DSR framework and methodology applied for creating our artifact is presented. In Section 4, the method for adapting the ISFAM model is presented. In Section 5, the evaluation and its results are presented. In Section 6, the findings are discussed. Finally, in Section 7, the results and implications of this study and the areas for future research are given.

2. Background and related research

In the simplest form, a maturity model provides a benchmark against which an organization can score its achievements in a progressive manner. The maturity model can represent attributes, characteristics, patterns or practices regarding certain capabilities and their arrangement on a scale that represent measurable states. Introduced by Crosby (1979), maturity modelling is widely adopted in software engineering and information systems domains following the popularity of capability maturity model (CMM) for software processes (Paulk *et al.*, 1993).

A distinction can be made between the maturity modelling variants. First, staged five-level models distinguish five levels of maturity. Each level has a number of focus areas defined specifically for that level. An example of this is the CMM model, although many others exist. Second, continuous five-level models are also based on five general maturity levels. However, the main difference with the staged five-level models is that the focus areas are not attributed to a certain level. Third, FAMMs differentiate from the abovementioned five-level models in that FAMMs have their own number of specific maturity levels for each focus area (Steenbergen *et al.*, 2007).

There are numerous works related to information security and cybersecurity maturity modelling. Some of these maturity models are given in Table I.

The first three models presented in Table I are characterized as maturity models where the last one is an FAMM. In the following paragraphs, we briefly discuss these models.

The US Department of Energy (2014), in collaboration with Carnegie Mellon University, USA, developed the Cybersecurity Capability Maturity Model from the Electricity Subsector Cybersecurity Capability Maturity Model (p. 2) Version 1.0 by removing sector-specific references and terminology. The model is organized into ten domains, and each domain is a logical grouping of cybersecurity practices. Practices within each domain are organized into objectives, which represent achievements within the domain. The Open Information Security Management Maturity Model (O-ISM3) (The Open Group, 2017) is The Open Group framework for managing information security. It aims to ensure that security processes operate at a level consistent with business requirements. O-ISM3 is technology-neutral and focusses on the common processes of information security which most organizations share. O-ISM3 defines four levels of security processes as generic processes, strategic-specific processes, tactical-specific processes and operational-specific processes. National Initiative for Cybersecurity Education (NICE) (US Department of Homeland Security, 2014) aims to help organizations apply the best practice elements of workforce planning in analysing their cybersecurity workforce requirements and needs. NICE segments key activities to three main areas as: process and analytics, integrated governance, skilled practitioners and enabling technology and defines three maturity levels as: limited, progressing, and optimizing. ISFAM (Spruit and Roeling, 2014) is an FAMM based on widely-implemented industry standards. The dependencies between the focus areas are presented to facilitate the implementation of improvement programmes within the organizations. The ISFAM model is elaborated in Section 2.3.

There have been other studies to address the maturity assessment and improvement of information security in SMEs (Cholez and Girard, 2014). In their paper, the authors define the main future challenge for their assessment is to set up an ontology that defines groups of organizations that share similar information security issues and objectives.

The existing models in the literature are far from addressing the OCs to provide a tailored approach for capability assessment and improvement for the SMEs.

2.1 Focus area maturity models

FAMM, being a more flexible descendent of the CMM, is "based on the concept of a number of focus areas that have to be developed to achieve maturity in a functional domain" (van Steenbergen *et al.*, 2010). Since the conceptualization of these models, Sanchez-Puchol and Pastor-Collado (2017) indicated 16 different FAMMs in literature, most originating from the IT domain. Some examples are the "FAMM for Information Use in Organizations"

Maturity model	Organization/authors	Purpose/target
Cybersecurity Capability Maturity Model (ES-C2M2) (US Department of Energy, 2014)	The US Department of Energy (DOE)	Assessment of critical infrastructures
Open Information Security Management Maturity Model (O-ISM3) (The Open Group, 2017)	The Open Group	Any type of organization
National Initiative for Cybersecurity Education – Capability Maturity Model (NICE) (US Department of Homeland Security, 2014)	The US Department of Homeland Security	Workforce planning for cybersecurity
Information Security Focus Area Maturity model (ISFAM) (Spruit and Roeling, 2014)	(Spruit and Roeling, 2014)	Any type of organization

Table I.
Information and cybersecurity maturity models

(Alves, 2013), "Disaster Risk Management Focus Area Maturity Model" (Waldt, 2013) and the ISFAM model (Spruit and Roeling, 2014).

As the name suggests, the core of an FAMM consists of focus areas, which can be divided into a number of capabilities. As the capabilities within an FAMM are positioned relatively to each other, the resulting model and positioning of capabilities represent an order of different aspects that should be addressed and implemented in a given functional domain. A functional domain can be described as "the whole of activities, responsibilities and actors involved in the fulfilment of a well-defined function within an organization" (van Steenbergen *et al.*, 2010). A focus area, then, is defined as: "an aspect that has to be implemented to a certain extent for a functional domain to be effective" (van Steenbergen *et al.*, 2010). Multiple focus areas in a FAMM should provide complete coverage of the functional domain that is to be assessed.

Each focus area (most FAMMs consist of 12–20 focus areas) has some capabilities associated with, that are indicated with a capital letter. The resulting maturity matrix, and the structure and position of the capabilities in that specific matrix define dependencies between capabilities within a certain focus area. For example, capability A should be implemented before B in a given focus area. The matrix also gives guidance on interdependencies between different focus areas, where it is advised to implement a given capability before, or after, a capability from another focus area. The final overall maturity score is based on the lowest scoring capability for a certain focus area.

2.2 The need for adaptive information security and situational awareness

The importance of situational awareness was illustrated in a technical report produced in the early 1990s. In this report (Hayes and Zubrow, 1995), the organizations were assessed during a seven-year period (1987–1994) using the CMM model. The researchers found that 73 per cent of the assessed organizations were stuck in the initial level (1), mainly because the prescribed requirements in a certain process area were too hard to be met. In a study by Baars *et al.* (2016), this problem was also addressed, although more geared towards the problems especially attributed to the ISFAM model. As the ISFAM model was co-developed in a medium-sized organization, the standards and best practices used for information security are also targeted at such organizations. Therefore, they argue that the resulting model is rigid by design, and "does not differentiate on the different characteristics of an organization" (Mijnhardt *et al.*, 2016). This results in implementation processes to be ineffective and that the capabilities can be irrelevant or inapplicable, thus especially SMEs will not be able to reach the higher maturity levels.

Adaptive information security here refers to an information security model which is capable to adapt to variable requirements that arise from OCs of companies. The need for adaptive information security stems from the fact that the finite resources have to be used in the optimal way producing required outputs.

2.3 ISFAM: the Information Security Focus Area Maturity model

The method we propose in this research builds on the ISFAM model (Spruit and Roeling, 2014). In this section, we outline the essential details of the model and elaborate on our rationale for choosing ISFAM as the reference maturity model to adapt.

The ISFAM model was proposed to help organizations, especially SMEs, achieve a strategy–IT security alignment in ever changing security risk environments. The ISFAM model consists of 13 focus areas and distributes 51 capabilities (A-E) over 12 model-wide maturity levels. The assessment is made up out of 161 yes/no questions, making it possible to conduct an information security assessment in a matter of hours. The maturity levels of ISFAM are grouped in categories as design, implementation, operational effectiveness and monitoring. The design stage is considered as the starting point, where an organization still has to put processes and procedures in place. Monitoring, on the other hand, is considered the

highest level, where an organization has most measures in place. To give an idea of the reference model we aim to adapt for SMEs in a cluster, we present the ISFAM model in Figure 1. In this figure, the focus areas and the maturity levels for these focus areas are depicted. In Spruit and Roeling (2014), the dependencies found in the literature, which facilitates an implementation order for the capabilities, were also presented by the authors.

ISFAM comprises the common structural elements of FAMMs (i.e. focus areas, capabilities, maturity levels) as defined by van Steenbergen *et al.* (2010) and described in Section 2.1.

2.4 OCs influencing SME information security maturity

With the aim of profiling the characteristics of target SMEs, we use the research of Mijnhardt *et al.* (2016), which presents the OCs influencing SMEs' information security maturity. Based on literature review and expert evaluations, they have identified 11 OCs consist of 47 measurement levels (Mijnhardt *et al.*, 2016) as presented in Figure 2. Hereafter, the moniker CHaracterizing Organizations' Information Security for SMEs (CHOISS) which was proposed by Mijnhardt *et al.* (2016) is used to refer to this research.

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 1.
The Information Security Focus Area Maturity (ISFAM) model

Source: Spruit and Roeling (2014)

Organizational characteristic	Measurement levels
General company information	
Number of employees	0–9 employees, 10–49 employees, 50–250 employees
Organization's revenue	0–2 m, 2–10 m, 10–50 m
Organization's sector	Aerospace and defense; agriculture and foresting; business services and consultancy; consumer, media, leisure, travel and entertainment; finance, banking and insurance; health; IT and telecom; industrial production; energy, utilities and mining; public, education and non-profit; transport, packaging and logistics
Degree of outsourcing	
To what degree is software development outsourced	0–25, 25–50, 50–75, 75–100%
To what degree are software and services hosted externally	0–25, 25–50, 50–75, 75–100%
Reliance on IT for running the business operations	
The organization can do business without IT support for × many hours	<10 min, 10 min to 1 h, 1–24 h, >24 h
CIA (confidentiality, integrity, availability)	
The importance of availability of the organization's critical information	Low, medium, high
The importance of confidentiality of the organization's critical information	Low, medium, high
The importance of integrity of the organization's critical information	Low, medium, high
Complexity of the IT environment	
The number of FTE supporting the IT environment	0–1 FTE, 1–2.5 FTE, 2.5–5 FTE, 5–10 FTE, > 10 FTE
The organization's annual spend on IT	<1, 1–2.5, 2.5–5, 5–10, >10%

Figure 2.
Organizational characteristics and measurement levels in CHOISS

Source: Mijnhardt *et al.* (2016)

2.5 An analytics approach to adaptive maturity models using OCs

With the aim of identifying the maximum maturity levels achievable by the target SMEs, we adopt the analytical approach proposed by Baars *et al.* (2016) to define adaptive maturity models based on OCs that pertain to SME information security profiles. In this approach, the OCs used for profiling were adopted from CHOISS (Mijnhardt *et al.*, 2016) (see Section 2.4). The research followed up on those previous efforts by further evaluating the OCs and their measurement levels, and how they pertain to ISFAM maturity matrix through a survey. This research concluded that ignoring OCs could result in unnecessary implementation of capabilities, the wrong order of priority when implementing capabilities or over-implementing of capabilities. Aside from the influence OCs have on the complete model, the authors present the results including a granular level of measurement: the influence of OCs on the focus areas in ISFAM. We used the values of the importance of the focus areas identified in this research (the details of the application are elaborated in Section 5.1). Hereafter, the moniker ANLYMM, an ANaLYtics approach to adaptive Maturity Models, using OCs is used to refer to this research.

3. Research method

This study is structured according to the DSR approach (Hevner *et al.*, 2004). The artifact of this research is the Method for Adaptive Information Security Maturity Modelling in Clusters (MAISMMC) that can be followed to adapt ISFAM to the SME profiles in a cluster. Our research method follows the DSR methodology described by Peffers *et al.* (2007) which consists of the following steps: problem identification, definition of solution objectives, design and development, demonstration, evaluation and communication. Accordingly, our research includes realising a problem situation, reviewing published literature, developing our artifact (method), demonstrating the use of our artifact in a case study, evaluating our results with experts and communicating the research objectives, structure and results to the other researchers.

Following this research approach, we present our artifact in Section 4. To provide a better understanding of our research context, we present our research framework adapted from Hevner *et al.* (2004) in Figure 3.

The abbreviations used for the articles in the knowledge base foundations refer to the corresponding articles we based our research on. These papers – ISFAM (Spruit and

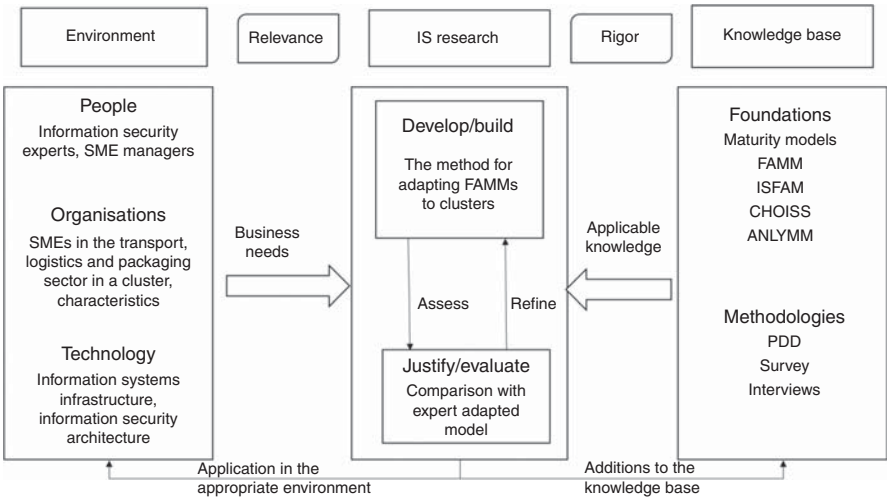


Figure 3.
Research framework

Source: Adapted from Hevner *et al.* (2004)

Roeling, 2014), CHOISS (Mijnhardt *et al.*, 2016) and ANLYMM (Baars *et al.*, 2016) – are elaborated in Section 2.

The practical value of a design study lies in its consideration for applicability beyond a single context-bound example (Williams and Pollock, 2012). A research criterion to assess the quality of design study results (e.g. design theories, principles and artifact) from this pragmatic perspective is projectability (Baskerville and Pries-Heje, 2014; Baskerville and Pries-Heje, 2019). Projectability has been proposed as DSR quality criteria that suits better to the future-oriented and prescriptive nature of DSR and as an alternative to generalizability which conventionally applies to descriptive and backwards-looking research contexts such as those of the social and natural sciences. Following this line of argumentation, in our research, we adopt projectability as an alternative to generalization for framing the future and assessing the propagation of the knowledge and artifact we propose following design science research.

4. Artifact description

In this paper, we present the MAISMMC that can be used to create an adapted information security FAMM based on OCs that represent the SMEs in a cluster.

As described in our research framework, the method uses the previous knowledge base and incorporates the findings from the previous research (Spruit and Roeling, 2014; Mijnhardt *et al.*, 2016; Baars *et al.*, 2016).

An overview of MAISMMC that results in an adapted information security FAMM model for a cluster is depicted in Figure 4.

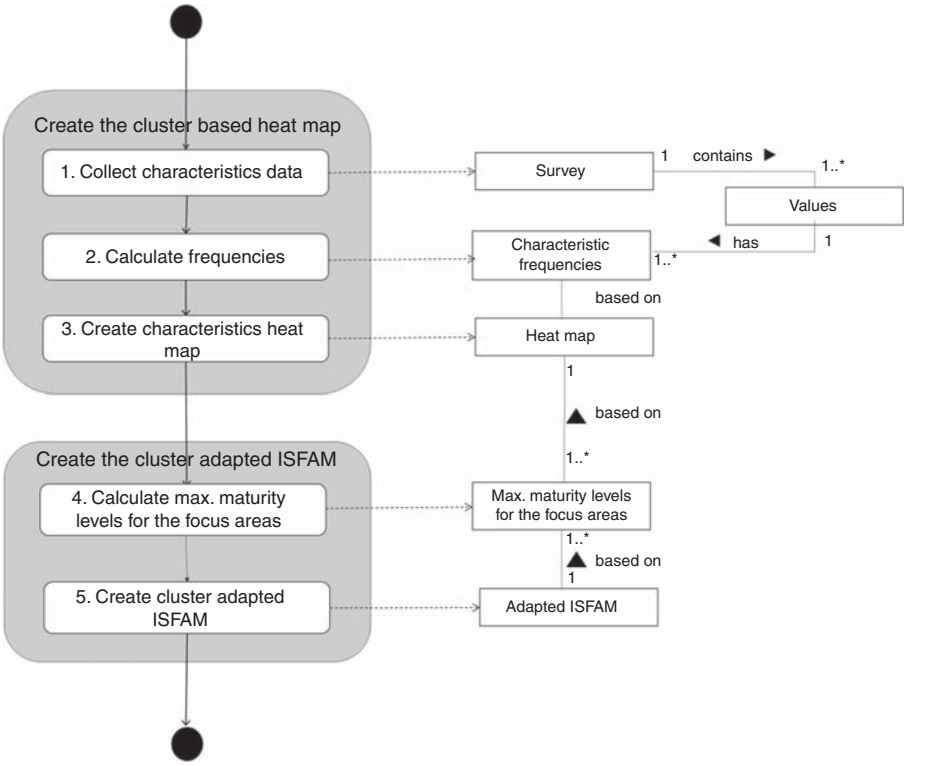


Figure 4.
Method for Adaptive Information Security Maturity Modelling in Clusters (MAISMMC)

The notation used is a process deliverable diagram as described by van de Weerd and Brinkkemper (2009), where the process view on the left-hand side of the diagram is based on a UML activity diagram (OMG, 2017) and the deliverable view on the right-hand side of the diagram is based on a UML class diagram (OMG, 2017).

Each step in the method is elaborated in the following paragraphs:

- Step 1: collect characteristics data – the aim in this step is to collect OCs data from the target SMEs to further construct an adapted AN information security FAMM model for a profile that represents the SME population in the cluster. Data collection can be done by several means such as by conducting an online or an offline survey or by interviewing the SME representatives.
- Step 2: calculate frequencies – this step involves the analysis of the data collected to identify frequencies for each OC. More specifically, in this step, the frequencies of individual characteristics in the SME cluster data set from Step 1 are calculated.
- Step 3: create characteristics heat map – a heat map is a graphical representation of data where the individual values contained in a matrix are represented as colours (Zhao *et al.*, 2014). In this step, a heat map is created as a visual aid using the calculated frequencies from the previous step to present the OCs of the target SMEs.
- Step 4: calculate maximum maturity levels for the focus areas – this step involves using the highest frequency values represented in the heat map as the OCs of SMEs in the cluster and entering these values into the model suggested by Baars *et al.* (2016). This will result in the automatic calculation of the maximum maturity levels for each focus area. The application of this step and the calculations are elaborated and demonstrated in Section 5. In this step, we identify the effect the OCs of the SMEs have on the information security FAMM model by using the results of ANLYMM (Baars *et al.*, 2016).
- Step 5: create cluster-adapted ISFAM (CA-ISFAM) – after identifying how the OCs of the SMEs in a cluster affect the focus areas and the capabilities of the information security FAMM, this step involves using the calculated maximum maturity levels to visualize the adapted maturity model.

5. Evaluation

Evaluation of design artefacts is an essential step in DSR (Hevner *et al.*, 2004). Our evaluation has a comparative set-up where the cluster-adapted FAMM generated by MAISMMC is compared and contrasted to the model adapted by two security experts for the same cluster. In Section 5.1, we present MAISMMC application steps, the interim products and the resulting cluster specific ISFAM. In Section 5.2, we present the expert adaption results for the same cluster and aggregate the experts' results.

5.1 A case study: application of MAISMMC for Port of Rotterdam SME cluster

To evaluate our method, we conducted a case study in an SME cluster at the Port of Rotterdam area in the transport, logistics and packaging sector. In the following paragraphs, we elaborate on the execution of MAISMMC.

Step 1: collect characteristics data. This step involved conducting a survey to identify OCs influencing information security maturity of SMEs in the transport, logistics and packaging sector for profiling purposes and for creating a heat map that visualizes the characteristics. The survey protocol, questions and possible answers are given in the Appendix. In the survey, the OCs, which were the result of a comprehensive literature study and interviews with a number of IS professionals, proposed by

Mijnhardt *et al.* (2016) were used. This enabled us to find out the effects of these characteristics on the ISFAM model using the analytical approach proposed by Baars *et al.* (2016). The survey was distributed amongst organizations (which responded to our call) situated within the ecosystem of a large European seaport area, the Port of Rotterdam. The resulting deliverable from this step was the survey data sets, which served as input for the next step. Amongst the invited companies during a cybersecurity resilience event in the port area, nine SMEs responded to our survey in the transport, logistics and packaging sector. The event was one of the bimonthly cybersecurity resilience events organized in the port in which participation is on a voluntary basis. The survey responders were key personnel assigned by the managers of the SMEs to represent their company as the key informants during the event.

Based on the results obtained from the survey, a heat map considering the cluster that was represented most by means of the number of respondents was constructed. Two transformation steps have been applied to the SPSS data set: first, the data set has been reduced by means of case selection. The rule applied for case selection restricted the data set to the results provided by the organizations active in the transport, logistics and packaging sector. Second, the resulting cases have been split-up based on the OC "Number of Employees" (NoE). Comparing the NoE against the other OCs of the CHOISS model allows for distinction between SMEs and the large organizations that participated in the survey.

Step 2: calculate frequencies. This step involved calculating the frequency of each measurement level for each characteristic.

Step 3: create characteristics heat map. Based on the calculated OC frequencies, a heat map was constructed. The heat map provides a visual representation of the distribution of characteristics in the cluster.

Table II depicts the heat map created based on the OC survey results from nine SMEs. This heat map shows the aggregated results from the OC surveys specific to the transport, logistics and packaging sector. As we aim for SMEs in the transport, logistics and packaging sector, the OC's organization's sector and the NoE are not explicitly stated. These OCs are the main "input ingredients" of the derived model. Therefore, the measurement level for the criterion of the maximum NoE at SMEs is assumed as fewer than 250. Moreover, the criterion of the sector is assumed as transport, logistics and packaging sector. Table II is used further in this research to answer the research question given in Section 1. The three colour scale used in the heat map depicts the frequencies of the data collected within the survey. The darker colour having the larger frequency value, the lighter colour having the smaller frequency value.

Table II.
Heat map visualizing the organizational characteristics of the SMEs within the cluster

Organisational Characteristics Influencing SME Information Security Maturity (Mijnhardt *et al.*, 2016)	Heat map of the Values Collected from the SMEs				
Amount of Revenue	0–2m	2–10m	10–50m	>50m	
Percentage of Total Software development is outsourced	0–25%	25–50%	50–75%	75–100%	
Percentage of Total Hosting/IT services is outsourced	0–25%	25–50%	50–75%	75–100%	
Importance of Confidentiality of Critical Data	Low	Medium	High		
Importance of Integrity of Critical Data	Low	Medium	High		
Importance of Availability of Critical Data	Low	Medium	High		
Time an Organization can Run without IT support	0–10m	10–60m	1–24h	>24h	
Amount of FTE supporting the IT environment	0–1	1–2.5	2.5–5	5–10	>10
Percentage of Annual Revenues spent on IT	0–1%	1–3%	3–5%	5–10%	>10%

Step 4: calculate maximum maturity levels for the focus areas. The OC heat map created during the previous step was used to create the adapted ISFAM model. The calculation was performed based on the survey data set from Baars *et al.* (2016), which gave a general direction on which capabilities can be excluded. Based on the original survey data set created by Baars *et al.* (2016) which contains relative valuations per focus area for each OC, we were able to calculate the maximum maturity level per focus area.

By choosing the characteristics represented in the heat map (Table II) for the SMEs in the cluster, we calculated the maximum maturity level per focus area as shown in Table III.

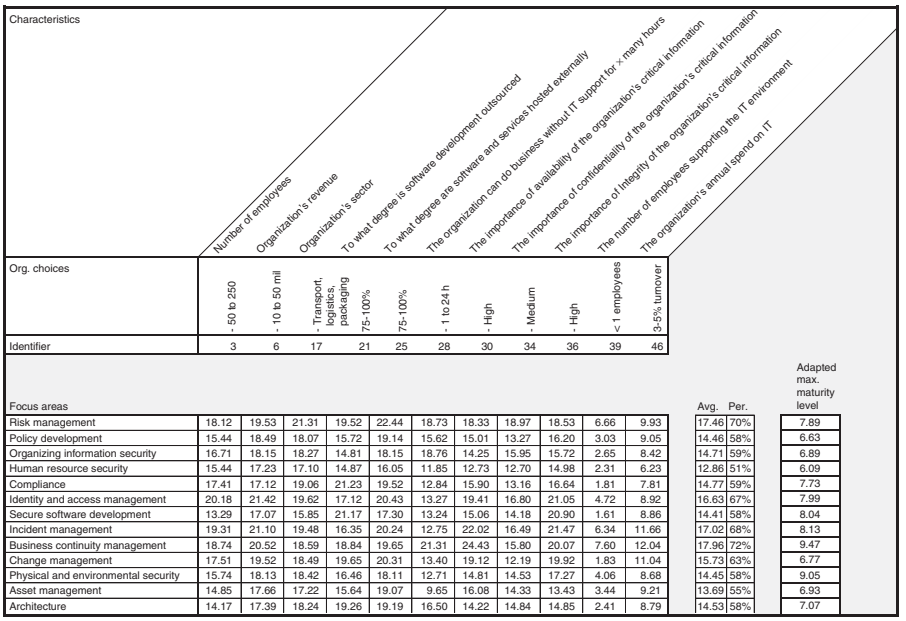
An enhanced version of the ISFAM was developed which implements a weighted model to account for OCs (Baars *et al.*, 2016).

A screenshot of the model with the OCs input according to the heat map (Table II) is presented in Figure 5.

We applied the calculations based on the organizational profile of the SMEs in our case study as follows. Every measurement level given in Figure 2 is identified by a unique number labelled as "Identifier" in Figure 5 which shows the respective number for the chosen identifier in the model. With the data set provided in the model, valuation for

ISFAM model focus area	A (average value of the importance of the focus area (over 25) (AVG.))	B (value of the importance of the focus area as percentage (PER.))	C (minimum maturity level in ISFAM model)	D (maximum maturity level in ISFAM model)	E (adapted maximum maturity level (B×(D−C)+C))
Risk management	17.46	69.85	3	10	7.89
Policy development	14.46	57.84	2	10	6.63
Organizing information security	14.71	58.85	1	11	6.89
Human resource security	12.86	51.45	3	9	6.09
Compliance	14.77	59.09	3	11	7.73
Identity and access management	16.63	66.52	4	10	7.99
Secure software development	14.41	57.65	4	11	8.04
Incident management	17.02	68.08	2	11	8.13
Business continuity management	17.96	71.85	3	12	9.47
Change management	15.73	62.90	3	9	6.77
Physical and environmental security	14.45	57.79	5	12	9.05
Asset management	13.69	54.76	2	11	6.93
Architecture	14.53	58.14	3	10	7.07

Table III.
ISFAM model focus areas and adaptive maximum levels calculated



Characteristics	Number of employees	Organization's revenue	Organization's sector	To what degree is software development outsourced	To what degree are software and services hosted externally	The organization can do business without IT support for > many hours	The importance of availability of the organization's critical information	The importance of confidentiality of the organization's critical information	The importance of integrity of the organization's critical information	The number of employees supporting the IT environment	The organization's annual spend on IT
Org. choices	- 50 to 250	- 10 to 50 mil	- Transport, logistics, packaging	75-100%	75-100%	- 1 to 24 h	- High	- Medium	- High	< 1 employees	3-5% turnover
Identifier	3	6	17	21	25	28	30	34	36	39	46

Focus areas												Avg.	Per.	Adapted max. maturity level
Risk management	18.12	19.53	21.31	19.52	22.44	18.73	18.33	18.97	18.53	6.66	9.93	17.46	70%	7.89
Policy development	15.44	18.49	18.07	15.72	19.14	15.62	15.01	13.27	16.20	3.03	9.05	14.46	58%	6.63
Organizing information security	16.71	18.15	18.27	14.81	18.15	18.76	14.25	15.95	15.72	2.65	8.42	14.71	59%	6.89
Human resource security	15.44	17.23	17.10	14.87	16.05	11.85	12.73	12.70	14.98	2.31	6.23	12.86	51%	6.09
Compliance	17.41	17.12	19.06	21.23	19.52	12.84	15.90	13.16	16.64	1.81	7.81	14.77	59%	7.73
Identity and access management	20.18	21.42	19.62	17.12	20.43	13.27	19.41	16.80	21.05	4.72	8.92	16.63	67%	7.99
Secure software development	13.29	17.07	15.85	21.17	17.30	13.24	15.06	14.18	20.90	1.61	8.86	14.41	58%	8.04
Incident management	19.31	21.10	19.48	16.35	20.24	12.75	22.02	16.49	21.47	6.34	11.66	17.02	68%	8.13
Business continuity management	18.74	20.52	18.59	18.84	19.65	21.31	24.43	15.80	20.07	7.60	12.04	17.96	72%	9.47
Change management	17.51	19.52	18.49	19.65	20.31	13.40	19.12	12.19	19.92	1.83	11.04	15.73	63%	6.77
Physical and environmental security	15.74	18.13	18.42	16.46	18.11	12.71	14.81	14.53	17.27	4.06	8.68	14.45	58%	9.05
Asset management	14.85	17.66	17.22	15.64	19.07	9.65	16.08	14.33	13.43	3.44	9.21	13.69	55%	6.93
Architecture	14.17	17.39	18.24	19.26	19.19	16.50	14.22	14.84	14.85	2.41	8.79	14.53	58%	7.07

Figure 5.
Using the CHOISS model to calculate the maximum maturity levels

each focus area was calculated as an average of all values for 11 OC. The maximum possible value for each "focus area influenced – by a given organisational characteristic pair" was 25 according to the study (Baars *et al.*, 2016). Column A in Table III presents these values for each focus area for the OCs in the heat map. Column B in Table III presents the value as calculated as a percentage. In the ISFAM, due to the dependencies between the information security capabilities, the minimum and maximum maturity level for each focus area were identified (Spruit and Roeling, 2014). These values are given in the respective columns C and D in Table III. The final profile was generated by using the values in column E. The formula for calculating the adaptive maximum level according to the OCs in the heat map is given in the column E header in Table III. This formula normalizes the focus area's maturity level taking into account the percentage calculated according to the findings of Baars *et al.* (2016).

Step 5: create the CA-ISFAM model. Using the maximum maturity levels calculated in the previous step, we created the adapted ISFAM model that we believe is applicable to our target SMEs in the transport, logistics and packaging sector.

The resulting CA-ISFAM model based on the heat map is depicted in Table II.

The coloured parts show the inapplicable maturity levels in the adapted model. For example, for the risk management focus area, the maximum maturity level that is applicable is 7 (which is calculated as 7.89 in Table III); therefore, the higher maturity levels are shown in red colour.

5.2 ISFAM model adaption by experts

In order to be able to compare and contrast our adapted model, we asked two experts to adapt ISFAM individually.

The process of adaption by security experts involved providing the experts with the original ISFAM model and asking them to evaluate this model's applicability and

achievability by the SMEs in the cluster. After the experts' adaption, the results obtained were compared with the CA-ISFAM to understand the variations.

The adaption process involved discussing the initial ISFAM model with experts from the cluster of interest. Information security experts in the Port of Rotterdam area have been considered due to their expertise in the transport, logistics and packaging sector in addition to their information security expertise. In this case, two experts were selected that have sufficient knowledge about the information security domain and practices of the organizations in the transport, logistics and packaging sector.

In order to obtain and validate the insights separately, it was chosen to conduct the adaption in two separate sessions.

The first adaption was performed with an expert with 19 years of professional experience. The expert's title within the organization was "Security and Risk Officer".

The second adaption was performed with an expert with 12 years of experience. The expert's title within the organization was "Chief Information and Security Officer".

Prior to the adaption sessions, the experts received the following documents:

- the heat map depicted in Table II: this was used by the experts to guide their reasoning about the suitability and achievability of different capabilities;
- initial ISFAM model capabilities and maturity levels: the complete ISFAM assessment including 13 focus areas and all statements used to determine the maturity; and
- hand-out of assessment questions: the experts received a copy of the assessment questions so that they could refer to them when adapting the model.

Each adaption session had a duration of approximately 2 h in which the experts were asked to consider the OC heat map and adapt the initial ISFAM model based on the suitability and achievability of the capabilities of each focus area for the SMEs in the cluster.

The experts had to rank each capability level with either a "−1" (not suitable), "0" neutral and "1" suitable for the target SMEs.

Since the research was conducted in the transport, logistics and packaging sector, we could reach only two information security experts experienced in this sector in the Port of Rotterdam area.

5.2.1 Expert adaption results. The results of both expert adaption sessions and the aggregated results are presented in Figure 6.

The aggregated results were created by adding up the values given by the experts based on the two separate adaption sessions. Therefore, scores of 2 indicate both experts agreed to include the capability in the model. Scores of 1 indicate at least one expert decided to include the capability in the model. 0 indicates an aggregated neutral attitude. Scores of −1 indicate at least one expert decided to exclude the capability. Scores of −2 indicate both experts agreed to exclude the capability from the model.

The results presented in Figure 6 are further discussed in Section 6 with details per focus area.

6. Evaluation findings and discussion

In this section, we present the comparison of aggregated expert adaption results (AEAR) and CA-ISFAM model based on the OC heat map. The combined findings per focus area are shown in Figure 8.

From the capabilities that are in the CA-ISFAM (Figure 7), as suggested by the OC heat map and calculated values, it seems that based on the expert adaptions only 3 capabilities out of 29 resulted in a final score of −1. This happened due to one expert rating these capabilities with a −1, whereas the other valued the capability with a 0, indicating that some statements were

ISFAM model focus areas		Maturity levels												
		0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational														
Risk management	Expert 1				1		1		−1			0		
	Expert 2				1		1		0			−1		
	Aggregated				2		2		−1			−1		
Policy development	Expert 1			1		1						−1		
	Expert 2			1		1						0		
	Aggregated			2		2						−1		
Organizing information security	Expert 1		1			1					−1		−1	
	Expert 2		1			1					0		0	
	Aggregated		2			2					−1		−1	
Human resource security	Expert 1				1		1		0		−1			
	Expert 2				1		1		0		−1			
	Aggregated				2		2		0		−2			
Compliance	Expert 1				1		1						−1	
	Expert 2				1		1						0	
	Aggregated				2		2						−1	
Technical														
Identity and access management	Expert 1					1		0		−1		−1		
	Expert 2					1		1		0		−1		
	Aggregated					2		1		−1		−2		
Secure software development	Expert 1					−1		−1			−1		−1	
	Expert 2					1		−1			−1		−1	
	Aggregated					0		−2			−2		−2	
Organizational and technical														
Incident management	Expert 1			1			1			0			−1	
	Expert 2			1			1			−1			−1	
	Aggregated			2			2			−1			−2	
Business continuity management	Expert 1				1		1		1			0		−1
	Expert 2				1		1		1			0		−1
	Aggregated				2		2		2			0		−2
Change management	Expert 1				1		1		1		−1			
	Expert 2				1		1		1		−1			
	Aggregated				2		2		2		−2			
Support														
Physical and environmental security	Expert 1						1		1		0			−1
	Expert 2						1		1		1			−1
	Aggregated						2		2		1			−2
Asset management	Expert 1			1				1			−1		−1	
	Expert 2			1				1			1		−1	
	Aggregated			2				2			0		−2	
Architecture	Expert 1				1		0			−1		1		
	Expert 2				1		−1			−1		−1		
	Aggregated				2		−1			−2		0		
		Design					Implementation		Operational effectiveness			Monitoring		

Figure 6.
Individual and aggregated expert adaption results (AEAR)

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 7.
The cluster-adapted ISFAM model based on the OC heat map (CA-ISFAM)

considered sufficient or achievable. Only one capability received a score of 1, whereas the other 25 capabilities are all ranked sufficient and relevant for the SMEs as defined in the CA-ISFAM, resulting in a score of 2. One of the capabilities (secure software development) that should be in the model as calculated based on the OC heat map resulted in a score of −2. Overall, the results

obtained from the experts were for the most part in-line considering the capabilities that were considered sufficient and achievable for SMEs in the cluster.

When considering the other half of the model which represents the excluded capabilities (the part of the CA-ISFAM that is marked red) the results are slightly different. In this part of the model, a total of 26 capabilities are considered in total. From these 26 capabilities, a total of 12 have been marked by both experts with a −1, resulting in a final score of −2. In these cases, both experts agreed that the capabilities can be omitted from the assessment when considering the SMEs presented by the heat map. Seven capabilities have a final score of −1; in these cases, one expert rated the capability with a −1, where the other expert rated the capability with a 0. Interestingly, a total of five capabilities have a neutral final score of 0. Lastly, two capabilities that could be omitted based on the calculations were indeed considered sufficient and achievable by the experts, resulting in one capability with a score of 1 and another capability with a score of 2. In this case, capability C of change management is considered by both experts as sufficient and achievable for the SMEs.

Since the experts were neutral when scoring the capabilities as 0, in Figure 8, we presented these capabilities in colour in line with CA-ISFAM as they are not considered as concrete variations.

6.1 Focus area based analysis of the results

Regarding the focus area "risk management" according to the aggregated expert adaption, there was a negative score (−1) obtained for capability level C. One expert argued that this capability, which prescribed risk management as a formalized process that is used in most projects as defined by the organization was not achievable.

For the focus areas "policy development" and "organizing information security", AEAR were in line with the CA-ISFAM.

For the focus area "human resource security", capability level C, AEAR present a neutral score of "0", while this capability was omitted in CA-ISFAM.

For the focus areas "compliance" and "identity and access management", AEAR were in line with CA-ISFAM.

ISFAM model focus areas		0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational														
Risk management	Expert				2		2		−1			−1		
	CA-ISFAM				A		B		C			D		
Policy development	Expert			2		2						−1		
	CA-ISFAM			A		B						C		
Organizing information security	Expert		2			2					−1		−1	
	CA-ISFAM		A			B					C		D	
Human resource security	Expert				2		2		0		−2			
	CA-ISFAM				A		B		C		D			
Compliance	Expert				2		2						−1	
	CA-ISFAM				A		B						C	
Technical														
Identity and access management	Expert					2		1		−1		−2		
	CA-ISFAM					A		B		C		D		
Secure software development	Expert					0		−2			−2		−2	
	CA-ISFAM					A		B			C		D	
Organizational and technical														
Incident management	Expert			2			2			−1			−2	
	CA-ISFAM			A			B			C			D	
Business continuity management	Expert				2		2		2			0		−2
	CA-ISFAM				A		B		C			D		E
Change management	Expert				2		2		2		−2			
	CA-ISFAM				A		B		C		D			
Support														
Physical and environmental security	Expert						2		2		1			−2
	CA-ISFAM						A		B		C			D
Asset management	Expert			2				2			0		−2	
	CA-ISFAM			A				B			C		D	
Architecture	Expert				2		−1			−2		0		
	CA-ISFAM				A		B			C		D		
		Design					Implementation		Operational effectiveness			Monitoring		

Figure 8.
Combined results from the aggregated expert adaption results (AEAR) and the cluster-adapted ISFAM model (CA-ISFAM)

For the focus area "secure software development", one expert argued that based on the OC heat map, all capabilities could be omitted (most organizations do not develop software and only have a limited amount of full-time equivalent (FTE)). Furthermore, capability level A introduces an approach to software development life cycle, based on a "waterfall" approach. This was in contrast to the more commonly used agile practices used in smaller projects, more suitable for SMEs (Balaji and Murugaiyan, 2012). However, the experts argued that, if a limited amount of FTE is available, working based on a prescribed method would be sufficient. Therefore, the experts agreed to exclude capability B, whereas it was included in CA-ISFAM.

Although "incident management" is considered an important practice, expert 2 argues that many SMEs will only be limited to a "ticket system" that registers incidents when they occur. Furthermore, as the heat map suggests that many of the IT services and hosting are outsourced, this would also be sufficient to cover the incidents. Although the expert argues that it would be better if, for example, systems would provide an audit trail, he does not believe that this is achievable for a single FTE on IT that also has to deal with all other daily IT matters. Therefore, expert 2 excluded capability C whereas it was included in CA-ISFAM.

For the focus area "business continuity management", capability level D, AEAR present a neutral score of "0", while this capability was omitted in CA-ISFAM.

The focus area "change management" showed an interesting finding. Both experts agreed that capability level C should be retained whereas it was excluded in CA-ISFAM. Both experts argued that this capability was suitable and achievable for SMEs and was important to implement as this prevents unwanted downtime of systems due to changes being implemented but not thoroughly assessed based on their potential impact on the business processes.

For the focus areas "physical and environmental security" and "asset management", AEAR were in line with CA-ISFAM.

The final focus area "architecture" introduced an interesting insight. Although both experts agreed that this practice was probably not introduced at SMEs, the capability A was considered suitable and achievable. However, both capability B was omitted from the model. In contrast, capability B was included in CA-ISFAM.

As an overall summary, 51 capabilities represented in 13 focus areas in the initial ISFAM model, AEAR and CA-ISFAM differ only in 5 of the capabilities. Four of the differences are regarding the exclusion of the capabilities by the experts, One is regarding the inclusion of the capability by the experts. This finding indicates that our method for adapting FAMMs was successfully implemented adapting ISFAM to the SME cluster in the case study.

7. Conclusion

In the information security domain, prior work has emphasized the need for adapting the maturity models according to the OCs of the entities that aim to utilize the models (Cholez and Girard, 2014). These OCs influencing information security maturity proposed by Mijnhardt *et al.* (2016) were used in this empirical research with the ambition of formulating a method for the adaption of the information security FAMM for an SME cluster. The proposed method was applied for the SMEs in transport, logistics and packaging sector in the Port of Rotterdam area, resulting in an adapted information security maturity model for the target SME cluster.

We experimented our method with a specific FAMM (ISFAM) which, to our knowledge, is the only FAMM in information security. We used the characteristics that influence information security maturity (CHOISS) and the analytics approach for adapting the reference FAMM (ANLYMM). The findings show that by introducing a heat map that visualizes the common OCs of SMEs in a specific cluster, a profile can be created that generates a baseline for the capabilities that can be excluded from the reference maturity model, based on the input selectors most common in the cluster. By comparing the model

obtained by executing the method to the results obtained by the information security experts' adaption, the proposed method was found to be successful.

The findings of this study have a number of practical implications. The cluster-adapted model can be used by the target SMEs to assess and capture their information security related IC. This can add value to the regional learning in the cluster and provide a basis for communicating on and comparing their information security capabilities. The cluster-adapted maturity model can cut the cost of over implementation of information security capabilities for the SMEs with scarce resources.

A limitation of our method along with its underlying design theory is its application in a single instance bound by the case study context. While this instance can be considered as an initial projection of our design, we identify two possible projections from our research: first, our method can be adapted for developing methods for the generation of adapted FAMMs in SME clusters in other domains. Second, the proposed method can be used to adapt the demonstrated FAMM (ISFAM) to other target SME clusters.

During this research, some opportunities for further research have been found. As a possible research direction, adaptability can further be introduced by altering the capabilities of the maturity model. This research mainly focussed on the exclusion of the capabilities. In certain cases, the experts excluded capabilities based on the fact that the SMEs had many practices outsourced. In these cases, the experts argued that the model should consider this more, as many capabilities are not relevant when most of the IT hosting and services are outsourced. In these cases, as argued by the experts, the operational responsibility lies with the suppliers, instead of the organization itself. The results of this study revealed some differences between using the proposed method and expert adaption. The cause for these differences can be traced back to the method components that are used. The component producing these differences is the ANLYMM. ANLYMM can further be investigated in the light of experts' point of view regarding the affected capabilities.

Having discussed the challenges that SMEs face in the formulation of information security management practices, considerably more work will need to be done to help them in this endeavour. Since this study was limited to adapting an existing FAMM, our current research focusses on developing a unified, personalized and self-service information security and cybersecurity focus area maturity model specifically for SMEs.

Acknowledgements

Conflict of interests: the authors declare that there are no competing interests regarding the publication of this paper.

This work was made possible with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). During this research, Bilge Yigit Ozkan was a full-time PhD candidate supported by the SMESEC project. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

References

Alves, J.F.A. (2013), "Finding maturity evolution paths for organisational use of information", master thesis, Instituto Superior Técnico, June, available at: https://fenix.tecnico.ulisboa.pt/downloadFile/395145528220/DMEIC-57552-Joana-Alves.pdf (accessed 22 November 2018).

Baars, T., Mijnhardt, F., Vlaanderen, K. and Spruit, M. (2016), "An analytics approach to adaptive maturity models using organizational characteristics", *Decision Analytics*, Vol. 3 No. 1, pp. 1-26.

Balaji, S. and Murugaiyan, M.S. (2012), "Waterfall vs. V-Model vs. Agile: a comparative study on SDLC", *International Journal of Information Technology and Business Management*, Vol. 2 No. 1, pp. 26-30.

Baskerville, R. and Pries-Heje, J. (2014), "Design theory projectability", in Doolin, B., Lamprou, E., Mitev, N. and McLeod, L. (Eds), *Information Systems and Global Assemblages: (Re)Configuring Actors, Artefacts, Organizations*, Springer, Berlin and Heidelberg, pp. 219-232.

Baskerville, R. and Pries-Heje, J. (2019), "Projectability in design science research", *Journal of Information Technology Theory and Application (JITTA)*, Vol. 20 No. 1, pp. 53-76.

Becker, J., Knackstedt, R. and Pöppelbuß, J. (2009), "Developing maturity models for IT management", *Business & Information Systems Engineering*, Vol. 1 No. 3, pp. 213-222.

Cholez, H. and Girard, F. (2014), "Maturity assessment and process improvement for information security management in small and medium enterprises", *Journal of Software: Evolution and Process*, Vol. 26 No. 5, pp. 496-503.

Crosby, P.B. (1979), *Quality is Free: The Art of Making Quality Certain*, McGraw-Hill, New York, NY.

Digital SME Alliance (2017), "Position paper on European cybersecurity strategy: fostering the SME ecosystem", 31 July, available at: www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf (accessed 16 October 2018).

Gañán, C.H., Ciere, M. and van Eeten, M. (2017), "Beyond the pretty penny: the economic impact of cybercrime", *Proceedings of the 2017 New Security Paradigms Workshop*, ACM Press, Santa Cruz, CA, pp. 35-45.

Hayes, W. and Zubrow, D. (1995), "Moving on up: data and experience doing CMM-based process improvement", Technical Report No. CMU/SEI-95-TR-008, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, p. 41.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS Quarterly*, Vol. 28 No. 1, pp. 75-105.

Kayworth, T. and Whitten, D. (2012), "Effective information security requires a balance of social and technology factors", SSRN Scholarly Paper No. ID 2058035, Social Science Research Network, Rochester, NY, available at: https://papers.ssrn.com/abstract=2058035 (accessed 31 May 2019).

Kertysova, K., Bhattacharyya, K., Frinking, E., Dool, K., van den, Maričić, A. and Bhattacharyya, K. (2018), "Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks - study", The European Economic and Social Committee, 22 May, available at: www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study (accessed 16 October 2018).

Lawson, C. and Lorenz, E. (1999), "Collective learning, tacit knowledge and regional innovative capacity", *Regional Studies*, Vol. 33 No. 4, pp. 305-317.

Lowry, P.B., Dinev, T. and Willison, R. (2017), "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 546-563.

Manso, C.G., Rekleitis, E., Papazafeiropoulos, F. and Maritsas, V. (2015), "Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises", ENISA, Heraklion, available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML (accessed 16 October 2018).

Mijnhardt, F., Baars, T. and Spruit, M. (2016), "Organizational characteristics influencing SME information security maturity", *Journal of Computer Information Systems*, Vol. 56 No. 2, pp. 106-115.

OECD (2017), *Enhancing the Contributions of SMEs in a Global and Digitalised Economy*, OECD, Paris, available at: www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf (accessed 31 May 2019).

OMG (2017), "Unified modeling language specification version 2.5.1", available at: www.omg.org/spec/UML/ (accessed 24 November 2018).

Paulk, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V. (1993), "Capability maturity model, version 1.1", *IEEE Software*, Vol. 10 No. 4, pp. 18-27.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007), "A design science research methodology for information systems research", *Journal of Management Information Systems*, Vol. 24 No. 3, pp. 45-77.

Poeppelbuss, J., Niehaves, B., Simons, A. and Becker, J. (2011), "Maturity models in information systems research: literature search and analysis", *Communications of the Association for Information Systems*, Vol. 29, available at: https://doi.org/10.17705/1CAIS.02927

Porter, M.E. (2000), "Location, clusters, and company strategy", in Clark, G.L., Feldman, M.P. and Gertler, M.S. (Eds), *The Oxford Handbook of Economic Geography*, Oxford University Press, Oxford, pp. 253-274.

Sanchez-Puchol, F. and Pastor-Collado, J.A. (2017), "Focus area maturity models: a comparative review", in Themistocleous, M. and Morabito, V. (Eds), *Information Systems*, Springer International Publishing, New York, NY, pp. 531-544.

Smedlund, A. and Pöyhönen, A. (2005), "Chapter 14 – intellectual capital creation in regions: a knowledge system approach", in Bounfour, A. and Edvinsson, L. (Eds), *Intellectual Capital for Communities*, Butterworth-Heinemann, Boston, MA, pp. 227-252.

Spruit, M. and Roeling, M. (2014), "ISFAM: the information security focus area maturity model", *Proceedings of the European Conference on Information Systems (ECIS) 2014, Association for Information Systems, Tel Aviv, 9-11 June*, p. 15.

Staples, M., Niazi, M., Jeffery, R., Abrahams, A., Byatt, P. and Murphy, R. (2007), "An exploratory study of why organizations do not adopt CMMI", *Journal of Systems and Software*, Vol. 80 No. 6, pp. 883-895.

Steenbergen, M.V., Berg, M.V.D. and Brinkkemper, S. (2007), "An instrument for the development of the enterprise architecture practice", *Proceedings of the Ninth International Conference on Enterprise Information Systems, Vol. 2, Madeira*, pp. 14-22.

The Open Group (2017), "Open Information Security Management Maturity Model (O-ISM3), Version 2.0", available at: https://publications.opengroup.org/c17b (accessed 19 July 2018).

US Department of Energy (2014), "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)", available at: www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf (accessed 31 August 2018).

US Department of Homeland Security (2014), "National Initiative for Cybersecurity Education – Cybersecurity Capability Maturity Model white paper", Department of Homeland Security, 4 August, available at: www.hsdl.org/?view&did=798503 (accessed 13 February 2019).

van de Weerd, I. and Brinkkemper, S. (2009), "Meta-modeling for situational analysis and design methods", in Syed, M.R. and Syed, S.N. (Eds), *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, IGI Global, PA, pp. 35-54.

van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I. and Bekkers, W. (2010), "The design of focus area maturity models", in Winter, R., Zhao, J.L. and Aier, S. (Eds), *Global Perspectives on Design Science Research*, Springer Berlin Heidelberg, Berlin and Heidelberg, pp. 317-332.

Waldt, G.V.D. (2013), "Disaster risk management : disciplinary status and prospects for a unifying theory : original research", *Jamba : Journal of Disaster Risk Studies*, Vol. 5 No. 2, pp. 1-11.

Williams, R. and Pollock, N. (2012), "Research commentary: moving beyond the single site implementation study: how (and why) we should study the biography of packaged enterprise solutions", *Information Systems Research*, Vol. 23 No. 1, pp. 1-22.

World Economic Forum (2018), "The global risks report", World Economic Forum, available at: www3.weforum.org/docs/WEF_GRR18_Report.pdf (accessed 5 October 2018).

Yigit Ozkan, B. and Spruit, M. (2019), "A questionnaire model for cybersecurity maturity assessment of critical infrastructures", in Fournaris, A.P., Lampropoulos, K. and Marín Tordera, E. (Eds), presented at the IOSEC Information and Operational Technology Security Systems 2018, Springer International Publishing, New York, NY, pp. 49-60.

Zhao, S., Guo, Y., Sheng, Q. and Shyr, Y. (2014), "Advanced heat map and clustering analysis using heatmap3", *BioMed Research International*, Vol. 2014, pp. 1-6.

Appendix. Organizational characteristics survey protocol and questionnaire

Investigators

Roland Wondolleck, University, Information and Computing Sciences Department.
Bilge Yigit Ozkan, University, Information and Computing Sciences Department.

Background

In our current research, we are investigating a method to adapt a comprehensive information security maturity model to the organizational characteristics (OCs) of SMEs in transport, logistics and packaging sector. This survey is prepared to collect OCs of the SMEs in the Port of Rotterdam area.

Past work

Mijnhardt *et al.* (2016) investigated the OCs influencing SMEs' information security maturity. Based on literature review and expert evaluations they have identified 11 OCs that consist of 47 measurement levels. This survey is based on these characteristics. The measurement levels are used as the possible answers for the survey questions.

Aims

The aim of this survey is to collect OCs (Mijnhardt *et al.*, 2016) data from the target SMEs to further construct an adapted ISFAM model (Spruit and Roeling, 2014) for a profile that represents the SME population in the sector.

Design

The survey has 11 questions. Each question has multiple choice answers, single answer permitted.

Population

The survey targets SMEs in the transport, logistics and packaging sector within the Port of Rotterdam area, the Netherlands. The Port of Rotterdam has a programme for cyber resilience. The aim of the programme is to encourage co-operation between companies in the port of Rotterdam and to raise awareness among companies about cyber risks in order to become the best digitally secured port in the world. The programme is an initiative of the Municipality of Rotterdam, Port of Rotterdam Authority, Seaport Police and Deltalinqs. The survey was handed out during a security event related to this cyber resilience programme. Due to the level of awareness within the Port of Rotterdam area, the companies that were present during the security event were very interested in our survey and they attended eagerly.

Method

The survey will be performed on paper. The answers will be transferred to an electronic file.

Only the answers from SMEs (NoE $<$ 250 will be considered.). A short introduction and explanation about the research will be given prior to the survey. The survey is expected to take maximum of 10 min.

Planned statistical analysis

The frequencies of the answers will be calculated for every question.

Survey questions

In sum, 11 questions for the OCs and possible answers for these questions are listed as follows.

(1) In which sector is your organization active?

- Aerospace and defense
- Professional services and finance
- Energy and utilities

- IT and telecom
- Public and education
- Consumer retail, leisure, travel, entertainment and media
- Health
- Transport, logistics and packaging
- Agriculture, forests and mining
- Industrial, construction, manufacturing and engineering
- Other

(2) What is the amount of revenue of your organization?

- 0–2m
- 2–10m
- 10–50m
- More than 50m

(3) What is the number of employees of your organization?

- 0–10
- 10–50
- 50–250
- More than 250

(4) What percentage of software development is outsourced?

- 0–25 per cent
- 25–50 per cent
- 50–75 per cent
- 75–100 per cent

(5) What percentage of hosting/IT services is outsourced?

- 0–25 per cent
- 25–50 per cent
- 50–75 per cent
- 75–100 per cent

(6) What is the importance of confidentiality of critical data?

- Low
- Medium
- High

(7) What is the importance of integrity of critical data?

- Low
- Medium
- High

(8) What is the importance of availability of critical data?

- Low

- Medium
- High

(9) How long can the organization run without IT support?

- 0–10 min
- 10–60 min
- 1–24 h
- More than 24 h

(10) How many FTE support the IT environment?

- 0–1
- 1–2.5
- 2.5–5
- 5–10
- More than 10

(11) What percentage of the annual revenues is spent on IT?

- 0–1 per cent
- 1–3 per cent
- 3–5 per cent
- 5–10 per cent
- More than 10 per cent

Corresponding author
Bilge Yigit Ozkan can be contacted at: b.yigitozkan@uu.nl