CYBERSECURITY MATURITY ASSESSMENT AND STANDARDISATION

BİLGE YİĞİT ÖZKAN

Cybersecurity Maturity Assessment and Standardisation

Bilge Yiğit Özkan

SIKS Dissertation Series No. 2022-19
The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

ISBN: 978-94-6423-887-7
DOI: 10.33540/869

Cover design by Vecteezy.com
Printed by ProefschriftMaken | www.proefschriftmaken.nl

Cybersecurity Maturity Assessment and Standardisation

Cybersecurity Maturity Assessment en Standaardisatie

(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de
Universiteit Utrecht
op gezag van de
rector magnificus, prof.dr. H.R.B.M. Kummeling,
ingevolge het besluit van het college voor promoties
in het openbaar te verdedigen op

maandag 11 juli 2022 des middags te 4.15 uur

door

Bilge Yiğit Özkan

geboren op 30 juli 1974
te Merzifon, Turkije

Promotoren:

Prof. dr. S. Brinkkemper
Prof. dr. M.R. Spruit

Beoordelingscommissie:

Prof. dr. B. van den Berg
Dr. S.A. Fricker
Prof. dr. W. Pieters
Prof. dr. K. Renaud
Prof. dr. A.A. Salah

This thesis was accomplished with financial support from European Union's Horizon 2020 research and innovation programme under grant agreement No: 740787 (SMESEC).

Acknowledgements

In October 2017, I moved to the Netherlands and started my PhD studies. The challenges of doing a PhD and living in a new county went along with their joy. Many people helped me professionally and personally during my journey.

First, my daily supervisor and promoter, prof. dr. Marco Spruit, you were always there when I needed it. A big thank you for being so nice, accessible, and supportive. I would also like to express my gratitude to my promoter prof. dr. Sjaak Brinkkemper, for offering valuable support. Sjaak's research group (Organisation and Information) was the first group I joined at UU. They made my life easier with their support, both professionally and personally. Special thanks to Başak Aydemir, Fabiano Dalpiaz, Gerard Wagenaar, Jan Martijn van der Werf, Matthieu Brinkhuis, Marcela Ruiz, Sietse Overbeek, Sergio Espana Cubillo, and Slinger Jansen.

We shared our successes (paper acceptances) and failures (paper rejections) and learnt from each other with the Applied Data Science lab members. Thanks, Chaïm van Toledo, Emil Rijcken, Friso van Dijk, Max van Haastrecht, Noha Tawfik, Pablo Mosteiro Romero, and Vincent Menger.

Although my research focus was not on NLP, when I joined his team, prof. dr. Kees Deemter offered support and invested time in me. I want to thank Kees Deemter and the members of the NLP group for welcoming me.

My colleagues from the EU Horizon 2020 SMESEC project partners, who made the endless project meetings enjoyable, many thanks for your support.

I want to thank the reviewers, editors, and conference organisers for their valuable contributions to the research community and my research. My assessment committee members provided me with valuable and constructive feedback on my thesis. I am grateful for their time.

Our lovely administrative colleagues; Corine Kranenberg-Jolles, Geraldine Leebeek, Gina Beekelaar, and Jet Haasbroek. Thank you for being so nice and supportive.

Some of my colleagues became my friends. I am so grateful for their existence and friendship: Alireza Shojaifar, Armel Lefebvre, Guru(raj) Maddodi, Ian (Zhengru) Shen, Injy Sarhan, Lamia Elloumi, and Verónica Burriel Coll. I have one non-colleague friend to mention, dear Honghong Bai; thank you for always being there for me. Ünal Aksu, it was a great pleasure for me that our paths crossed again at UU. Thanks for being such a supportive friend.

I left my friends and family in Turkey when I moved to the Netherlands. Nevertheless, the distance does not affect the strong bonds between us. Although being far away, they were always with me. Special thanks to my oldest friends Burcu Özbek, Görkem Yaran, and Melek Can. I fully expect we shall be part of each other's lives forever.

My former colleagues and still beloved friends: Aylin Sönmez, Ayşegül Dalkıran, Duygu Tuncay, Ebru Çetin, Hale Erdem, Şule Tüzül and Yener Cehiz, I always miss you.

The most hardworking and determined person I've ever known, Sırma Çelik, since you moved from Turkey, you have always been far away, first in Japan and now in the US, but I know you're always there. I was lucky enough to have friends from Turkey who live in the Netherlands. Banu Aysolmaz, Coşkun Özaşçılar, Deniz İren, Hilal Akçomak, Hülya Zalaltuntaş, Mustafa Kaygısız, Nermin Yavaş, Sema Çam, and Oktay Türetken, thank you all for being such great friends. Aysun Çetinyürek and Yalçın Yavuz, many thanks for your valuable and continuous friendship.

I cannot thank my dear parents, Gülten and Mustafa Yiğit, enough for always encouraging me to be the best I can be, being there no matter what, and being such inspiring persons.

Finally, my beloved partner Barış Özkan, I am always grateful to have you in my life. I found doing a PhD to be a solitary endeavour that I could not have finished without you keeping me motivated.

Contents

LIST OF FIGURES

LIST OF TABLES

1 Introduction

We first provide the relevant background information for this dissertation. Then, we elaborate on the problem statement, research questions, framework, scope, and significance. Finally, we present the outline of the dissertation.

1.1 Research Background

We explore cybersecurity maturity assessment and standardisation from an information systems research perspective. Both cybersecurity maturity assessment and standardisation have been used in practice to improve enterprises' cybersecurity. In this dissertation, we define *cybersecurity* as the preservation of confidentiality, integrity, and availability of enterprise assets in cyberspace (ISO/IEC, 2012). Further, we define *information security* as the preservation of confidentiality, integrity, and availability of enterprise assets (information) in cyberspace and physical space (ISO/IEC, 2018a).

Cybersecurity is becoming increasingly important as digital connectivity and dependency of organisations' raise and brings along the need for effective management of cybersecurity risks. The World Economic Forum publishes yearly global risk reports. In 2021, the global risk report listed cybersecurity failure among the top ten risks in terms of likelihood (McLennan & Group, 2021). As expected, we see the ongoing pandemic places the risk of infectious diseases on the top rank in terms of impact. The ongoing pandemic caused an increase in teleworking, which also raised concerns about the required security measures (Belzunegui-Eraso & Erro-Garcés, 2020). Cyber criminals, on several occasions, have taken advantage of vulnerable people and information systems throughout the pandemic (Pranggono & Arabo, 2021).

As the cybercrimes increase, policymakers and governments want to know the impact of these crimes. The cost of cybercrimes is one of the critical figures. The United Kingdom (UK) government commissions yearly Cyber Security Breaches Surveys. In the 2021 version of this survey, 1419 UK businesses were interviewed. The average cost of all breaches or attacks identified in the last 12 months is reported as £8,170 for micro/small organisations and £13,400 for medium/large organisations identifying breaches with an outcome. These figures highlight that cyber security breaches and attacks can do substantial financial damage to smaller businesses as well as larger ones. The survey report also emphasises that due to the COVID-19 pandemic, new ways of working were introduced, making cybersecurity more complicated for many organisations (Mori, 2021). In a 2019 article, global cybersecurity spending was predicted to exceed $1 trillion from 2017 to 2021 (Morgan, 2019). Recently, this spending is predicted to exceed $1.75 trillion from 2021 to 2025. The increase in the figures is partly attributed to the dramatic change that the COVID-19 pandemic has wrought (Braue, 2021). Cybersecurity maturity assessment and standardisation can be used by organisations to set up, maintain and improve their cybersecurity in these challenging times.

We refer to *cybersecurity maturity assessment* as assessing organisational cybersecurity capabilities based on a reference model and to *cybersecurity standardisation* as adopting best cybersecurity practices based on international standards. Cybersecurity

maturity assessment and cybersecurity standardisation have well-acknowledged benefits (Le & Hoang, 2016); (Siponen & Willison, 2009). The former enables organisations to benchmark their cybersecurity capabilities and plan to acquire the missing capabilities. The latter helps organisations manage their risks, build trust, and incorporate good cybersecurity practices into their business.

1.1.1 Cybersecurity Maturity Assessment

Maturity models have been used to assess the maturity of organisations in different domains since it was introduced by the Software Engineering Institute of Carnegie Mellon University (Paulk, Curtis, Chrissis, & Weber, 1993). In the Capability Maturity Model (CMM) for Software, the authors address the reader and explain how the model can be used. This "To The Reader" section of the well-known maturity model properly demonstrates the main objectives of using maturity models, such as "to understand the key practices that are part of effective processes", "to identify the key practices that are needed to achieve the next maturity level" (Paulk et al., 1993). Since effectiveness and maturity is important not only in the software development domain, the concept of maturity modelling has been adopted, and many instances of maturity models in domains other than the software engineering domain evolved in the literature (Rosemann & Bruin, 2005; Becker, Knackstedt, & Pöppelbuß, 2009).

Although maturity models have different constructs, structures, and characteristics, their objective is often to assess the maturity of an organisation in a particular functional domain through assessing its processes' capabilities (de Bruin, Freeze, Kulkarni, & Rosemann, 2005). Maturity models adopt the structure of CMM for software and typically include maturity levels that indicate process capability, key process areas, and key practices. Maturity models quite commonly use a five-point Likert scale of maturity levels starting from the lowest (e.g., initial) to the highest (e.g., optimising). There are also maturity models in the literature that do not focus on process capability but other capabilities (e.g., people capability (Nonaka, 1994; Curtis, Hefley, & Miller, 2009)). Cybersecurity, a challenge in any contemporary organisation, has received attention in terms of maturity assessment (Le & Hoang, 2016; Rabii, Assoul, Ouazzani Touhami, & Roudies, 2020).

Maturity assessment models have been investigated as design science research artifacts (Mettler, 2009). In design science research, Jones & Gregor (2007) propose artifact mutability which is the adaptability of DSR artifacts as one of the components of design theories. Winter (2011) refers to the design of adaptable artifacts as situational artifact construction (SAC) and argues that SAC allows the researcher to develop artefacts which are adaptable to different design problems within a problem class, and to understand the relevant design situations within this class. As the costs for adapting a more generic solution artifact to a specific design problem are higher than those for adapting the more specific solution artifact, developing situational artifacts reduces the cost of adaptation (Winter, 2011). Gregor & Iivari (2007) introduce the term "semizoa" to define design artifacts that exhibit the characteristic of mutability to some degree, that is, they grow, change (or are changed), and exhibit adaptive behaviour. Adaptive maturity models are also referred to as *situational maturity models* (Mettler & Rohner, 2009). In their study, Mettler & Rohner (2009) argue that it is crucial for maturity models with the intention of organizational engineering to consider the situational characteristics and/or to define configuration parameters to extend the focus of the maturity model for its audience. In maturity assessment model design

research, adaptivity is investigated as part of design principles (Pöppelbuß & Röglinger, 2011). Pöppelbuß & Röglinger (2011) introduces design principles that are related to the adaptivity of maturity models: "Advice on the adaptation and configuration of criteria", "Advice on the concretization and adaption of the improvement measures", and "Advice on the adaptation and configuration of the decision calculus" as design principles for maturity models to address different situational characteristics.

Maturity assessment models have three purposes of use: descriptive, prescriptive, and comparative. These purposes of uses explain why organisations opt to use the models as per their requirements. Maturity models' use for evaluating the as-is situation is referred to as the *descriptive purpose of use*. A maturity model can be used to identify desirable maturity levels and the improvement steps to reach these levels, which is considered as the p*rescriptive purpose of use*. Finally, for *comparative purpose of use*, maturity models are considered internal and external benchmarking tools (Pöppelbuß & Röglinger, 2011). When using maturity models for comparative purposes, in terms of adaptive maturity models, comparing assessment results can be done within a set of organisations that have similar characteristics. Group of organisations having similar characteristics can be considered as different design situations thus different design problems in a problem class. Comparing assessment results of organisations that have similar characteristics can yield more meaningful outcomes than comparing assessment results of completely disparate organisations.

In the organisational cybersecurity or information security research, researchers have investigated organisational characteristics' influence. The approach to organisational characteristics' falls into two major categories. The first category adopts an indicator-based approach (e.g. number of employees, revenue) (Mijnhardt, Baars, & Spruit, 2016) (Sánchez, Villafranca, & Piattini, 2006). The second category adopts an internal characteristics based approach (Yigit Ozkan & Spruit, 2020) (Heidt, Gerlach, & Buxmann, 2019). Parkin, Fielder, & Ashby (2016) identify archetype organisations (i.e. SMEs) based on size, network design (i.e. infrastructure) and daily interactions (i.e. user-IT system interactions) for identifying a set of security controls per archetype.

In terms of adaptivity of cybersecurity solutions and standards, organisations' roles (e.g., Small and Medium-sized Enterprises (SMEs)) in the digital ecosystem play an important role (The European Digital SME Alliance, 2020a). It is clear that the cybersecurity requirements of organisations that provide cybersecurity solutions are different from that of only end-users of digital solutions. However, the research in adaptivity of cybersecurity maturity models lacks investigating this phenomenon.

Table 1-1 presents a summary of the research on adaptive cybersecurity maturity assessment and the adaptivity approach that is followed in these researches.

Research Article	Adaptivity Approach
(Sánchez et al., 2006)	Indicator based; such as the number of employees, the annual turnover.
(Sánchez, Villafranca, & Piattini, 2007)	- Indicator based; such as the number of employees, the annual turnover. - The nature of business processes such as the level of enterprise dependency on I.S. outsourcing.
(Cholez & Girard, 2014)	- Selection of interviewees - Questions' vocabulary and the depth of details requested during the interview.
(Mijnhardt et al., 2016)	- Indicator based; such as the number of employees, revenue. - The nature of business processes such as outsourcing of or complexity in information technologies.
(Yigit Ozkan & Spruit, 2020)	Internal characteristics based; such as lack of organizational capabilities, short-term vision, and orientation
(Benz & Chatterjee, 2020)	Only one set of selected assessment criteria based on the researchers' with risk-reduction evaluation. The same set is used for all SMEs.

Table 1-1 Adaptivity Approaches in Cybersecurity Maturity Modelling Research

This dissertation focuses on the organisational context affecting cybersecurity needs from three different perspectives. First, we consider organisational characteristics (or indicators) such as revenue and the number of employees. Then, we focus on internal organisational characteristics such as lack of organisational capabilities, short-term vision and orientation. Finally, we focus on the phenomenon of organisations' roles in the digital ecosystem, such as digital solution providers and end-users of digital solutions. We investigate the effects of organisational situations on the needs, goals, and requirements of the stakeholders in cybersecurity maturity assessments.

1.1.2 Cybersecurity Standardisation

Standards offer several benefits to organisations, such as increased competitiveness and access to markets, reduced costs, and increased efficiency. Cybersecurity standards help improve the security capabilities based on best practices and conformance requirements (Scarfone, Benigni, & Grance, 2009). As a means of improving cybersecurity, cybersecurity standardisation is our second focus within the cybersecurity domain. Even though many organisations (e.g. the Internet Engineering Task Force (IETF), the Open Group) are committed to and promote open standards, most standards are not free. This can be challenging for organisations that lack enough resources, such as Small and Medium-Sized Enterprises (SMEs). Another challenge is the resources needed to implement standards.

These two challenges induce the need for the adaptivity of standards. Few standards were developed with the concern of adaptivity in standard development processes. Some examples–all published by ISO–are in the environmental management (ISO, 2019b), innovation management (ISO, 2019c), and human resources management (ISO, 2018a) domains.

There are international standards developing organisations such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU). In addition, there are regional and national standards developing organisations. Some examples of regional standard developing organisations are the International Telecommunication Union (ETSI) and the European Committee for Standardization (CEN) in Europe. There are also national standards developing organisations such as the Royal Netherlands Standardization Institute (NEN) in the Netherlands. The international, regional and national standards developing organisations work in collaboration to ensure varying needs of different stakeholders. ISO and IEC published a guide for writing standards considering the needs of micro, small and medium-sized enterprises (ISO/IEC, 2016). In Europe, an alliance of digital SMEs, the Digital SME Alliance (2021) represents more than twenty thousand SMEs. It is an SME organisation that represents and defends SMEs' interests in the standardisation process at European and international levels (SBS, 2021).

There is an abundance of cybersecurity and information security standards. The European Cybersecurity Organisation (ECSO) published an overview of existing cybersecurity standards and certification schemes (ECSO, 2017). In ISO, the ISO/IEC joint technical committee 1 (JTC1) and their subcommittee 27 specialises in information security, cybersecurity, and privacy protection standards. According to ISO's JTC1 standard catalogue, this subcommittee has published 212 standards, and 78 standards are under development (ISO, 2021). The substantial volume of standards makes it difficult for organisations to find out where to start. This is significantly more difficult for SMEs. Even if they know where to start, there is always the challenge of adopting the standards that were predominantly developed for and in collaboration with large enterprises. This is why involving SMEs in the standard development processes is important.

1.2 Problem Statement

Understanding the problem space is crucial to propose purposeful artifacts to unsolved problems (Hevner, March, Park, & Ram, 2004). In this dissertation, we investigate the problem space mainly by conducting a literature search and a workshop with various cybersecurity staheholders. This enables us to understand the key concepts of the problem space as conceptualised by Maedche, Gregor, Morana, & Feine (2019) and illustrated in Figure 1.1.

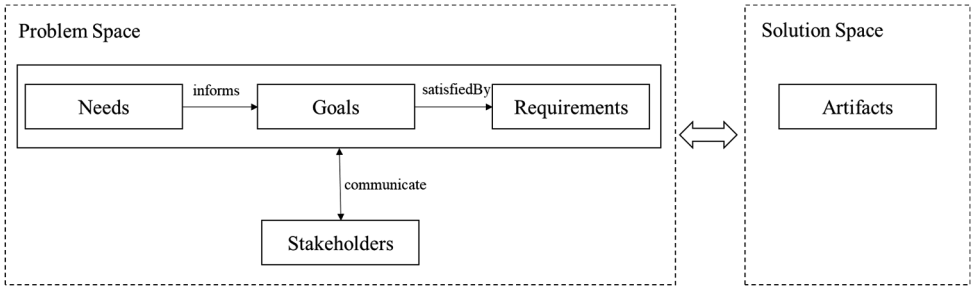


Figure 1.1 Conceptual Model of Problem and Solution Space (Maedche et al., 2019)

Understanding the problem space is interconnected with the artifact's design (Purao, 2013). The conceptual model of Maedche et al. presents what is needed to be known in the problem space to propose a solution (i.e., design artifact). The key concepts used to identify the problem space are stakeholders, needs, goals, and requirements (Maedche et al., 2019). **Needs** state what is desired or wanted as perceived by the stakeholders. **Goals** represent the desired result and describe the intentions of stakeholders. **Requirements** are derived from the needs and goals, and they present a condition or capability needed by the stakeholders. Finally, **stakeholders** are people or organisations involved in the development of the artifacts or affected by the development of the artifacts.

Using the conceptual model in Figure 1.1, we investigate the problem space and propose artifacts to address the problems identified in the problem space. Accordingly, the key concepts of the problem space, the thesis chapters in which they are investigated, and the artifacts we developed in the solution space are presented in Figure 1.2.

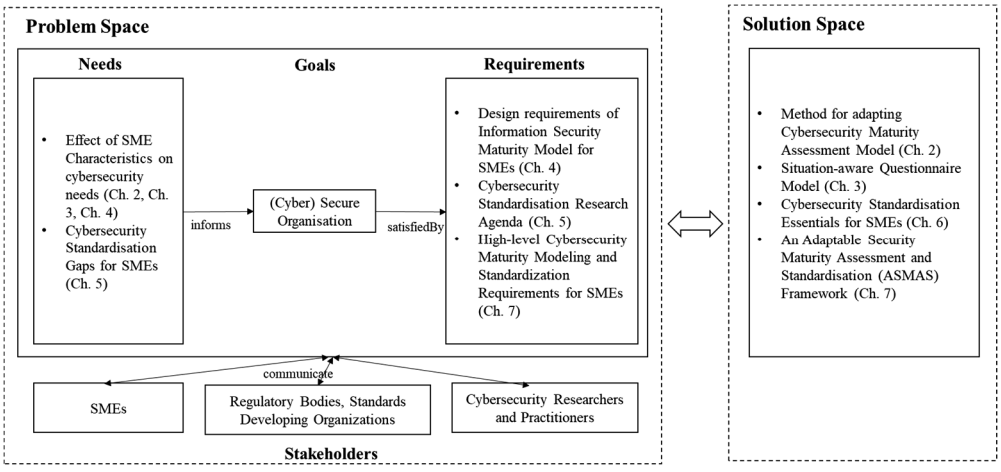


Figure 1.2 Problem Space and Solution Space (based on (Maedche et al., 2019))

In the following, we articulate the four key concepts of our research.

Stakeholders: Small and Medium-Sized Enterprises (SMEs) are the main stakeholders in our research. We consider SMEs as identified by the criteria defined by the European Commission (European Commission, 2016). SMEs are the main drivers of

economic growth; they represent 90% of businesses and more than 50% of employment worldwide (World Bank, 2021). According to 2017 data, 43% of cyberattacks target small businesses, and they were affected by 54,000 ransomware incidents in the United States. The average amount demanded during a ransomware attack was $1,077 – but the average cost to businesses was $133,000 (SCORE, 2018). Although SMEs deal with similar level of risk to large organisations, they are inclined to not to prioritise cybersecurity or information security (Kurpjuhn, 2015), Regulatory bodies such as governments and commissions impose regulatory requirements regarding cybersecurity. Standards developing organisations revise exiting standards to reflect emerging cybersecurity standardisation requirements and develop new standards. Other stakeholders are cybersecurity researchers and practitioners to whom we communicate our research results and future research proposals. We investigate the identified stakeholders' needs, goals, and requirements in the chapters presented in Figure 1.2.

Needs: To identify the needs of the stakeholders, in Chapters 2, 3, and 4, we focus on the organisational characteristics of SMEs that trigger different needs in terms of cybersecurity maturity assessment and standardisation. In Chapter 5, we dive deep into standardisation needs and identify groups of stakeholders. We organise a workshop to identify the cybersecurity standardisation needs and gaps collaboratively.

Goals: In our research, the ultimate goal is to establish and improve (cyber) secure organisations. We consider secure organisations as organisations that implement cybersecurity practices in accordance with their organisational context, characteristics, digital roles in the ecosystem, and risks. We investigate this goal in two parts, through cybersecurity maturity assessment and cybersecurity standardisation.

Requirements: To translate the needs and goals of the stakeholders, we identify requirements in the problem space in Chapters 4, 5, and 7. Chapter 4 presents the design requirements for information security maturity models to address SME characteristics. Chapter 5 presents a research agenda on cybersecurity standardisation for SMEs. In Chapter 7, we identify the high-level requirements of SMEs in cybersecurity maturity assessment and standardisation.

Having described the problem space, we present our research objective as follows:

To support the improvement of organisations' cybersecurity through maturity assessment and standardisation.

1.3 Research Questions

In Section 1.2, we identified SMEs as the main stakeholders of our research. Although cybersecurity maturity assessment models and standards are mostly designed for large enterprises, in Section 1.1 we touched upon the related research on adaptivity of maturity models and standards by SMEs. Maturity models have the basic design principle of "Definition of central constructs related to the application domain" (Pöppelbuß & Röglinger, 2011). If the application domain has achieved a level of maturity to have published standards by standards developing organisations, these standards can be used as sources for defining domain specific constructs of the maturity model (Shrestha, Cater-Steel, Toleman, & Rout, 2018). A maturity assessment model having constructs based on standards in the application

domain can help organisations in both their maturity improvement and standardisation efforts simultaneously. Such maturity assessment models integrate maturity assessment and standardisation in the same tool (design artifact). Organisations using the maturity assessment model to improve their cybersecurity would be able to adhere to (or adopt) the standards in the application domain.

To achieve our research objective as described in Section 1.2, our research questions to guide our research are organised in three parts. The first part focuses on adaptivity in cybersecurity maturity assessments. The second part focuses on cybersecurity standardisation. The third part focuses on the integration of cybersecurity maturity assessments and standardisation. Before explaining the research questions (RQ) in these three parts, we pose our main research question (MRQ) as follows.

MRQ: *How can we integrate cybersecurity maturity assessment and cybersecurity standardisation to provide tailored support for organisations in their cybersecurity improvement efforts?*

We pose this research question as an overarching question to guide our research. This research question guides us to understand the problem space (needs, gaps, requirements, and stakeholders) and envision our design artifacts in the solution space.

Part 1: Research questions related to the adaptivity of cybersecurity maturity assessments to different organisational contexts and characteristics.

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

With this research question, we investigate a method to adapt an existing maturity model to the context of organisations in the empirical study. As the organisational characteristics and context drive the needs, goals, and requirements for cybersecurity, in this work, we conduct a survey to collect organisational characteristics that can affect the factors in the problem space and propose a method to achieve an adapted maturity model.

RQ2: *How can we design an instrument for the assessment and improvement of cybersecurity capabilities with implementation guidance while taking into account the organisational characteristics?*

We investigate how to design a situation-aware cybersecurity assessment instrument with this research question. We demonstrate the assessment instrument through a critical infrastructure example. As elaborated in the Conclusion chapter, the assessment instrument was then adapted to SMEs. A situation-aware assessment instrument aims to achieve a dynamic maturity assessment that adapts according to the context of the organisation or entity being assessed.

RQ3: *What information security maturity model design requirements can be drawn by considering SME characteristics and the design principles of maturity models?*

The design of a maturity model affects the applicability of the model as the product of the design effort and design decisions. With this research question, we investigate the factors to be considered in designing information security maturity models to address SME

characteristics. We investigate the design requirements to be addressed by information security maturity models to be applicable to SMEs.

Part 2: Research questions related to cybersecurity standardisation.

RQ4: *What are the gaps in cybersecurity standardisation for SMEs?*

With this research question, we investigate the trends in the literature on cybersecurity standardisation research focusing on SMEs. We identify the stakeholders in SME cybersecurity standardisation and conduct a workshop to identify the needs and gaps collaboratively.

RQ5: *What are the cybersecurity standardisation essentials for SMEs considering their diverse roles in the digital ecosystem?*

This research question focuses on SMEs and their diverse roles in the digital ecosystem. Although enterprises are categorised as micro, small, medium, and large according to some indicators such as the number of employees and revenue, they have different cybersecurity requirements. The requirements are fundamentally altered by the organisation's role in the digital world. An SME providing cybersecurity solutions has different requirements than an SME that only uses some digital services with a limited scope.

Part 3: Research questions related to integrating adaptive cybersecurity maturity assessment and standardisation.

RQ6: *How can security maturity assessment and standardisation be integrated into an adaptive instrument to support concurrent implementation efforts of digital SMEs?*

This research question investigates the high-level SME requirements and the aspects to be included in an integrated security maturity assessment and standardisation framework to address these requirements. When studying this RQ, we use the findings from RQ3 (design requirements), RQ4 (standardisation needs and gaps), and RQ5 (cybersecurity essentials).

RQ7: *What is the perceived usefulness, ease of use, and intention to use such an integrated cybersecurity maturity assessment and standardisation framework for SMEs?*

With this research question, we investigate the perceived usefulness, ease of use, and intention to use the integrated framework proposed to answer RQ6.

1.4 Research Scope

Our research questions presented in Section 1.3 have three main purposes as presented by Thuan, Drechsler, & Antunes (2019): 1) defining the research scope, 2) guiding the research process, and 3) positioning the contributions. In Section 1.3, we present how our research questions guided our research. Section 1.6 presents how we position our contributions to answer the research questions.

As explained in Section 1.2, SMEs are the main stakeholders in our research thus; our research mainly investigates adaptivity for SMEs. The only exception is the investigation of critical infrastructures' characteristics for demonstration purposes in Chapter 3. Therefore, we have chosen a broader scope for our project and this is reflected in the title of the thesis. This section presents how our research questions define the scope of this Design Science Research (DSR) project. The shaded areas in Figure 1.3 illustrate the scope of our DSR project in the cybersecurity application domain. We predominantly focus on cybersecurity standardisation, cybersecurity maturity assessment, and adaptivity in cybersecurity in the cybersecurity domain. The shaded intersections of these sub-domains show our research focus.

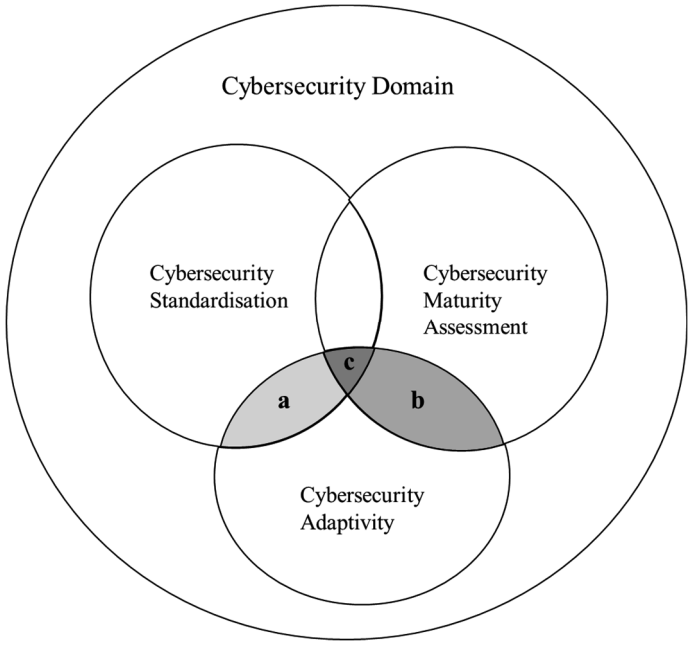


Figure 1.3 Research Scope (shaded areas)

Our research focus consists of the shaded areas *a, b* and *c* as depicted in Figure 1.3. Area *a* is the intersection of cybersecurity standardisation and adaptivity. With this focus, we investigate the adaptivity of cybersecurity standards to organisations characteristics for cybersecurity standardisation. Area *b* is the intersection of cybersecurity maturity assessment and adaptivity. Organisations use maturity assessment models for assessing and improving their cybersecurity capabilities. With this focus, we investigate the adaptivity of cybersecurity maturity assessment models to organisations characteristics for assessing and

improving cybersecurity capabilities. Area *c*, is the intersection of cybersecurity standardisation, maturity assessment and adaptivity. With this focus, we investigate the idea of the adaptivity of cybersecurity maturity assessment that also facilitates standardisation.

Revisiting our research questions, *Table 1-2* presents the corresponding research scope (see Figure 1.3) we focus on with each question.

Ch.	SRQ	Short Description	Research Scope
2	1	Adapting an ISMM	b
3	2	Questionnaire Model	c
4	3	Design Requirements	b
5	4	Standardisation Gaps	a
6	5	Cybersecurity Standardisation Essentials	a
7	6	Integrated Framework	c
7	7	Evaluating the Framework	c

Table 1-2 Research Questions and Research Focus

The characters in the last column represent the shaded areas of research focus in Figure 1.3.

Figure 1.4 presents the research questions (simplified for readability) organised in three parts. To complement the research questions, the research objective introduced in Section 1.2 is also presented in Figure 1.4.

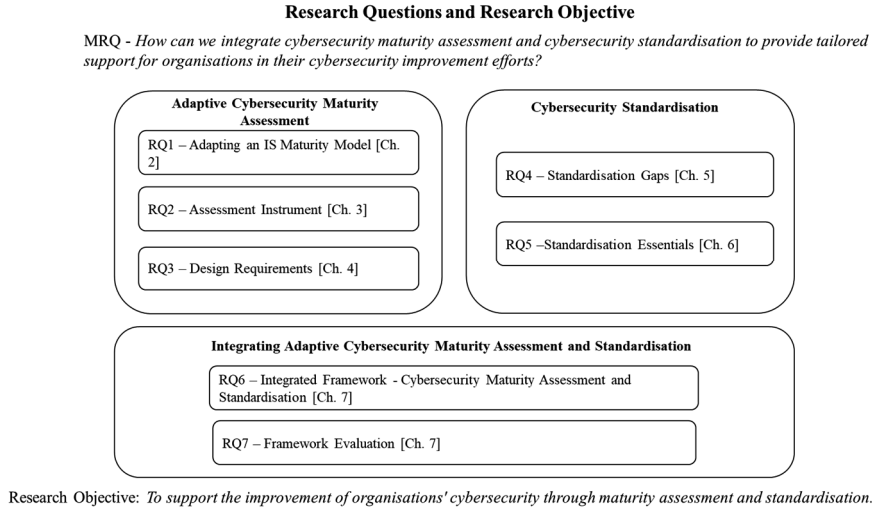


Figure 1.4 The Research Questions' Categorisation and the Research Objective

1.5 Research Framework

We used the Design Science Research (DSR) paradigm as our research approach. DSR deals with designing artificial products to solve an information systems problem. Hevner et al. proposed a conceptual framework for design research in information systems (Hevner et al., 2004). The design science framework has three research cycles: relevance cycle, design cycle, and rigor cycle. Figure 1.5 presents our research framework based on (Hevner et al., 2004). The research questions that guided our research are presented in Section 1.3.

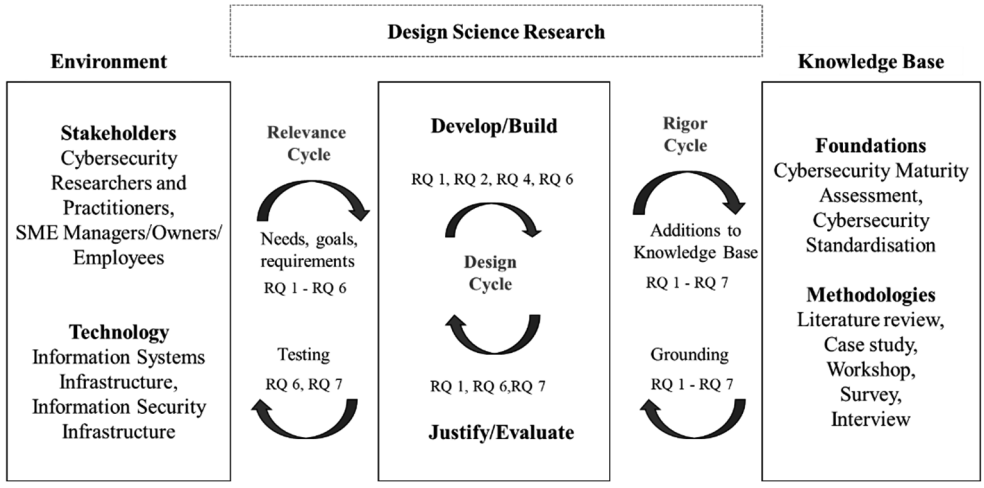


Figure 1.5 Research Framework of the Thesis

The following paragraphs explain these cycles and how they are applied in this dissertation, including the relationship between the cycles and our research questions.

Relevance Cycle: We identify opportunities and problems in the application environment in the relevance cycle. This process relates to identifying the problem space as presented by (Maedche et al., 2019). Reiterating from Section 1.2, the key concepts in the problem space are needs, goals, requirements, and stakeholders. Testing the proposed artifacts in the application environment is part of the relevance cycle and provides inputs to the next iteration of the cycle (Hevner, 2007).

Research questions 1 to 6 investigate the needs, gaps, requirements, and stakeholders in our application environment in the relevance cycle. The findings are used as input to our design cycle and used to develop and build the corresponding design artifacts. Research questions 6 and 7 are used for testing purposes in the relevance cycle.

Design Cycle: The design cycle receives input (needs, goals, requirements, stakeholders, and testing findings) from the environment and input from the knowledge base through the state-of-the-art in the application domain, design and evaluation theories, existing artifacts, and processes (Hevner, 2007; Maedche et al., 2019). In the design cycle, we develop artifacts and other contributions to the knowledge base and iteratively evaluate the artifacts by using the inputs mentioned above.

In the design cycle, using research questions 1, 2, 4, and 6, we develop and evaluate the artifacts presented in this dissertation. The research to answer research questions 1, 6, and 7 includes evaluation activities.

Rigor Cycle: Research rigorousness lies in grounding the research activities in the knowledge base. Hevner points out that the inspirational sources for design science could be extended to include other creative insights (Hevner, 2007). We argue that this promotes the creativity of researchers and the novelty of design products and processes. The rigor cycle includes applying scientific theories and methods, experience, and practice during the development and evaluation research activities in the design cycle. Design theories in information science, also known as theories on design and action are considered as theorized knowledge (i.e. guidelines and principles) that can be followed in practice (Gregor, 2002) (Goldkuhl, 2004).

In the rigor cycle, we explored existing theories, experiences, design products, and processes related to cybersecurity maturity assessment and standardisation, specifically investigating their adaptivity to different organisational contexts. We selected and applied appropriate theories and methods to design and evaluate our artifacts. In the maturity assessment research, there are design theories that can help in practice which we used in our research. The design principles of maturity models proposed by Pöppelbuß & Röglinger (2011), research design steps proposed by Mettler (2011), the method for designing focus area maturity models proposed by Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers (2010) are the main design theories we adopted during this thesis. In addition, we used design theories on design principles, such as the guidelines supporting the formulation of design principles (Cronholm & Göbel, 2018), and the characteristics of effective design principle formulation (Chandra, Seidel, & Gregor, 2015).

We discussed the artifact mutability in the context of adaptivity in our research in Section 1.1. Here, we want to focus on the evaluation of artifact mutability. Pöppelbuß & Goeken (2015) discuss two distinct perspectives on artifact mutability: (1) as the purposeful design of adaptable artifacts (in-design) and (2) the evolution of artifacts (in-use) over time based on the proposition of Sjöström, Ågerfalk, & Lochan (2011). Mutability-in-design refers to designing artifacts that are adaptable to various organizational contexts. Mutability-in-design is discussed as adaptivity in this dissertation. Pöppelbuß & Goeken (2015) investigate and define mutability dimensions per design artifact type (i.e., construct, method, model, instantiation). The adaptivity focus in our reseach project is related to “mechanism type” mutability dimension for model type of artifacts. This dimension has “configuration” and “adaptation” categories. An example of configuration mechanisms is the selection of a set of security controls according to the predefined organisational contexts. Mutability-in-design can be evaluated analytically (i.e. static analysis (Hevner et al., 2004)) as mutability will be part of the artifact structure.

In this dissertation, we employ the DSR methodology and use literature review, case study, workshop, survey, and interview research methods. All research questions (RQ 1 - 7) produce new knowledge. Figure 1.6 presents our research questions and corresponding produced knowledge. The produced knowledge in Figure 1.6 is elaborated in Section 1.6.

			Produced Knowledge							
Ch.	RQ	Short Description	Model	Method	Framework	Prototype	Design Requirements	Research Agenda	Guideline	Evaluation Results
2	1	Adapting an IS Maturity Model		✓						✓
3	2	Assessment Instrument	✓							
4	3	Design Requirements					✓			
5	4	Standardisation Gaps						✓		
6	5	Standardisation Essentials							✓	
7	6	Integrated Framework	✓		✓	✓				✓
7	7	Framework Evaluation								✓

Figure 1.6 Research Questions and Additions to Knowledge Base

1.6 Dissertation Outline and Research Significance

This dissertation consists of 8 chapters. Chapter 1 is the introduction in which we provide the research background, our motivation, problem statement, research questions, and research approach. The main body of the dissertation is presented in three sections. Section 1 is titled "Adaptive Cybersecurity Maturity Assessment", Section 2 is titled "Cybersecurity Standardisation", and Section 3 is titled "Integrating Adaptive Cybersecurity Maturity Assessment and Standardisation".

DSR projects may have different types of contributions to the knowledge base. Descriptive knowledge and prescriptive knowledge are considered the two overarching types of contributions in DSR (Gregor & Hevner, 2013). Descriptive knowledge is "the *what* knowledge about natural phenomena and the laws and regularities among phenomena," and prescriptive knowledge is "the *how* knowledge of human-built artifacts" (Gregor & Hevner, 2013). Drechsler & Hevner (2018) also distinguish the project design knowledge that is "project-specific, possibly untested, conjectural, and temporary" from descriptive and prescriptive knowledge.

Our knowledge contribution in this dissertation is predominantly prescriptive, presenting guidance on the steps to be followed by the stakeholders of our DSR project. Drechsler & Hevner (2018) point out two sub-categories of knowledge contributions as prescriptive: solution design knowledge and solution design entities. Solution design knowledge comprises technological rules, requirements, principles, features of design artifacts, and knowledge for design processes and systems (e.g., methodological contributions) (Drechsler & Hevner, 2018).

We present our knowledge contributions per dissertation chapters as follows and comment on our contributions' position in the view of the conceptual framework proposed by Drechsler & Hevner (2018).

Section 1, "Adaptive Cybersecurity Maturity Assessment," consists of the following chapters.

In Chapter 2, Adaptive Cybersecurity Maturity Assessment, we investigate the applicability of an existing information security maturity model to SMEs in a cluster at the Port of Rotterdam. This chapter proposes a method to adapt a maturity model to a group of SMEs with the aim of collective and collaborative improvement of information security capabilities. In this empirical study, we propose a tailored maturity model according to the characteristics of the SMEs in the cluster. This research presents an example of how a maturity assessment

model that is adapted to organisational characteristics can be used as a benchmarking tool (comparative purpose of use of maturity models (Pöppelbuß & Röglinger, 2011)) for a group of organisations. The adapted maturity model can be used to compare maturity levels of the SMEs in the cluster and can support collective learning. In this research, we approached adaptivity by identifying the maximum maturity level applicable to an organisational context. By knowing the maximum level of maturity, the target organisations will have the optimum set of capabilities that fits their characteristics. This approach addresses the "Advice on the adaptation and configuration of criteria" design principle of maturity models. The adapted maturity model in this research serves descriptive, prescriptive and comparative purposes of uses of maturity models (Pöppelbuß & Röglinger, 2011). We consider this contribution as a design (meta-) artifact.

Chapter 2 is published as Yigit Ozkan, B., Spruit, M., Wondolleck, R., & Burriel Coll, V. (2019). Modelling adaptive information security for SMEs in a cluster. Journal of Intellectual Capital, 21(2), 235–256. DOI: 10.1108/JIC-05-2019-0128.

In Chapter 3, Situation-Aware Cybersecurity Maturity Assessment, we focus on situational awareness as part of adaptivity and propose an assessment instrument for situation-aware maturity assessments. The proposed assessment instrument is dynamic, and the flow of the assessment questions alters according to the context of the organisation being assessed. The assessment instrument differentiates the assessment questions that question cybersecurity capabilities from the questions about the organisational context. The answers given to the questions about the organisational context affect the capability assessment questions. The questionnaire model can be used in designing adaptive maturity assessment models that serve descriptive, prescriptive and comparative purposes of uses of maturity models (Pöppelbuß & Röglinger, 2011). The model addresses the design principles related to the adaptivity of maturity models (see Section 1.1.1) by providing advice on adapting or configuring the assessment criteria and the improvement measures (tasks as defined in the model). The guidance on the selection of the improvement measures is embedded in the design of the model, as the answers to the focus are assessment questions trigger the required improvement measures (tasks). The questionnaire model was illustrated in a critical infrastructure context, which resulted in exemplar situational questions such as "What is the number of people supplied by the critical infrastructure?" which is related to the criticality of the infrastructure. As explained in the chapter, the questionnaire model can potentially be adapted to other organizational contexts. The questionnaire model was adapted to maturity assessment of SMEs in the SMESEC project (SMESEC, 2017). We elaborate on this adaption in the Conclusion chapter.

We consider this contribution as a design (meta-) artifact.

Chapter 3 is published as Yigit Ozkan, B., & Spruit, M. (2019a). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. In A. P. Fournaris, K. Lampropoulos, & E. Marín Tordera (Eds.), Information and Operational Technology Security Systems (pp. 49–60). Heraklion, Crete, Greece: Springer International Publishing, New York, USA. DOI: https://doi.org/10.1007/978-3-030-12085-6_5.

In Chapter 4, Organisational Characteristics Affecting Cybersecurity Maturity Assessment, we investigate how SME characteristics can be addressed for designing SME applicable information security or cybersecurity maturity models. In this work, we focus on

the internal characteristics of SMEs based on literature and investigate how these characteristics can be addressed concerning design principles of assessment models. As a result of this investigation, we propose 18 design requirements and map these design requirements to the design principles and internal SME characteristics. We consider this contribution as solution design knowledge.

Chapter 4 is published as Yigit Ozkan, B., & Spruit, M. (2020). Addressing SME Characteristics for Designing Information Security Maturity Models. In N. Clarke & S. Furnell (Eds.), Human Aspects of Information Security and Assurance (pp. 161–174). Cham: Springer International Publishing, New York, USA. DOI: 10.1007/978-3-030-57404-8_13.

Section 2, "Cybersecurity Standardisation," consists of the following chapters.

In Chapter 5, Cybersecurity Standardisation Gaps for SMEs, we identify the gaps in cybersecurity standardisation for SMEs. We organise a workshop with relevant stakeholders (standardisation bodies, cybersecurity organisations, policymakers, and SMEs). The findings of this workshop and our literature search yield a research agenda on cybersecurity standardisation research for SMEs (Yigit Ozkan & Spruit, 2019b). We consider this contribution solution design knowledge since the research questions constitute knowledge for future design artifacts.

Chapter 5 is published as Yigit Ozkan, B., & Spruit, M. (2019b). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. International Journal of Standardization Research (IJSR), 17(2), 32. DOI: 10.4018/IJSR.20190701.oa1.

In Chapter 6, Cybersecurity Standardisation Essentials for SMEs, following the gaps identified in Chapter 5, we investigate and compare several standards and frameworks that are applicable to SMEs and propose cybersecurity standardisation essentials for SMEs according to their roles in the digital ecosystem (Yigit Ozkan & Spruit, 2021a). In this work, we first introduce the basic concepts of cybersecurity. Second, we provide a five-step process for cybersecurity risk management. Finally, we propose a unified set of controls to reduce cybersecurity risks from different standards and frameworks applicable to SMEs. We provide guidance on the set of controls that can be applied to different SME categories. This work puts all the information together for SMEs to start implementing cybersecurity in their organisations. As this work includes processes to be followed, we consider this contribution a design artifact (as presented by Drechsler and Hevner as artifact instances).

Chapter 6 has been accepted for publication as Yigit Ozkan, B., & Spruit, M. (2021) (In press). Cybersecurity Standardisation Essentials for European SMEs.", In Fricker, S., Ruiz, J.F., & Tselios, C. (Eds.), SMESEC: Protecting Small and Medium-sized Enterprises digital technology through an innovative cyberSECurity framework. Springer.

Additionally, the European Telecommunications Standards Institute (ETSI) has published an extended version of this chapter as ETSI technical report CYBER; Cybersecurity for SMEs; Part 1: Cybersecurity Standardization Essentials (Technical Report No. ETSI TR 103 787-1) (ETSI TC CYBER, 2021).

Section 3, "Integrating Adaptive Cybersecurity Maturity Assessment and Standardisation" consists of the following chapters.

In Chapter 7, ASMAS: An Adaptable Security Maturity Assessment and Standardization Framework for Digital SMEs, we propose a multi-aspect and adaptable cybersecurity maturity assessment and standardisation framework that supports different SME categories. The framework consists of the following aspects: risk management, standardisation, organisational, assessment and measurement, and improvement. We implement the framework with a software prototype to demonstrate its validity and technical feasibility. This work integrates cybersecurity maturity assessment and standardisation in one framework to facilitate efforts that aim for both cybersecurity assessment and improvement and standardisation concurrently. In this chapter, we further evaluate the proposed framework with SME representatives to determine its perceived usefulness, perceived ease of use and perceived intention to use. We propose an integrated cybersecurity maturity assessment and standardisation meta-model, framework, and prototype. We consider these contributions as design (meta-) artifacts. In this chapter, we also evaluate the proposed framework and present the results. We consider this knowledge as project design knowledge as a result of our evaluation actions in the solution space.

Finally, in Chapter 8, we conclude the dissertation by reiterating the research questions, summarising the findings and the contributions of our research, and discussing the limitations of our approaches. In the Conclusion section, we also provide insights into future research and close with personal reflections. In summary, we present our knowledge contributions per chapter in *Table 1-3*.

Ch.	RQ	Short Description	Knowledge Contributions (Drechsler & Hevner, 2018)	Contribution Type (Drechsler & Hevner, 2018)
2	1	Adapting an IS Maturity Model	A method for adapting an existing information security maturity model to SMEs in a cluster.	Solution design entity (Design (meta-) artifact)
3	2	Assessment Instrument	A situation-aware assessment instrument that enables adaptation of cybersecurity maturity assessments to organisational contexts.	Solution design entity (Design (meta-) artifact)
4	3	Design Requirements	The design requirements of an information security maturity model that addresses SMEs as its target audience.	Solution design knowledge
5	4	Standardisation Gaps	The cybersecurity standardisation gaps for SMEs and a research agenda to address the gaps.	Solution design knowledge
6	5	Standardisation Essentials	The cybersecurity standardisation essentials for SMEs.	Solution design entity (Design artifact)
7	6	Integrated Framework	An integrated cybersecurity maturity assessment and standardisation meta-model, framework, and a prototype	Solution design entity (Design (meta-) artifact)
7	7	Framework Evaluation	Evaluation results	Project design knowledge

Table 1-3 Knowledge Contributions and Their Types per Chapter in this Dissertation

SECTION 1 ADAPTIVE CYBERSECURITY MATURITY ASSESSMENT

2 Modelling Adaptive Information Security for SMEs in a Cluster

This paper presents a method for adapting an information security focus area maturity model to the organizational characteristics of an SME cluster. The purpose is to provide SMEs with a tailored maturity model enabling them to capture and improve their information security capabilities. Design Science Research was followed to design and evaluate the method as a design artifact. The method has successfully been used to adapt the information security focus area maturity model to a group of SMEs within a regional cluster resulting in a model that is aligned with the organisational characteristics of the cluster. Areas for further investigation and improvements were identified. 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. 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. This paper makes a contribution to the existing body of knowledge by proposing a method for tailoring an information security maturity model according to the organizational characteristics of SMEs in a cluster.

This work was originally published as:

Yigit Ozkan, B., Spruit, M., Wondolleck, R., & Burriel Coll, V. (2019). Modelling adaptive information security for SMEs in a cluster. *Journal of Intellectual Capital, 21*(2), 235–256.

2.1 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 (WEF) has revealed that cyberattacks are in the top ten risks both in terms of likelihood and impact (World Economic Forum, 2018). 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, Ciere, & van Eeten, 2017).

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

Management of cybersecurity has many challenges both in technical and non-technical factors (Kayworth & Whitten, 2012). Many organizations struggle with cybersecurity not 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 cyber security 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 & Spruit, 2019a) (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 organisations 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 perspective, organisations assessing themselves utilising a maturity model can capture their related intellectual capital (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 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 organisations, many of these are not well suited for SMEs (Manso, Rekleitis, Papazafeiropoulos, & Maritsas, 2015). This is mainly because these tools are complex and require specialists to be hired in order to utilise 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 organisations, SMEs in this case (Cholez & Girard, 2014). Given these phenomena, utilisation of maturity models for self-assessing information security or cybersecurity capabilities can be a remedy for SMEs.

Lawson & 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 & 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: (1) intangible assets, (2) competencies and capabilities, and (3) 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 & 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 organisations.

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 model according to their differentiating sectoral organisational 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 improvement of organisational 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 personalised guidance on applying the maturity model and improving their capabilities.

The tailored model in our research is based on the Information Security Focus Area Maturity (ISFAM) model (Spruit & 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, Dinev, & Willison (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 & 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, Niehaves, Simons, & Becker, 2011) (Staples et al., 2007). Providing an adaptive method that accounts for organizational characteristics, 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:

> *"How can the focus area maturity model in information security be methodologically adapted to the organisational characteristics profiles of an SME cluster for focused 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, focus area maturity models, 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 information security focus area maturity 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.

2.2 Background and Related Research

In the simplest form, a maturity model provides a benchmark against which an organisation 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 CMM for software processes (Paulk et al., 1993).

A distinction can be made between the maturity modelling variants. First, staged 5-level models distinguish five levels of maturity. Each level has a number of focus areas defined specific for that level. An example of this is the CMM model, although many others exist. Second, continuous 5-level models are also based on five general maturity levels. However, the main difference with the staged 5-level models is that the focus areas are not attributed to a certain level. Third, focus area maturity models (FAMM) differentiate from the abovementioned 5-level models in that FAMMs have their own number of specific maturity levels for each focus area (Steenbergen, Berg, & Brinkkemper, 2007).

There are numerous works related to information security and cybersecurity maturity modelling. Some of these maturity models are given in Table 3-2.

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 organisation
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 & Roeling, 2014)	(Spruit & Roeling, 2014)	Any type of organisation

Table 2-1 Information and Cybersecurity Maturity Models

The first three models presented in Table 3-2 are characterised as maturity models where the last one is a focus area maturity model. In the following paragraphs, we briefly discuss these models.

The US Department of Energy (DOE), in collaboration with Carnegie Mellon University, USA, developed the Cybersecurity Capability Maturity Model (C2M2) from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (US Department of Energy, 2014, 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 focuses on the common processes of information security which most organizations share. O-ISM3 defines four levels of security processes as Generic Processes (GP), Strategic-Specific Processes (SSP), Tactical-Specific Processes (TSP), and Operational-Specific Processes (OSP). NICE (National Initiative for Cybersecurity Education) (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 & Roeling, 2014) is a focus area maturity model based on widely-implemented industry standards. The dependencies between the focus areas are presented to facilitate the implementation of improvement programs within the organisations. ISFAM model is elaborated in Section 2.2.3.

There have been other studies to address the maturity assessment and improvement of information security in SMEs (Cholez & 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 organisations 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.

2.2.1 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, Bos, Brinkkemper, van de Weerd, & Bekkers, 2010). Since the conceptualization of these models, Sanchez-Puchol & 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" (Alves, 2013), "Disaster Risk Management Focus Area Maturity Model" (Waldt, 2013) and the ISFAM model (Spruit & Roeling, 2014).

As the name suggests, the core of a FAMM consists of focus areas, which can be divided into a number of capabilities. As the capabilities within a 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 a complete coverage of the functional domain that is to be assessed.

Each focus area (most FAMMs consist of 12 to 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.

2.2.2 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 & Zubrow, 1995), the organisations were assessed during a 7 year period (1987 – 1994) using the CMM model. The researchers found that 73% of the assessed organisations 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, Mijnhardt, Vlaanderen, & Spruit (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 organisation, the standards and best practices used for information security are also targeted at such organisations. 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.

2.2.3 ISFAM: The Information Security Focus Area Maturity Model

The method we propose in this research builds on ISFAM model (Spruit & 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.

ISFAM model was proposed to help organizations, especially SMEs, achieve strategy-IT security alignment in ever changing security risk environments. 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 organisation still has to put processes and procedures in place. *Monitoring*, on the other hand, is considered the highest level, where an organisation 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 2.1 The Information Security Focus Area Maturity (***ISFAM***) model)

((Spruit & Roeling, 2014))

In this figure, the focus areas and the maturity levels for these focus areas are depicted. In (Spruit & Roeling, 2014) the dependencies found in the literature, which facilitates an implementation order for the capabilities, were also presented by the authors.

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 2.1 The Information Security Focus Area Maturity (ISFAM) model) ((Spruit & Roeling, 2014))

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 2.2.1.

2.2.4 Organizational characteristics influencing SME information security maturity

With the aim of profiling the characteristics of target SMEs, we used the OCs influencing SMEs' information security maturity (Mijnhardt et al., 2016). 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 2.2. Hereafter, the moniker CHOISS: CHaracterizing Organizations' Information Security for SMEs which was proposed by Mijnhardt et al. (2016) is used to refer to this research.

Organizational characteristic	Measurement levels
General company information	
Number of employees	0–9 employees, 10–49 employees, 50–250 employees
Organization's revenue	0–2 Million, 2–10 Million, 10–50 Million
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 x 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 2.2 Organisational Characteristics and Measurement Levels in CHOISS (Mijnhardt et al., 2016).

2.2.5 An analytics approach to adaptive maturity models using organizational characteristics

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, Mijnhardt et al. (2016) present the results including a granular level of measurement: the influence of organizational characteristics on the focus areas in ISFAM. We used the values of the importance of the focus areas identified in this research (the details of application are elaborated in Section 2.5.1). Hereafter, the moniker ANLYMM: An ANaLYtics approach to adaptive Maturity Models using organizational characteristics is used to refer to this research.

2.3 Research Method

This study is structured according to 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 DSR methodology described by Peffers, Tuunanen, Rothenberger, & Chatterjee (2007a) which consists of the following steps: (1) problem identification, (2) definition of solution objectives, (3) design and development, (4) demonstration, (5) evaluation and (6) 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 2.4. To provide a better understanding of our research context, we present our research framework adapted from (Hevner et al., 2004) in Figure 2.3.

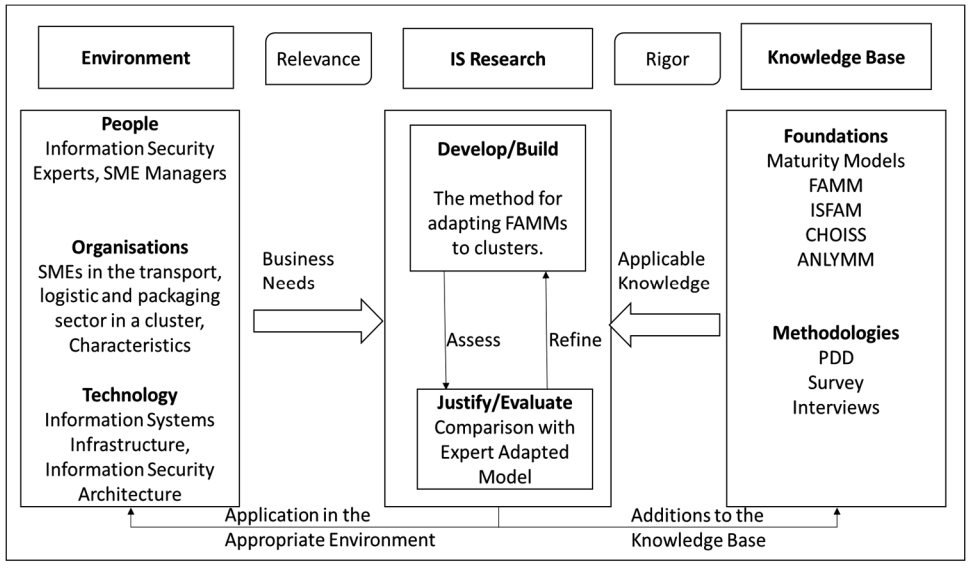


Figure 2.3 Research Framework .Adapted from (Hevner et al., 2004)

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 & Roeling, 2014), CHOISS (Mijnhardt et al., 2016) and ANLYMM (Baars et al., 2016) are elaborated in Section 2.2.

The practical value of a design study lies in its consideration for applicability beyond a single context-bound example (Williams & Pollock, 2012). A research criteria to assess the quality of design study results (e.g., design theories, principles, and artifact) from this pragmatic perspective is projectability (Baskerville & Pries-Heje, 2014) (Baskerville & 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.

2.4 Artifact Description

In this paper, we present the Method for Adaptive Information Security Maturity Modelling in Clusters (MAISMMC) that can be used to create an adapted information security FAMM based on OCs that represent the SMEs in a cluster. An overview of MAISMMC that results in an adapted information security FAMM model for a cluster is depicted in Figure 2.4.

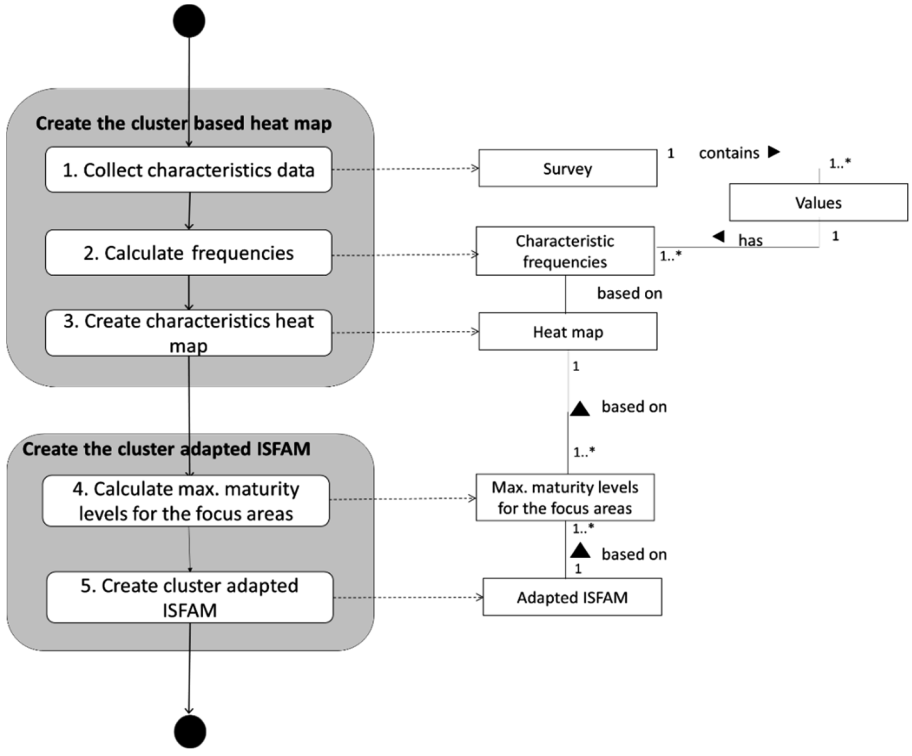


Figure 2.4 Method for Adaptive Information Security Maturity Modelling in Clusters (MAISMMC).

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

The notation used is a Process Deliverable Diagram (PDD) as described by van de Weerd & 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 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 dataset 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, Guo, Sheng, & Shyr, 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 2.5. 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 - 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.

2.5 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.

2.5.1 A Case Study: Application of MAISMMC for Port of Rotterdam SME cluster

To evaluate our method we conducted a case study in a SME cluster at the Port of Rotterdam area in the transport, logistic and packaging sector. In the following paragraphs, we elaborate 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 visualises the characteristics. The survey protocol, questions and possible answers are given in 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) was 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 organisations (which responded to our call) situated within the ecosystem of a large European sea port area, the Port of Rotterdam. The resulting deliverable from this step was the survey datasets, which served as input for the next step. Amongst the invited companies during a cybersecurity resilience event in the port area, 9 SMEs responded to our survey in the transport, logistics and packaging sector. The event was one of the bimonthly cybersecurity resilience events organised in the port in which participation is on 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 number of respondents was constructed. Two transformation steps have been applied to the SPSS dataset: first, the dataset has been reduced by means of case selection. The rule applied for case selection restricted the dataset to the results provided by the organisations active in the transport, logistics and packaging sector. Secondly, 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 organisations 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 2-2 depicts the heat map created based on the OC survey results from 9 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 *number of employees* 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 number of employees at SMEs is assumed as fewer than 250. Moreover, the criterion of the sector is assumed as transport, logistics and packaging sector. Table 2-2 is used further in this research to answer the research question given in Section 2.1. 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.

Organisational Characteristics Influencing SME Information Security Maturity (Mijnhardt et al., 2016)	Heat map of the Values Collected from the SMEs				
Amount of Revenue	0 – 2 million	2 – 10 million	10 – 50 million	> 50 million	
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 – 10 min	10 – 60 min	1 – 24 hr	> 24 hr	
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%

Table 2-2 Heat Map Visualizing the Organizational Characteristics of the SMEs within the Cluster

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 dataset from (Baars et al., 2016), which gave a general direction on which capabilities can be excluded. Based on the original survey dataset 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 2-2) for the SMEs in the cluster, we calculated the maximum maturity level per focus area as shown in Table 2-3.

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

A screenshot of the model with the OCs input according to the heat map (Table 2-2) is presented in Figure 2.5.

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 x 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, Logi	75-100%	75-100%	- 1 to 24 hours	- 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 2.5 Using the CHOISS Model to Calculate the Maximum Maturity Levels.

We applied the calculations based on the organisational profile of the SMEs in our case study as follows Every measurement level given in Figure 2.2 is identified by a unique number labelled as "Identifier" in Figure 2.5 which shows the respective number for the chosen identifier in the model. With the data set provided in the model, valuation for 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). The column A in Table 2-3 presents these values for each focus area for the OCs in the heat map. The column B in Table 2-3 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 was identified (Spruit & Roeling, 2014). These values are given in the respective columns C and D in Table 2-3. 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 2-3. This formula normalises the focus area's maturity level taking into account the percentage calculated according to the findings of Thijs Baars et al. (2016).

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 2-3 ISFAM Model Focus Areas and Adaptive Maximum Levels Calculated

Step 5: Create cluster adapted 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, logistic and packaging sector.

The resulting cluster adapted ISFAM model (CA-ISFAM) based on the heat map is depicted in Table 2-2**.**

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 2.6 The ClusterAdapted ISFAM Model Based on the OC Heat Map (CA-ISFAM).

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 2-3) therefore, the higher maturity levels are shown in red colour.

2.5.2 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 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 organisations 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 2-2. This was used by the experts to guide their reasoning about the suitability and achievability of the 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.

- 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 hours 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.

2.5.2.1 Expert Adaption Results

The results of both expert adaption sessions and the aggregated results are presented in Figure 2.7.

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.

		Maturity Levels												
ISFAM Model Focus Areas		**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 2.7 Individual and Aggregated Expert Adaption Results (AEAR).

The results presented in Figure 2.7 are further discussed in Section 2.6 with details per focus area.

2.6 Evaluation Findings and Discussion

In this section, we present the comparison of aggregated expert adaption results (AEAR) and cluster adapted ISFAM model based on the OC heat map (CA-ISFAM). The combined findings per focus area are shown in Figure 2.8.

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 2.8 Combined Results from the Aggregated Expert Adaption Results (AEAR) and the Cluster Adapted ISFAM Model (CA-ISFAM).

From the capabilities that are in the CA-ISFAM (Figure 2.6), 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 where 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 where 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. 7 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 5 capabilities have a neutral final score of 0. Lastly, 2 capabilities that could be omitted based on the calculations where 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 2.8, we presented these capabilities in colour in line with CA-ISFAM as they are not considered as concrete variations.

2.6.1 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 organisation 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.

For the focus area "secure software development", one expert argued that based on the OC heat map, all capabilities could be omitted (most organisations 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 & 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 is outsourced, this would also be sufficient to cover the incidents. Although the expert argues that it would be better if e.g. 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 where as 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. 4 of the differences are regarding the exclusion of the capabilities by the experts, 1 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.

2.7 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 & 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 an adapted information security maturity model for the target SME cluster.

We experimented our method with a specific focus area maturity model (ISFAM) which to our knowledge is the only focus area maturity model 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 visualises 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 intellectual capital. 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:

Firstly, our method can be adapted for developing methods for the generation of adapted FAMMs in SME clusters in other domains. Secondly, 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 focused 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 organisation 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 in 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 focuses on developing a unified, personalised and self-service information security and cybersecurity focus area maturity model specifically for SMEs.

Competing Interests

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

2.8 Appendix: Organisational Characteristics Survey Protocol and Questionnaire

Investigators

Roland Wondolleck, Utrecht University, Information and Computing Sciences Department.

Bilge Yigit Ozkan, Utrecht 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 of SMEs in transport, logistics and packaging sector. This survey is prepared to collect organisational characteristics of the SMEs in the Port of Rotterdam area.

Past work

Mijnhardt et al. (2016) have investigated the organisational characteristics influencing SMEs' information security maturity. Based on literature review and expert evaluations they have identified 11 organisational characteristics 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 organisational characteristics (Mijnhardt et al., 2016) data from the target SMEs to further construct an adapted ISFAM model (Spruit & Roeling, 2014) for a profile that represents the SME population in the sector.

Design

The survey has 11 questions. Each questions 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 program for cyber resilience. The aim of the program is to encourage cooperation 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 program 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 program. 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 (number of employees < 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 10 minutes.

Planned Statistical Analysis

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

Survey Questions

11 questions for the organizational characteristics and possible answers for these questions are listed below.

1. In which sector is your organization active?

- Aerospace & defense
- Professional services & finance

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

2. What is the amount of revenue of your organization?

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

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%
- 25 – 50%
- 50 – 75%
- 75 – 100%

5. What percentage of hosting / IT services is outsourced?

- 0 – 25%
- 25 – 50%
- 50 – 75%
- 75 – 100%

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 minutes
- 10 – 60 minutes
- 1 – 24 hour
- More than 24 hour

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%
- 1 – 3%
- 3 – 5%
- 5 – 10%
- More than 10%

3 A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures

Critical infrastructures are important assets for everyday life and wellbeing of the people. People can be effected dramatically if critical infrastructures are vulnerable and not protected against various threats. Given the increasing cybersecurity risks and the large impact that these risks may bring to the critical infrastructures, assessing and improving the cybersecurity capabilities of the service providers and the administrators is crucial for sustainability.

This research aims to provide a questionnaire model for assessing and improving cybersecurity capabilities based on industry standards. Another aim of this research is to provide service providers and the administrators of the critical infrastructures a personalized guidance and an implementation plan for cybersecurity capability improvement.

This work was originally published as:

Yigit Ozkan, B., & Spruit, M (2019). A Questionnaire Model for Cybersecurity Maturity Assessment for Critical Infrastructures. In Fournaris, A., Lampropoulos, K., & Tordera, E. (Eds.), *Lecture Notes in Computer Science (LNCS) 11398 11398*, *Information and Operational Technology Security Systems. First International Workshop, IOSec 2018, CIPSEC Project* (pp. 49–60). IOSec 2018, 13 Sept 2018, Heraklion, Crete, Greece: Springer.

3.1 Introduction

It is important to understand the relationship between different security domains. According to ISO 270032 (ISO/IEC, 2012), Information security is concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user. Whereas cybersecurity relates to actions that stakeholders should be taking to establish and maintain security in the cyberspace. Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks. The relationships between these security domains are shown in Figure 3.1.

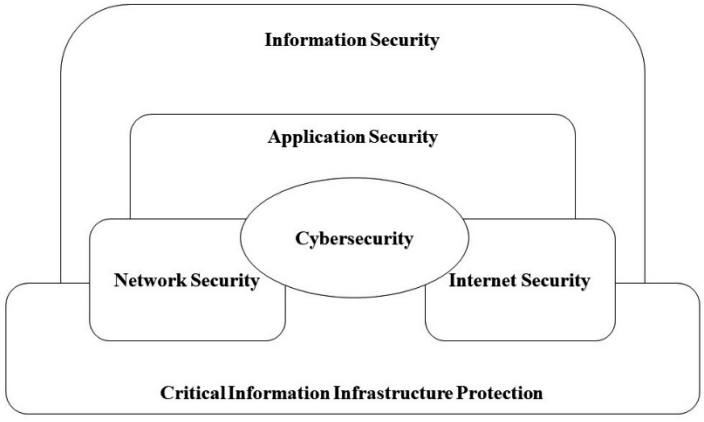


Figure 3.1 Relationships between Cybersecurity and Other Security Domains (redrawn from ISO/IEC 27032 (ISO/IEC, 2012)

Within the cybersecurity and information security domains, there are several subdomains. Subdomains may have different names in different sources but most of the time their scopes are similar. In this research, among the several subdomains of cybersecurity, the *Identity Management and Access Control* subdomain is selected as an example to demonstrate the proposed questionnaire model. Besides being part of the security standards, Identity Management and Access Control is also defined as a category in the Framework for Improving Critical Infrastructure Cybersecurity document published by NIST (National Institute of Standards and Technology, 2018). Identity Management and Access Control is a security discipline comprised of people, processes and technologies to manage identities and access to resources.

Many maturity models have been developed by academics or practitioners to assess domain specific capabilities. In section 3.2, we give some examples of maturity models including the information security and cybersecurity related ones. These information security

and cybersecurity maturity models are complex and comprehensive. They are not easy to implement for self-assessment and, therefore, suitable for preparing customized improvement plans. Another drawback of these information and cybersecurity maturity models is that they do not consider organizational characteristics. These inadequacies led us to our research question: 'How can we design a questionnaire to assess and improve cybersecurity capabilities with implementation guidance and taking into account the organizational characteristics?". Based on this research question, we propose a situational-aware questionnaire model for cybersecurity maturity self-assessment of critical infrastructures that also facilitates the generation of a customized improvement plan. The model and its components are described in depth in section 3.3.

Using the proposed questionnaire based self-assessment model the service providers or administrators of the critical infrastructures can identify areas of improvement and create a plan to improve its cyber security practices, thereby reaching a higher maturity level.

3.2 Background

3.2.1 Maturity Models

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. Maturity models in different domains have been developed and used mostly since they became popular after the introduction of the Capability Maturity Model (CMM) of the Software Engineering Institute (SEI) of Carnegie Mellon University (Paulk et al., 1993). Some maturity model examples for different domains are given in Table 3-1.

Maturity Model	Organization/ Authors
The Smart Grid Maturity Model (SGMM) ("Smart Grid Maturity Model, Version 1.2: Model Definition," n.d.)	CMMI Institute-SEI
Business Process Maturity Model ("About the Business Process Maturity Model Specification Version 1.0," n.d.)	OMG
People Capability Maturity Model ("People CMM: A Framework for Human Capital Management (SEI Series in Software Engineering Series) | ISBNdb," n.d.)	CMMI Institute-SEI
Test Maturity Model integration (TMMi) ("TMMi Model," n.d.)	TMMi Foundation

Table 3-1 Maturity Model Examples for Different Domains

There is an abundance of work related to information security and cybersecurity maturity modelling. Some of these maturity models are given in Table 3-2.

Maturity Model	Organization/ Authors
Cybersecurity Capability Maturity Model ("Cybersecurity Capability Maturity Model (C2M2) | Department of Energy," n.d.)	US The Department of Energy (DOE)
Open Information Security Management Maturity Model (The Open Group, 2017)	The Open Group
NICE Cybersecurity Capability Maturity Model (Christopher et al., 2014)	US The Department of Homeland Security
ISFAM(the Information Security Focus Area Maturity Model) (Spruit & Roeling, 2014)	Spruit & Roeling

Table 3-2 Information and Cybersecurity Maturity Models

Spruit & Roeling (2014) developed the Information Security Focus Area Maturity Model (ISFAM) which is focused on the information security domain. ISFAM is capable of determining the current information security maturity level and can be used to incrementally and structurally improve information security maturity within the organization. ISFAM is successfully evaluated through several case studies in telecommunications, logistics, healthcare and finance sectors. As the name implies, ISFAM does not focus particularly on cybersecurity related focus areas.

There is no consensus among the maturity models on how to designate the domain specific capability categories. Some of the most common used terms are focus area, process and category. The terms used in the maturity models also depend on the type of the maturity model. In this research, we opted to use the term 'focus area' which is used in the focus area maturity models (van Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2013).

3.2.2 Self-assessment and Required e-Skills for the Questionnaire

As the term implies, self-assessment is a means by which an organization assesses compliance to a selected reference model or module without requiring a formal method (Blanchette & Keeler, 2018).

Eventually, the questions included in the questionnaire are domain specific and require cybersecurity domain awareness and skills. The European e-Competence Framework (CEN, 2016) can be used as a reference to understand the required competencies to effectively answer the proposed questionnaire. In the competency area "Manage", the "Information Security Management" competency is the one that matches most of the skills the user of the questionnaire is desired to have.

3.3 Questionnaire Model

3.3.1 Components and Their Purposes

In the questionnaire model we have developed, there are nine object types: Focus Area, Question, Standard, Capability, Capability Level, Answer, Action, Training Material/Tip and Task. The relationships between these components are shown in Figure 3.2.

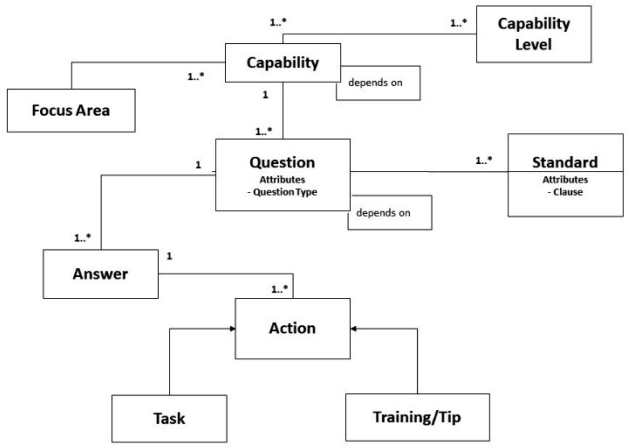


Figure 3.2 Relationships between the Model Components

Focus Area: The sub domains under the cybersecurity security domain such as 'Identity management and access control`.

Question: There are two types of questions: Focus Area Questions and Situational Questions. Focus area questions are the ones questions the cybersecurity capability's implementation. For uniqueness, focus area questions are numbered as F#Q#: Focus Area Number and Question Number. In this paper, Identity Management and Access Control focus area is selected as an example to demonstrate the model.

The Situational questions are used to identify organizational characteristics for adapting the focus area questions' flow and giving personalized guidance. Situational questions are numbered as SQ#: Situational Question Number.

Standard: Focus area questions are elaborated by investigating different information security and cybersecurity standards. Standards and standard clauses are referenced for the focus area questions.

Capability: The ability to achieve an objective for the focus area. Each focus area consists of a number of different capabilities representing progressive maturity levels.

Capability Level: The level of the organizations capability for a focus area. Questions are prepared to identify different levels of capabilities.

Answer: Possible answers to the questions. Answers are numbered as A#: Answer number.

Action: An action triggered by the answer to a question. Actions can either refer to a Training Material/Tip and/or a Task.

Training Material/Tip: The capability related training or tip that will be displayed to the user for a given answer. Training Materials/Tips are identified as TA#: Training Action Number. The purpose to have training material/tip is to increase the awareness of the organization on the specific capability.

Task: The capability related piece of work that should be done to improve the capability level. Tasks are triggered by answers to a question. Tasks are identified by T#: Task Number. The purpose to have Tasks is to provide organizations an implementation guidance for the specific capability. After scheduling the required tasks and the responsible for implementation, the organization will have an implementation plan for capability improvement for the focus area. The organization will have the opportunity to modify the suggested text for the task.

3.3.2 Identifying the Focus Area Questions

To be able to use a focus area maturity model as an instrument to assess the current maturity of a functional domain, measures must be defined for each of the capabilities. This can be done by formulating control questions for each capability. These questions can be combined in a questionnaire that can be used in assessments. Formulation of the questions is usually based on the descriptions of the capabilities and on experience and practices (Steenbergen et al., 2010).

In this research, we have prepared the assessment questions based on ISO 27002 (ISO/IEC, 2013b) and ETSI TR 103 305 (ETSI, 2018b) for the 'Identity Management and Access Control' focus area. In Table 3-3, the referenced standard and the specific clause of the standard can be seen in the third column. Along with the standards, literature can also be used for identifying the capabilities and therefore the focus area questions.

3.3.3 Identifying the Situational Questions

The situational questions complement the model with a risk analysis perspective that vary by the organizational characteristics. These questions are peculiar to the entity type whose cybersecurity capabilities are being assessed. One of the requirements of establishing an information security management according to ISO 27001 (ISO/IEC, 2013a) is understanding the organization and its context in order to perform effective risk analysis. The situational questions presented in the model serve the same objective, understanding the organization and its context in order to address the specific requirements of the organization.

An example of a situational question for service providers or administrators of the critical infrastructures can be 'What is the number of people supplied by the Critical Infrastructure?'. The flow of the focus area questions will depend on the answer given to this question. The more people effected by the shutdown of the critical infrastructure, the more complex cybersecurity capabilities are expected to be implemented.

The implementation of more complex cybersecurity capabilities makes the organization more mature in terms of cybersecurity practices. As the number of people supplied by the critical infrastructure increases the impact that a threat may cause also increases hence this increases the risk faced.

Regarding the critical infrastructures, according to Fekete (2011), criticality can be described by the following three general characteristics and described as follows:

- Critical proportion: Critical proportion contains aspects such as the critical number of elements or nodes of an infrastructure, choke points, as well as critical number of services, size of population, or magnitude of customers affected.
- Critical time: Critical time summarizes aspects such as duration of outage, speed of onset, and specific critical time frames, but also notes the capacities before, during, and after a crisis.
- Critical quality. Critical quality summarizes aspects such as the quality of the service delivered (for example water quality), and includes public trust in (water) quality.

Since the criticality is directly related to the risks faced by the organization in case of any successful attack, these three characteristics can be used to identify the situational questions for the critical infrastructures. For instance, 'What is the number of people supplied by the Critical Infrastructure?' question is related to 'critical proportion' criterion. In Table 3-5, other possible situational questions for the critical infrastructures are given as examples.

Different characteristics of an organization/entity should be considered while designing adaptive maturity assessment models. We will further investigate the applicability of the CHOISS model (Mijnhardt et al., 2016) for designing adaptive maturity assessment models.

3.3.4 The Relationships between the Model Components

The relationships between the model components are depicted in Figure 3.2. Question has the attribute 'Question Type' that can be scale, multiple-choice etc. Standard has an attribute 'Clause' that indicates the specific clause of the relevant standard related to the capability.

3.4 Questionnaire for Identity Management and Access Control

3.4.1 Focus Area Questions and Scoring for Capability Implementation

In the questionnaire model, questions are prepared for each capability level (A, B and C). Table 3-3 shows some example questions selected for the Identity Management and Access Control focus area for each capability level.

In the Prerequisite column, the prerequisite questions or answers can be seen for each of the questions if there is a prerequisite condition for that question. For instance, F1Q3 will only be asked if the answer to F1Q2 is "Yes" (Answer 1). This is an example of intra-focus area dependency i.e. focus area questions depending on the answer for the other questions in the same focus area. The dependency can also be inter-focus area. Another

dependency relation may be between the situational questions and the focus area questions. For F1Q5 in Table 3-3, we see this kind of dependency. F1Q5 is a capability level C question which is the highest level. Designated answers for situational questions in Table 3-5 show a level of increase with the associated cybersecurity risks. For instance, risk associated with A4 to SQ 2 is higher that the risk associated with A3 and so on. In this perspective, the organization is expected to answer questions that are more complex and intend the higher maturity levels, as their risk is increases. This interpretation also enables the constitution of a personalized capability improvement plan.

In the Action for Answer columns, each specific action defined according to the specific answers can be seen. For instance, If the answer to F1Q1 is "No" (Answer 2) then TA1 and T1 will be triggered.

Question Number	Question	Standard, Clause	Capability Level	Question Type	Prerequisite Question/ Answer	Action for Answer 1	Action for Answer 2	Action for Answer 3	Action for Answer 4
F1Q1	Do your users login to your systems by unique user-ids?	ISO 27002, 9.2.1.a	A	Scale			TA1, T1	TA1, T1	TA1, T1
F1Q2	Do you periodically review your access rights (including administrator accounts)?	ISO 27002, 9.2.2.f 9.2.3.f 9.2.5, ETSI TR 103 305, CSC 16	B	Scale			TA2, T2	TA2, T2	TA2, T2
F1Q3	How frequently do you review your access rights (including administrator accounts)?	ISO 27002, 9.2.5	-	Multiple choice	F1Q2A1				
F1Q4	When have you reviewed your access	-	-	Date/ Time	F1Q3	T3	T3	T3	T3

Question Number	Question	Standard, Clause	Capability Level	Question Type	Prerequisite Question/ Answer	Action for Answer 1	Action for Answer 2	Action for Answer 3	Action for Answer 4
	rights (including administrator accounts) the last time?								
F1Q5	Have you enabled audit logging for your administrator accounts?	ISO 27002, 12.4.3	C	Scale	SQ1A2, SQ1A3, SQ1A4, SQ2A2, SQ2A3, SQ2A4 SQ3A2, SQ3A3, SQ3A4, SQ4A1.		TA3, T4	TA3, T4	TA3, T4

Table 3-3 An excerpt from the Identity Management and Access Control Questionnaire

The focus are questions can be answered as to reflect the implementation ratio of the capability that is being assessed. A question contributes to the scoring only if it has an assigned capability level. Some of the questions are intended to gather additional information from the user or assist the user in some situations in order to increase awareness regarding the capability. These type of questions do not contribute to the scoring. Each question in a capability level contributes to the scoring equally. According to the implementation level that the user chooses, the gathered answer contributes to the score with the percentages given in Table 3-4. The implementation rating scale used here is adapted from ISO/IEC 15504 standard (ISO/IEC, 2003). Answer # column shows the respective answer options used for the questions in Table 3-3.

Answer #	Implementation Level	% Contribution to the Score
Answer 1	Fully Implemented (FI)	100
Answer 2	Largely Implemented (LI)	85
Answer 3	Partially Implemented (PI)	50
Answer 4	Not Implemented (NI)	0

Table 3-4 Implementation Levels of the Capabilities and their Contribution Percentage to the Score

3.4.2 Situational Questions

Examples of the situational questions identified for the critical infrastructures are given in Table 3-5.

Question Number	Question	Question Type	Answer 1	Answer 2	Answer 3	Answer 4
SQ1	What is the number of people supplied by the Critical Infrastructure?	Scale	0 - 500.000	500.000 – 1 million	1 million – 2 million	More than 2 million
SQ2	What is the mean time to repair, replace, restore the functionality in case of a cyber attack?	Scale	0 - 10 minutes	10 min - 1 hour	1 - 24 hours	24 or more hours
SQ3	What is the mean time to react in case of a cyber attack?	Scale	0 -10 minutes	10 min - 1 hour	1 - 24 hours	24 or more hours
SQ4	Does any breakdown in the critical infrastructure impact any other critical infrastructures due to interconnectedness?	Yes/No	Yes	No		

Table 3-5 An excerpt from the Situational Questions for Critical Infrastructures (adopted from (Fekete, 2011))

3.4.3 Training Actions and Tasks for Capability Implementation

In Table 3-6, the training material and tips are given. Training material can also be videos along with text material. As an example, TA1 has training material to increase awareness for the usage of unique user-ids. Training material and tips can be compiled from various sources such as standards and literature.

Training Material / Tip Number	Text/Video for the Training Material/Tip
TA1	Using unique user IDs enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and should be approved and documented
TA2	The review of access rights should consider the following guidelines: • users' access rights should be reviewed at regular intervals, e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment

Training Material / Tip Number	Text/Video for the Training Material/Tip
	• user access rights should be reviewed and re-allocated when moving from one employment to another within the same organization; • authorizations for special privileged access rights should be reviewed at more frequent intervals, e.g. at a period of 3 months;
TA3	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

Table 3-6 Training Material and Tips for the Excerpt Questions.

In Table 3-7, it can be seen that T1 is the task to ensure that all users have unique user-ids. According to the model implementation, user can modify the text for the task and schedule a deadline for it, also assign a responsible.

Task Number	Task Definition
T1	Ensure that users login to your systems by unique user-ids.
T2	Ensure that access rights (including administrator accounts) are periodically reviewed.
T3	Schedule a reminder task for date + the review period.
T4	Ensure that audit logging for user accounts (including administrator accounts) is enabled.

Table 3-7 Tasks for the Excerpt Questions.

3.4.4 Capability Improvement Plan

After answering all the questions, and scheduling the tasks respectively, the organization will have an implementation plan for the capability improvement.

An example capability improvement plan is given in Table 3-8. In Table 3-8, we can see the description of the tasks, deadlines for implementation and the responsible persons assigned to the tasks that are scheduled. The tasks for implementing the missing capabilities are grouped by the focus areas. In this capability improvement plan, we can also see the resulting capability score for the focus area. The capability score for the focus area is calculated by accumulating the implementation ratios determined by the user of the assessment questionnaire.

Information Security Capability Improvement Plan For UU			
Identity Management and Access Control Tasks		**Capability Score: 50%**	
Task Number	Description	Deadline	Responsible
T1	Ensure that audit logging for user accounts (including administrator accounts) is enabled.	01/08/2018	B.Y. Ozkan
Patch Management Tasks		**Capability Score: 35%**	
Task Number	Description	Deadline	Responsible
T1	Ensure that automated patching of the operating system is enabled on all machines.	01/07/2018	M.R. Spruit
T2	Ensure that automated patching is enabled for all services and devices interfacing to the internet.	01/08/2018	B.Y. Ozkan
T3	Ensure that users do not have the administrator rights on their computers	01/08/2018	B.Y. Ozkan

Table 3-8 An Exemplar Capability Improvement Plan

3.5 Conclusion

In this research, we have proposed a questionnaire model with various components serving different purposes such as questions for assessing capability, training material for providing awareness, tasks for capability improvement.

The model's implementation with all the components as a whole acts as a potentially useful instrument for self-assessing cybersecurity and improvement planning. The actual application and implementation of the questionnaire model within an organization is beyond the scope of this research. Further research has to be conducted to validate the questionnaire model and to monitor its applicability. Another issue that needs to be addressed in future research is the process of integrating several international or multi-national standards on cybersecurity to compose a coherent set of focus area questions.

In the Horizon2020 SMESEC project, the evaluation of the proposed questionnaire model to assess and improve the cybersecurity capabilities of Small and Medium Sized Enterprises (SMEs) is planned. The focus area questions will remain mainly the same but the situational questions will significantly differ when they are adapted to the characteristics of SMEs.

Acknowledgements

This work was made possible with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

4 Addressing SME Characteristics for Designing Information Security Maturity Models

This paper identifies the effects of small and medium-sized enterprises' (SME) characteristics on the general design principles for maturity models in the information security domain. The purpose is to guide the research on information security maturity modelling for SMEs that will fit in form and function for their capability assessment and development purposes, and promote organizational learning and development. This study reviews the established frameworks of general design principles for maturity models and projects the design requirements of our envisioned information security maturity model for SMEs. Maturity models have different purposes of uses (descriptive, prescriptive and comparative) and design principles with respect to these purposes of uses. The mapping of SME characteristics and design principles facilitates the development of an information security maturity model that systematically integrates the desired qualities and components addressing SME characteristics and requirements.

This work was originally published as:

Yigit Ozkan, B., & Spruit, M. (2020). Addressing SME Characteristics for Designing Information Security Maturity Models. In Clarke N., Furnell S. (Eds.), *IFIP Advances in Information and Communication Technology: Human Aspects of Information Security and Assurance* (pp. 161–174). HAISA 2020, 8-10 July, Online: IFIP.

4.1 Introduction

Small and medium-sized enterprises (SMEs), which are the predominant form of enterprise and make up 99.8% of European enterprises in the Organisation for Economic Co-operation and Development (OECD) area (Digital SME Alliance, 2017), are ill-prepared for cyberattacks (Yigit Ozkan, Spruit, Wondolleck, & Burriel Coll, 2019).

One way of tackling the challenges of managing and implementing information security is through the use of maturity models (Yigit Ozkan et al., 2019). 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 & Spruit, 2019a) (Becker et al., 2009).

Previous research shows that maturity models promote greater levels of organisational learning (Bititci, Garengo, Ates, & Nudurupati, 2015). Organisational capabilities are developed through organisational learning processes (Curado, 2006). From a socio-technical perspective, since information security domain is quite complex (Tisdale, 2016), the value of maturity models is indisputable for developing the necessary information security capabilities. Addressing the characteristics and the requirements of the target organisation will yield to more effective individual and organizational learning and development.

From the perspective of information security maturity models (ISMM), 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). In a recent study for adaptive information security modelling for SMEs, the authors state that utilisation of maturity models for self-assessing information security capabilities can be a remedy for SMEs (Yigit Ozkan et al., 2019).

There have been studies conducted on the development and design of maturity models. Mettler (2009) investigated maturity models as a subject of design science. Becker et al. considering maturity models as design science artifacts, propose a procedure model that distinguishes eight phases in the development of maturity models (Becker et al., 2009). De Bruin et al. propose a methodology to generalize the phases of developing a maturity model and outlined the main phases of generic model development (de Bruin et al., 2005). Pöppelbuß and Röglinger (2011) propose a framework of general design principles for maturity models.

The utilisation of maturity models in different organisational structures has been another aspect that has been studied in the literature. Mettler and Rohner (2009)present a first design proposition of a situational maturity model. In the information security domain, there have been several studies addressing the effect of organisational characteristics. Mijnhardt et al. (2016) investigated organisational characteristics influencing SME information security maturity. In this study, they focused on four different categories of characteristics (General, in and out sourcing, IT dependency and IT complexity). These categories include 11 characteristics such as size, revenue, number of employees, time an organization can run without IT support.

Baars et al. (2016) conclude that a maturity framework should consider the differences between the characteristics of their target organizations. There have also been

cluster based approaches to SME information security (Mayer, 2010) (Yigit Ozkan et al., 2019).

The design principles applied during the development and design of the maturity models affect their applicability in several ways. For example, designing a situational-aware maturity model enables its adaption to different organisational contexts. Being inspired by the studies investigating the maturity models as design artifacts (Becker et al., 2009) (Mettler, 2009) and those providing guidance on the design and development of maturity models (de Bruin et al., 2005) (Pöppelbuß & Röglinger, 2011), the research question this paper addresses is formulated as follows.

"How can SME characteristics be addressed for designing information security maturity models?"

The purpose is to support the development of SME aware ISMMs as design artifacts that will promote greater levels of individual and organisational learning.

To answer this research question, we used the SME characteristics resulting from a literature review (Cocca & Alberti, 2009). These characteristics guided us to identify the "boundary/context" as discussed by Cronholm & Göbel in their study on guidelines supporting the formulation of design principles (Cronholm & Göbel, 2018). We discuss the effects of the SME characteristics' (Cocca & Alberti, 2009) on the general design principles (Pöppelbuß & Röglinger, 2011) and propose 16 design requirements for an ISMM for SMEs.

The rest of the paper is organised as follows. First, background and related research are presented. Second, the general design principles for maturity models (Pöppelbuß & Röglinger, 2011) are investigated with respect to SME characteristics and the findings are presented. Third, the associations between the SME characteristics and the design principles are presented by including the proposed design principles as a summary. Finally, conclusions are drawn.

4.2 Background and Related Research

4.2.1 Design Principles

To date, several studies have investigated the phenomenon of *"Design Principles"*. According to Hevner and Chatterjee (2010), a principle is a clear statement of truth that guides or constrains action. A principle can also be formed as a rule or a standard of conduct. Jones and Gregor (2007) state that design principles "… define the structure, organization, and functioning of the design product or design method". Chandra et al. focused on the characteristics of effective design principle formulation (Chandra et al., 2015). A recent study by Cronholm & Göbel (2018) proposed guidelines supporting the formulation of design principles.

4.2.2 Design Principles for Maturity Models

In the literature, the maturity models are distinguished by their purpose of use as descriptive, prescriptive and comparative. The maturity models for descriptive purpose of use focus on the assessment of the as-is capabilities of an organisation. The maturity models for prescriptive purpose of use provide guidance on how to proceed on the evolutionary path of the maturity levels. The maturity models for comparative purpose of use enables internal and external benchmarking through the assessment results (Becker et al., 2009; de Bruin et al., 2005; Maier, Moultrie, & Clarkson, 2012). De Bruin et.al. argue that even though maturity model types (descriptive, prescriptive and comparative) can be seen as distinct types, they actually represent evolutionary phases of a model's lifecycle. In the final phase of this lifecycle, to be used comparatively the model must be applied in a wide range of organizations in order to attain sufficient data to enable valid comparison (de Bruin et al., 2005).

Pöppelbuß and Röglinger proposed general design principles (DPs) for maturity models grouped according to typical purposes of use and justified on the foundation of maturity modelling literature (Pöppelbuß & Röglinger, 2011). It is important to note that Pöppelbuß and Röglinger states that they deliberately omitted the comparative purpose of use as the fact of whether corresponding DPs can be met largely depends on external factors (Pöppelbuß & Röglinger, 2011).

4.2.3 SME Characteristics

Several studies in the literature suggest that SMEs may be differentiated from larger companies by a number of key characteristics (Cocca & Alberti, 2009) (Storey, 1994) (Hudson, 2001). Different approaches to the phenomena of organisational characteristics were taken in the literature. Yu et al. abstract organisations as organic entities similar to humans and investigate organisational characteristics in categories theoretically rooted in psychology (Yu, Xiao, & Bo, 2018). Mijnhardt et al. (2016) use an indicator-based approach to distinguish between a wide variety of different organizations.

In this paper, we focus on the characteristics present in the literature related to SME research. Cocca and Alberti (2009) conducted a literature review and analysed many papers focusing on SMEs in different fields of science. Their findings were grouped into two main categories: external and internal. The factors related to external environment are typically outside the control of organisation (Cronholm & Göbel, 2018). As the implementation of maturity models (MM) is often considered as part of improvement initiatives (Helgesson, Höst, & Weyns, 2012), they primarily depend on the internal environment of the organisations (Rainer & Hall, 2002).

In Internal characteristics are related to resources, structure, and management practices. , we present the internal characteristics that we investigated in regard to their effects to general design principles proposed by Pöppelbuß and Röglinger (Pöppelbuß & Röglinger, 2011). To increase the readability and to enable more comprehensible referral, the third column in Internal characteristics are related to resources, structure, and management practices. presents the keywords used for the corresponding internal characteristics. Internal characteristics are related to resources, structure, and management practices. The keywords

were selected in a way that we consider they represent the characteristic in a recallable manner.

#	Internal Characteristics (IC)	Keyword
1	Flexible and adaptable to changes, innovative	Flexible
2	Loose and flat structure, lack of bureaucracy	Structure
3	Skills shortages	Skills
4	Lack of management expertise	Management
5	Risk of personal assets	Personal Assets
6	Limited resources: time, human, financial	Resources
7	Lack of organizational capabilities	Capabilities
8	Specialist and tacit knowledge	Knowledge
9	Poor strategic planning	Strategic
10	Reliance on financially based performance measures	Performance
11	Control and decision-making rest primarily with one or a few people	Control
12	Reactive, fire-fighting strategy	Reactive
13	Intuition-based decision making	Decision
14	Learning-by-doing processes	Learning-by-doing
15	Short term vision and orientation	Short-term
16	Incremental improvements and adjustments	Improvements
17	Poor human resource management	HRM
18	Focus on technical aspects and production	Technical
19	Misconception of performance measurement	Performance

Table 4-1 Internal Characteristics and Whether They Affect the Design of Information Security MMs for SMEs. (Cocca & Alberti, 2009)

4.3 Addressing SME Characteristics for Designing Information Security Maturity Models

In order to answer the research question, we investigated each design principle proposed by Pöppelbuß and Röglinger (2011) and analysed the effect of the internal SME characteristics proposed by Cocca and Alberti (2009) on the design principles. The authors of the paper did this analysis thus the findings need to be validated. We further elaborate on the constraints of validity in the conclusion section.

In this section, we present descriptive and prescriptive design principles proposed by Pöppelbuß and Röglinger (2011) and we discuss the effect of SME characteristics, requirements and needs on these design principles. Additionally, we present our insights for the comparative type maturity models. For each design principle, we discuss the SME characteristics' effect on the design principle and we propose design requirements **(DR)** for an ISMM for SMEs. *Table 4-2*, *Table 4-3* and *Table 4-4* present basic, descriptive and prescriptive design principles respectively. To increase the readability and to

enable a more comprehensible referral, the third column in these tables presents the keywords used for the corresponding design principles. The keywords were selected in a way that we consider they represent the characteristic in a recallable manner.

4.3.1 Basic Design Principles

The basic design principles proposed by Pöppelbuß and Röglinger (2011) are given in *Table 4-2*.

#	Principle	Keyword
1.1	Basic Information	Information
1.2	Definition of central constructs related to maturity and maturation	Maturity
1.3	Definition of central constructs related to the application domain	Domain
1.4	Target group-oriented documentation	Users

Table 4-2 Basic Design Principles (Pöppelbuß & Röglinger, 2011)

For an information security model for SMEs, we elaborate on the basic design principles given in *Table 4-2* as follows.

Regarding Information (DP1.1), the domain coverage and prerequisites for applicability of the maturity model should be provided by possibly referring SMEs to some resources. The prerequisites for applications might be confusing for SMEs who have skill shortages (Skills-IC3), lack of organisational capabilities (Capabilities-IC7) and lack of management expertise (Management-IC4). Regarding the target group, in the case of SMEs, the employees or managers who have the most experience in the information security domain should be addressed (Knowledge-IC8) but poor human resources management might make this difficult to accomplish (HRM-IC17). The results should be reported in an easily understandable way. Since SMEs have short-term vision and orientation (Short-term-IC15) and information security is a continuous initiative, it should be made clear to the target group how the ISMM would be beneficial for their business in the long term (Strategic-IC9). SMEs that are aiming at using the ISMM might not have heard of any other maturity models (Skills-IC3, Capabilities-IC7, Reactive-IC12). Therefore, the differences in the ISMM at hand from the other models available should be made clear. The differences might occur in the domain coverage, the purpose of use, target group, design process and the extent of empirical validation.

DR1 – The information on security domain coverage and prerequisites for applicability of the ISMM should be accompanied by extra resources for SMEs.

DR2 – The long-term benefits of utilising the ISMM should be made clear.

DR3 – The differences in the ISMM at hand from the other models available should be made clear.

Regarding Maturity (DP1.2), as information security is a complex domain (Tisdale, 2016), a low level of abstraction would provide more granularity and help better realisation of improvement steps to be taken by the SMEs. This design principle is related to IC14,

"Learning-by-doing processes", IC16, "Incremental improvements and adjustments" and IC18 "Focus on technical aspects and production". Having these characteristics in nature, SMEs will benefit from a low-level granularity in an ISMM.

DR4 – Low-level granularity should be provided to help better realisation of improvement steps to be taken by the SMEs.

Regarding Domain (DP1.3), it is needed to provide the definitions of central constructs related to the information security domain. The utilisation of any well-known frameworks in the information security domain will increase the understandability of the maturity model (Hudson, 2001). Well-known standards published by Standard Developing Organisations (SDOs) in the information security domain (e.g. ISO/IEC 27002 (ISO/IEC, 2013b)) might be a good reference to facilitate the usage of adequate language and understandability of the maturity model. This design principle is related to Skills-IC3, Resources-IC6, and Capabilities-IC7. SMEs having these internal characteristics will benefit by being provided with central constructs that are recognised and well-perceived by their stakeholders.

DR5 – The central constructs that are recognised and well-perceived by SMEs' stakeholders (i.e. standards) should be provided to facilitate the usage of adequate language and understandability of the maturity model.

Regarding Users (DP1.4), given the complexity of information security and the internal characteristics of SMEs (Skills-IC3, Capabilities-IC7, Learning-by-doing-IC14, Improvements-IC16), the documentation of the ISMM should be self-explanatory and easy to understand. Poor human resources management (HRM-IC17) should be considered here as a factor. The risk of Personal Assets (IC5) increases the importance of the ISMM for SMEs. Managing the information security risks reduces the risk of assets which is a direct positive effect for the target group. Providing SMEs with some guidance on how to estimate the cost of efforts with respect to capabilities and maturity levels should be considered (Performance-IC10).

DR6 – The documentation of the ISMM should be self-explanatory and easy to understand.

DR7 – The benefit of using the ISMM for protecting the assets should be made explicit.

DR8 – The documentation of the ISMM should include guidance on how to estimate the cost of efforts with respect to capabilities and maturity levels.

4.3.2 Design Principles for a Descriptive Purpose of Use

The design principles for a descriptive purpose of use are proposed by Pöppelbuß and Röglinger (2011) as follows (*Table 4-3*).

#	Principle	Keyword
2.1	Intersubjectively verifiable criteria for each maturity level and level of granularity	Criteria
2.2	Target group-oriented assessment methodology	Assessment

Table 4-3 Design Principles for a Descriptive Purpose of Use (Pöppelbuß & Röglinger, 2011)

Regarding Criteria (DP2.1), assessment criteria should be concise, precise and clear as defined by Pöppelbuß and Röglinger (2011) as a general principle, specifically for information security maturity modelling for SMEs, the information source (Maier et al., 2012) for the criteria should be also be provided. The SME characteristics Skills-IC3, Capabilities-IC7, Learning-by-doing-IC14 and Improvements-IC16 are related to this principle. SMEs would benefit from well-founded assessment criteria as they rather plan for small steps of improvements (Learning-by-doing-IC14 and Improvements-IC16) and they have a lack of expertise and capabilities.

DR9 – The assessment criteria should be concise, precise and clear and the information source for the assessment criteria should be provided.

As a consequence of several SME characteristics related to lack of expertise and skills (Skills-IC3, Resources-IC6, Capabilities-IC7), SMEs might prefer to outsource the management and implementation of information security. Outsourcing information technology infrastructure is also an identifier in the decision to outsource the security of this infrastructure. Regarding Assessment (DP2.2), outsourcing decisions should be one of the parameters to consider for the applicability of assessment criteria.

DR10 – The assessment methodology should enable the configuration of the criteria according to SMEs' outsourcing decisions.

The European Digital SME Alliance has recently published a position paper on the EU Cybersecurity Act and the role of standards for SMEs (The European Digital SME Alliance, 2020a). In this paper, the need for distinction between different types of SMEs is emphasized. The reason of this differentiation is presented as to make sure that cybersecurity solutions and standards are tailored to them. Regarding Assessment (DP2.2), the SME categories proposed by the Digital SME Alliance can be considered to configure the assessment criteria provided by the maturity model (Knowledge-IC8).

DR11 – The assessment methodology should enable the configuration of the criteria ac-cording to different categories of SMEs' according to their role in the digital ecosystem.

The assessment methodology should be reusable to allow multiple assessments and comparisons over the time of the assessment results to present and observe the improvement (Cholez & Girard, 2014).

4.3.3 Design Principles for a Prescriptive Purpose of Use

The design principles for a prescriptive purpose of use are proposed by Pöppelbuß and Röglinger (2011) as follows (*Table 4-4*).

#	Principle	Keyword
3.1	Improvement measures for each maturity level and level of granularity	I-Measures
3.2	Decision calculus for selecting improvement measures	D-Calculus
3.3	Target group-oriented decision methodology	D-Methodology

Table 4-4 Design Principles for a Prescriptive Purpose of Use (Pöppelbuß & Röglinger, 2011)

Regarding I-Measures (DP3.1), prescriptive maturity models must include improvement measures that enable the development of a road-map for improvement (Pöppelbuß & Röglinger, 2011) (de Bruin et al., 2005). In consideration of information security as the application domain and SMEs as the target group for maturity modelling, the improvement measures should be organised in small and achievable steps which could be facilitated by lack of bureaucracy (Structure-IC2, Learning-by-doing-IC14, Improvements-IC16).

DR12 – The improvement measures should be organised in small and achievable steps.

DR13 – The improvements required to progress to the next maturity level should be explicit.

D-Calculus (DP3.2) is related to decision alternatives and prioritization for improvement planning. Improvement objectives may stem from different sources e.g. internal (management) or external (customers). Given the limited skills, resources, capabilities and management expertise of SMEs (Skills-IC3, Management-IC4, Resources-IC6 and Capabilities-IC7), the decisions for choosing amongst different improvement road-maps is more critical and needs to be justified thus should be further supported to be clear and rational.

DR14 – Clear and rational guidelines should be provided for selecting the improvement measures.

In addition to providing a well-grounded decision for improvement, regarding D-Methodology (DP3.3), a maturity model should also provide SMEs with the tailored advice for adapting the improvement measures considering their role in the digital ecosystem (The European Digital SME Alliance, 2020a), flexibility, control and decision-making mechanisms (Flexibility-IC1, Knowledge-IC8, Control-IC11, Decision-IC13).

DR15 – Tailored advice for adapting the improvement measures should be provided for different categories of SMEs.

4.3.4 Design Principles for a Comparative Purpose of Use (CPoU)

As stated earlier, our reference study for the general design principles, Pöppelbuß and Röglinger deliberately omitted the principles for the comparative purpose of use (Pöppelbuß & Röglinger, 2011). De Bruin et al. states that for a model to be used comparatively it must be applied in a wide range of organizations in order to attain sufficient data to enable valid comparison. Cholez and Girard presented a framework that allows multiple assessments and successive comparisons over the time of the assessment results in their study on information security maturity assessment in SMEs. The exemplar assessment result in this study presents a radar graphic depicting the enterprise profile (Cholez & Girard, 2014). We recognize that the utilisation of this kind of visuals to present the assessment results for comparative purposes can assist SMEs for better understanding and presenting their as-is and to-be positions. This will help to reduce "Misconception of performance measurement" in regards to Performance-IC19 (Table 4-1). As stated in Section 4.3.1, SMEs may gain strategic advantage by comparatively using the assessment results (Strategic-IC9).

DR16 – Visual presentation of the assessment results for comparative purposes should be utilized to assist SMEs to better understand and present their as-is and to-be positions.

4.4 Mapping of SME Characteristics and Design Principles

In this section, the mapping of internal characteristics given in Table 4-1 and design principles given in respective tables (*Table 4-2*, *Table 4-3*, *Table 4-4*) are presented here as a summary in *Table 4-5*. This table shows the associations between the SME characteristics and the design principles by specifying the corresponding design requirements as discussed in this paper.

Internal Characteristics	Design Principles									
	Information DP1.1	**Maturity DP1.2**	**Domain DP1.3**	**Users DP1.4**	**Criteria DP2.1**	**Assessment DP2.2**	**I-Measures DP3.1**	**D-Calculus DP3.2**	**D-Methodology DP3.3**	**CPoU**
Flexibility (IC1)									DR15	
Structure (IC2)							DR12, DR13			
Skills (IC3)	DR1, DR3		DR5	DR6	DR9	DR10		DR14		
Management (IC4)	DR1							DR14		

Internal Characteristics	Design Principles									
	Information DP1.1	**Maturity DP1.2**	**Domain DP1.3**	**Users DP1.4**	**Criteria DP2.1**	**Assessment DP2.2**	**I-Measures DP3.1**	**D-Calculus DP3.2**	**D-Methodolog v DP3.3**	**CPoU**
Personal Assets (IC5)				DR7						
Resources (IC6)			DR5			DR10		DR14		
Capabilities (IC7)	DR1, DR3		DR5	DR6	DR9	DR10		DR14		
Knowledge (IC8)	DR1					DR11			DR15	
Strategic (IC9)	DR2									DR16
Performance (IC10)				DR8						
Control (IC11)									DR15	
Reactive (IC12)	DR3									
Decision (IC13)									DR15	
Learning-by-doing (IC14)		DR4		DR6	DR9		DR12, DR13			
Short-term (IC15)	DR2									
Improvements (IC16)		DR4		DR6	DR9		DR12, DR13			
HRM (IC17)	DR1			DR6						
Technical (IC18)		DR4								
Performance (IC19)										DR16

Table 4-5 Mapping of SME Characteristics and Design Principles

4.5 Conclusion

In this paper, we investigated the SME characteristics (Cocca & Alberti, 2009) that may affect the general design principles of maturity models for SMEs (de Bruin et al., 2005) (Pöppelbuß & Röglinger, 2011). We discuss the possible effect of the SME characteristics on the general design principles and propose 16 design requirements for an ISMM for SMEs.

We present the mapping of the internal SME characteristics and the design principles by specifying the corresponding design requirements as a summary. Since the mapping of the internal SME characteristics and the design principles was done by the authors, it is important to bear in mind the possible bias in these. This limitation stimulates further research to assess the validity of the proposed design requirements by means such as evaluation by SMEs and maturity model developers. Another possibility for future research is a review of a set of existing ISMMs concerning the proposed design principles.

We believe that if the proposed design principles are taken into account from the very start of ISMM development for SMEs, one can systematically account for diverse SME characteristics profiles, thereby significantly increasing the potential usability and applicability of the resulting maturity model. This will yield a better individual and organisational learning with respect to information security.

SECTION 2 CYBERSECURITY STANDARDISATION

5 Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda

There are various challenges regarding the development and use of cybersecurity standards for SMEs. In particular, SMEs need guidance in interpreting and implementing cybersecurity practices and adopting the standards to their specific needs. As an empirical study, the workshop "Cybersecurity Standards: What impacts and gaps for SMEs" was co-organized by the StandICT.eu and SMESEC Horizon 2020 projects with the aim of identifying cybersecurity standardisation needs and gaps for SMEs. The workshop participants were from key stakeholder groups that include policymakers, Standard Developing Organizations, SME alliances and cybersecurity organisations. This paper highlights the key discussions and outcomes of the workshop and presents the themes, current initiatives, and plans towards cybersecurity standardisation for SMEs. The findings from the workshop and multivocal literature searches were used to formulate an agenda for future research.

This work is an extended version of the paper originally published as:

Yigit Ozkan, B., & Spruit, M (2019). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. *International Journal of Standardization Research, 17*(2), 1–25.

5.1 Introduction

A survey in the Global Risks Report (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 losses and expenses (Gañán et al., 2017).

Small and medium-sized enterprises (SMEs), which are the predominant form of enterprise and make up 99.8% of European enterprises in the Organisation for Economic Co-operation and Development (OECD) area (Digital SME Alliance, 2017), are ill-prepared for cyberattacks.

Although there is a multitude of standards available to measure, identify and improve the cybersecurity practices at organisations, many of these are not well suited for SMEs (Manso et al., 2015).

In the standardisation processes, in many cases, SMEs are dependent stakeholders, and they lack resources to properly participate in the process. SMEs typically require financial support, access to technical expertise and other types of assistance to be involved in the standardisation process (de Vries, Verheul, & Willemse, 2003). In addition, SMEs may face other barriers to benefit from standards and involvement in standardisation. Awareness of standards and the process of standardisation are two important barriers (de Vries, Blind, Mangelsdorf, & Verheul, 2009).

The goal of this research is to identify the gaps (e.g. knowledge or facilitation gaps) regarding cybersecurity standardisation for SMEs by performing a literature study, analysing the trends in the literature, describing the initiatives that address SMEs, conducting an empirical study through a workshop with applicable stakeholders, and identifying opportunities for future research. Therefore, the following main research question is put forward: "What are the gaps in cybersecurity standardisation for SMEs?"

To answer this main research question in a structured way, three sub research questions were formulated. The first sub research question examines the trends in the literature and state of the art in European level initiatives addressing cybersecurity standardisation for SMEs. The second sub research question addresses the experiences and views of the stakeholders. The third sub research question addresses the future research directions to be considered to fill the gaps.

A visual depiction of these research questions is shown in Figure 5.1.

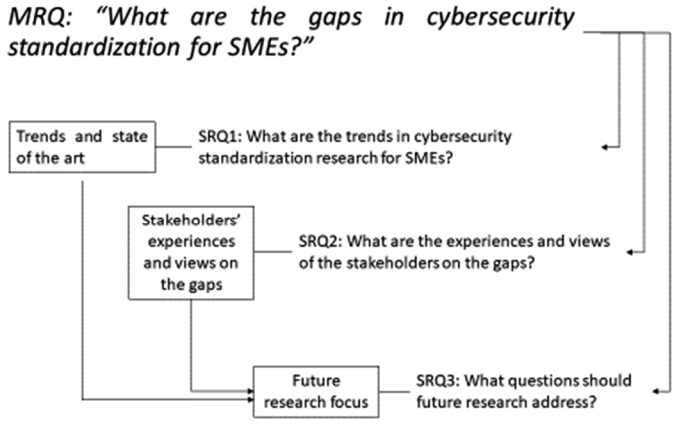


Figure 5.1 Main Research Question and Sub Research Questions

SRQ1 is addressed by performing multivocal literature searches to show the trends in the literature on cybersecurity standardisation for SMEs and the state of the art in the European landscape. The findings are presented in the Literature Study section.

SRQ2 is addressed by identifying the stakeholders in cybersecurity standardisation for SMEs and organising a workshop to gather stakeholders' views and perspectives. In that sense, given the importance of cybersecurity, SMEs' challenging situation, lack of research addressing SMEs and the diverse stakeholders, the SMESEC and StandICT.eu EU Horizon 2020 projects co-organized the "Cybersecurity Standards: What impacts and gaps for SMEs" workshop to investigate experiences, needs and gaps in cybersecurity standardisation for SMEs by bringing the key parties together. Thus, the workshop addresses the second sub research question: "What are the experiences and views of the stakeholders on the gaps?" The workshop was held on May 24, 2019, in Brussels, Belgium.

SRQ3 is addressed by synthesising all findings from SRQ1 and SRQ2 into a focused agenda for future research.

The contribution of this paper to cybersecurity standardisation for SMEs is two-fold: on one hand, it presents the trends in the literature for cybersecurity standardisation research addressing SMEs and the experiences and views of the stakeholders for SME cybersecurity standardisation, on the other hand, it aggregates the related gaps and needs towards an agenda for the standardisation research.

The remainder of the paper is organized as follows. The Literature Study section explains the key terms for information security and cybersecurity that are used for searching

the literature, presents the European landscape in SME Standardisation including cybersecurity specific initiatives, and other related literature for the study at hand.

The Empirical Study section presents the design of the workshop that was co-organised by the StandICT.eu and SMESEC EU funded Horizon 2020 projects ("Workshop Cybersecurity Standards," 2019), workshop stakeholder groups and participants, information about the workshop including the structure of the workshop, workshop contributions categorised by the stakeholder groups and the key outcomes of the workshop. The gaps and the research agenda formulated from the findings are presented next. The final section provides an overview of practical impacts and concludes the paper.

5.2 Literature study

Since the concepts in the cybersecurity and information security domain are intertwined the authors used the terms cybersecurity and information security together for identifying the trends in literature. Albeit, it is important to note the differences between these terms. In this section, first, the respective coverage of these domains is described. Second, to address SRQ1 the literature searches that were performed to identify the trends are presented with the results. Third, findings from the grey literature are presented. This knowledge base comprises the European SME standardisation landscape including cybersecurity-specific initiatives. Finally, a review of SMEs' organisational characteristics influencing their information security (Mijnhardt et al., 2016) that was particularly used to draw questions for future research to address the insights stemming from the workshop ("Workshop Cybersecurity Standards," 2019) is presented.

5.2.1 Information Security and Cybersecurity

Concepts in the information security and cybersecurity domain are intertwined, making things considerably more complex for untrained stakeholders. Therefore, it is important to distinguish between the scopes and goals of the two distinct fields. According to the ISO/IEC 27032–guidelines for cybersecurity–standard, information security is concerned with "the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user" (ISO/IEC, 2012). On the other hand, cybersecurity is defined as "the preservation of confidentiality, integrity and availability of information in the cyberspace". The cyberspace has several characteristics:

1. It is a virtual environment; the environment does not exist in any physical form.
2. It is a complex environment, which resulted from the emergence of interconnected networks (such as the internet).
3. It has multiple 'dimensions': it is also formed by the people, the organisations and the activities on a plethora of devices and networks that have a connection to the cyberspace.

The ISO/IEC 27032 standard differentiates cybersecurity and other domains of security as depicted in Figure 5.2 (ISO/IEC, 2012).

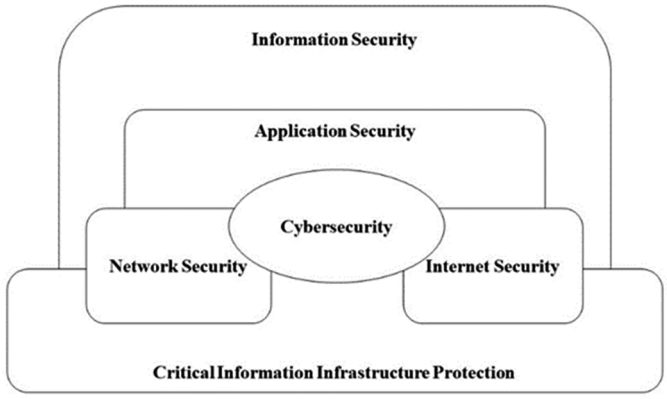


Figure 5.2 Relationship between Cybersecurity and Other Security Domains (redrawn from ISO/IEC 27032 (ISO/IEC, 2012))

The ISO/IEC 27032 standard defines the relationship between cybersecurity and other domains as follows: *Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks…It has a unique scope requiring stakeholders to play an active role in order to maintain, if not improve the usefulness and trustworthiness of the Cyberspace.* (ISO/IEC, 2012).

5.2.2 Information Security and Cybersecurity Standards for SMEs

In order to help organisations and individuals to improve awareness on standardisation, certification and labelling in cybersecurity, the European Cybersecurity Organisation (ECSO) published an overview of existing cybersecurity standards and certification schemes (ECSO, 2017). Given the extensive number of domain-related standards, this document facilitates the identification of relevant standards easily.

In this state of the art syllabus document, ECSO not only focuses on the standards specific to sectors, but also the standards applicable to generic organisations. The generic organisations in this sense are the ones not associated with any particular industry vertical (e.g. energy, healthcare, and telecom). The standards applicable to generic organisations are also perfectly applicable to industry verticals but may not include the sector-specific requirements. 20 standards and schemes are listed as applicable to generic organisations in the ECSO document. Seven of them are international standards published by ISO (International Organization for Standardization). Only one of these 20 standards and schemes

–the Finnish Cyber Security Certificate (FINCSC)– has been identified as addressing specifically SMEs (JAMK University of Applied Sciences, 2020). As the name implies, it is rather a certification scheme than a standard. It is based on self-assessment questionnaires to assess companies followed by the review of the findings by an accredited certification body.

To identify any standards specifically addressing SMEs published by ISO, CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization), we conducted searches using these organisations' search tools. We identified 3 standards only from ISO – one related with environmental management (ISO, 2019b), one related with innovation management (ISO, 2019c) and one related with human resources management (ISO, 2018a)– that either supports phased implementation of a standard or provides additional guidance for SMEs. These are all recent standards; we expect that SDOs will publish more standards addressing SMEs in the future. As described in the "Cybersecurity Specific Initiatives" section of the paper, the Small Business Standards (SBS) guide –"SME Guide for the implementation of ISO IEC 27001 on Information Security Management" (SBS, Digital SME Alliance, 2018)– is under consideration for adoption by CEN-CENELEC.

In a study investigating the suitability of information systems security management standards for SMEs, the authors provide a list of 17 standards and methods (in Appendix 1, Table 2) (Barlette & Fomin, 2008). Only two of these are marked as theoretically suitable for SMEs. Despite the name of this study implies that more standards had been investigated, the ISO 27001 standard was the only focus of this study regarding information security standards.

ENISA published an overview study titled "Information security and privacy standards for SMEs", which also provides recommendations to improve the adoption of the standards (Manso et al., 2015). In Annex A of ENISA's document, a list of information security and privacy standards for SMEs is provided but with no discussion on how these standards could be adopted by SMEs.

The Digital SME Alliance has recently published a position paper titled "The EU Cybersecurity Act and the role of standards for SMEs" (The European Digital SME Alliance, 2020). This position paper presents the most important challenges for SMEs in the adoption of standards and offer recommendations to SDOs to support SMEs in their challenges. The recommendations include the following options:

- Option 1: Further the evolution of existing standards
- Option 2: Develop lightweight standards or guides
- Option 3: Develop new standards specifically for SMEs
- Option 4: Combine different standards into packages tailored to SMEs

The Digital SME alliance differentiates SMEs by their role in the digital ecosystem and states that the solutions should be tailored according to their specific needs (The European Digital SME Alliance, 2020).

5.2.3 Trends in the Literature

In order to investigate the publication trends (SRQ1), four different search queries were formulated (Table 5-1) and executed in Scopus and Web of Science (WoS) research index databases. The search scope was limited to publication title, abstract and keywords for Scopus, and topic and title for WoS.

Search #	Target Population	Search String
S1	The entire population of papers in cybersecurity domain	("cyber security" OR "cybersecurity" OR "information security")
S2	The sub-population that relates to Standardisation/Standards	(("cyber security" OR "cybersecurity" OR "information security") AND "standard*")
S3	The sub-population that relates to SMEs	(("cyber security" OR "cybersecurity" OR "information security") AND "SME*")
S4	The sub-population that relates to SMEs and Standardisation/Standards	(("cyber security" OR "cybersecurity" OR "information security") AND "standard*" AND "SME*")

Table 5-1 Literature Search Strings (Cybersecurity, Standard and SME)

Figure 5.3 presents the results from S1 and S2 respectively. The earliest year of publications found in the databases are: in Scopus, 1967 for S1 and 1985 for S2; in WoS, 1996 for S1 and 1991 for S2.

Accordingly, an increase in the number of publication over the years with an increasing trend is clearly visible (Figure 5.3-left). In parallel, an increase in the number of publications on cybersecurity standardisation over the years is observed however not trending as much and visible only in recent years (Figure 5.3-right).

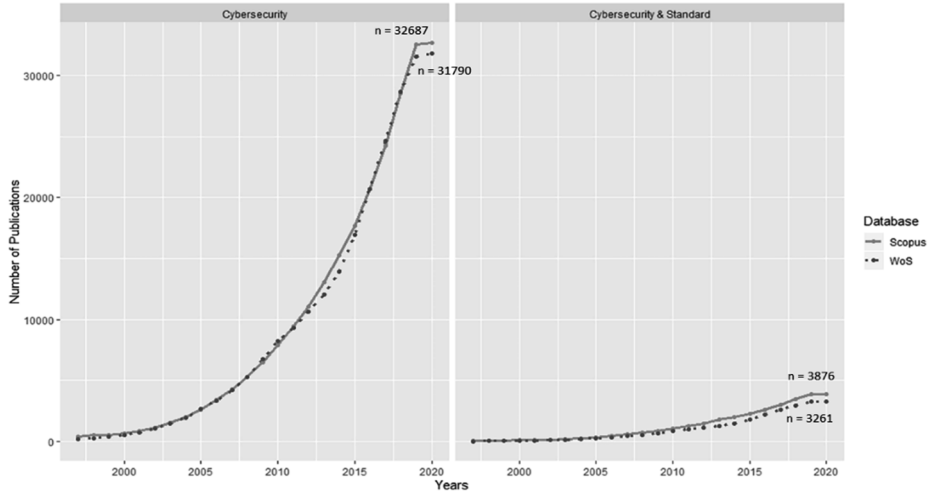


Figure 5.3 Trends in the Number of Research Publications on Cybersecurity (left) versus Cybersecurity Standardisation (right)

Figure 5.4 presents the results from S3 and S4. The earliest year of publications found in the databases are: in Scopus, 1998 for S3 and 2004 for S4; in WoS, 2006 for S3 and 2007 for S4.

Accordingly, security research, in general, has started to consider SMEs after 2005 with a stable trend (Figure 5.4-left). Among these, very few publications also consider the standardisation aspects (Figure 5.4-right). They also increase with a stable however lower trend. The proportion of the sub-population that considers SME in the entire security population (Figure 5.3-left) is less than 1 percent (the number of cybersecurity publications addressing SMEs (Figure 5.4-left) divided by the number of total cybersecurity publications (Figure 5.3-left)). Furthermore, what is clear from Figure 5.3 and Figure 5.4 is the significant difference between the number of publications on cybersecurity standardisation that addresses SMEs (Figure 5.4-right) and that does not (Figure 5.3-right).

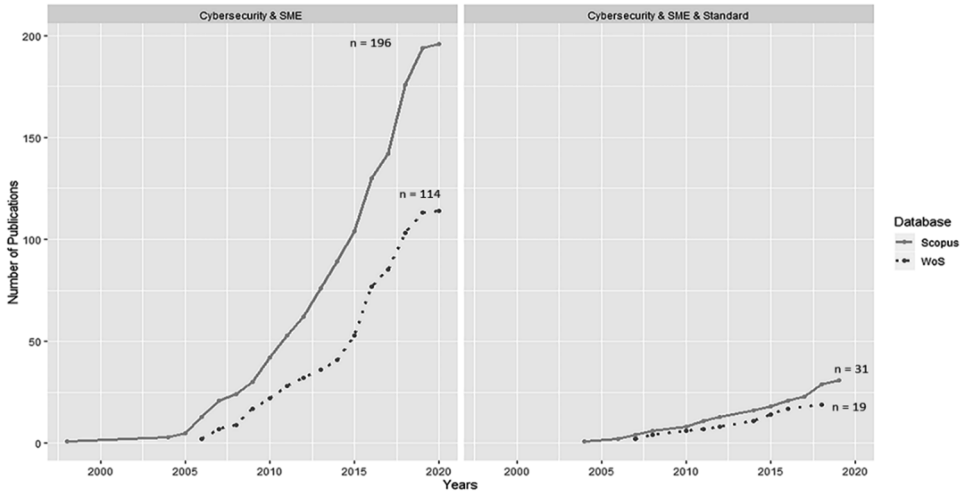


Figure 5.4 Trends in the Number of Research Publications on Cybersecurity & SMEs (left) versus Cybersecurity, SMEs and Standardisation (right)

To sum up, the evidence from the cyber- and information security publications search suggests that the research interests and outputs that address standardisation in an SME context are few and the topic has only begun to attract the attention of a few researchers in recent years.

In relation to the main research question of this study, the publications results for the right side of Figure 5.4 were investigated in further detail. This search resulted in 31 publications from the Scopus database and 16 publications from the WoS database. Only three of the publications were identical. Accordingly, the searches from the two databases resulted in 44 unique publications. Detailed investigation showed that, among those publications, 11 articles and 1 conference paper are not addressing SMEs. The SME abbreviation was used for other phrases such as subject matter experts in these articles. Excluding these reduces the number of relevant publications to 32. Table 5-2 shows the number of publications per publication type. As can be seen from this table, five of the resulting publications are conference review papers. Excluding these papers results in 27 relevant publications in total. Therefore, the Number of Relevant Publications column in Table 5-2 shows the total number of papers by excluding the publications that are not addressing SMEs and the conference review publications. The list of the relevant and non-relevant publications –presented as a bibliography– can be found in APPENDIX.

Publication Type	Total Number of Publications	Number of Relevant Publications
Article	21	10
Book Chapter	1	1
Conference Paper	17	16
Conference Review	5	0
Total	44	27

Table 5-2 Number of Publications per Publication Type (Cybersecurity, SME and Standard)

From the results of the searches performed, the authors conclude that although a considerable amount of literature has been published on information security and cybersecurity standardisation, at a large extent, this literature does not address SMEs. In their paper on a standardisation research agenda, de Vries et al. (2018) point out that the enormous number of standards (which is the case in the cybersecurity domain) represents a considerable burden for SMEs. In their paper, the authors also state that research on standards' impact on SMEs is limited. Our findings from the literature search support these arguments.

5.3 SME Standardisation and European Landscape

In this section, the state of the art with respect to four types of standardisation initiatives aimed at SMEs in European level is presented: Initiatives of Standard Developing Organisations, Initiatives of SME Organisations, Cybersecurity Specific Initiatives, and the EU Rolling out plan for ICT (Information and Communications Technology) standardisation.

5.3.1 Initiatives of Standards Developing Organisations

International, regional or national level Standards Developing Organisations (SDOs) have undertaken several initiatives for helping SMEs in standardisation processes. The SME Standardisation Toolkit (CEN-CENELEC, 2019c) is an example of tools provided by CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) to facilitate SME involvement in standardisation. This toolkit is mainly aimed at national standardisation organisation.

Another example to support SMEs in standardisation is the interactive online educational tool (CEN-CENELEC, 2019d) which provides SMEs with a chance to learn about standardisation in a quick and easy way. This e-learning tool is available in 23 languages. Furthermore, BSI (British Standards Institution) has published a guide to standards for small businesses that emphasizes the benefits of standards.

Finally, ETSI (European Telecommunications Standards Institute) published a white paper (ETSI, 2011) on the results of a study to evaluate how to improve the participation of Small and Medium-sized Enterprises (SMEs) in ETSI standardisation. As reported by the Digital SME Alliance, *ETSI recently reviewed its internal procedures to mandate that proposers of new standards describe their relevance to SMEs. As decided by the ETSI Board in January 2020, all new standards projects at ETSI will be accompanied*

with a form that displays information on their impact on SMEs (The European Digital SME Alliance, 2020b). This news article announces the decision as a success story as the result of the work of SBS in the ETSI decision-making bodies.

5.3.2 Initiatives of SME Organisations

The European DIGITAL SME Alliance is the largest network of the small and medium-sized ICT enterprises in Europe, representing about 20,000 digital SMEs. SBS (Small Business Standards) is a non-profit organisation representing SMEs within the European Standardisation System. SBS published a user guide for European SMEs on ISO 26000 guidance on social responsibility (SBS, 2016).

5.3.3 Cybersecurity Specific Initiatives

With the Communication on ICT Standardisation Priorities, the European Commission (EC) proposes to focus standard-setting resources and communities on 5 priority areas: 5G, Internet of Things, cloud computing, cybersecurity and data technologies because they are essential for wider EU competitiveness (EC, 2016). Every year, the EC releases the Rolling plan on ICT Standardisation, which identifies ICT standardisation activities in support of EU policies. The 2019 plan was published in March. The rolling plan provides a unique overview of standardisation activities in the field of information and communication technologies (ICT) linked to EU legislation and policies, such as healthcare, cloud computing, intelligent transport systems, security, accessibility, Internet of Things, eGovernment, smart grids and many others (EC, 2019). In the "Cybersecurity/ Network and Information Security" section of this plan, EC defines 7 actions requested from the Standard Developing Organisations (SDOs). Among these actions, one of them directly addresses SMEs' needs as follows:

SDOs to develop a "guided" version of ISO/IEC 270xx series (information security management systems including specific activity domains) specifically addressed to SMEs, possibly coordinating with ISO/IEC JTC1 SC27 WG1 to extend the existing guidance laid out in ISO/IEC 27003. This guidance should be 100% compatible with ISO/IEC 270xx and help SMEs to practically apply it, including in scarce resource and competence scenarios (EC, 2019)

Perfectly aligning with the abovementioned action, the Digital SME alliance and SBS have published the "SME Guide for the implementation of ISO IEC 27001 on Information Security Management" (SBS, Digital SME Alliance, 2018). This guide is currently under consideration for adoption by CEN-CENELEC.

The European Union Agency for Network and Information Security (ENISA) is conducting security surveys and publishing dedicated cyber security guides for SMEs. ENISA published guidelines for SMEs on the security of personal data processing (European Network and Information Security Agency, 2016) and cloud security guide for SMEs (Dekker, Liveri, Europäische Union, & Agentur für Netz- und Informationssicherheit, 2015). Another publication of ENISA aims to provide a set of relevant recommendations regarding

how to increase the adoption of information security and privacy standards in SMEs (Manso et al., 2015).

ECSO (the European Cyber Security Organisation) has a working group (WG4: Support to SMEs, coordination with countries and regions) to support SMEs (ECSO, 2019b).

The National Cybersecurity Centre supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the public. The National Cybersecurity Centre operates Cyber Essentials which is an information assurance scheme that encourages organisations to adopt good practices in information security (National Cybersecurity Centre, 2017). Cyber Essentials includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet. To support SMEs in adhering to the approach, the UK government has deployed a specific voucher scheme including coaching, documentation and certification.

The Information Systems Security Association (ISSA) published the ISSA 5173 standard to encourage SMEs to take steps to secure their customer's and employee's data (ISSA UK, 2018). The standard sets out a hierarchy of security controls that are considered both appropriate and affordable.

5.3.4 Cybersecurity Standard Gap Analysis

The challenges for SMEs regarding cybersecurity standardisation are elaborately discussed in the "Cybersecurity standard gap analysis" whitepaper (Cyberwatching.eu, 2018). This white paper was prepared by surveying the cybersecurity research, industry, public sector and user communities in order to get inputs into identifying the perceived gaps. 16% of the survey responders were SMEs. In the whitepaper, the following issues regarding SMEs are listed as recommendations:

- The cost issue for SMEs looking toward standards and cybersecurity certification must be addressed.
- SMEs must be able to access standards and related certification without breaking the bank.
- Self-assessment and other low-cost solutions need to be explored.

5.3.5 Organisational Characteristics Influencing SME Information Security Maturity

It is important to understand the organisational characteristics influencing SME cybersecurity or information security maturity. Based on literature review and expert evaluations, Mijnhardt et al. (2016) have identified 11 organisational characteristics (OCs) consisting of 47 measurement levels as presented in Figure 5.5. These OCs can be utilised as an input for developing SME specific cybersecurity standards or tailoring the existing standards for SME characteristics.

Organizational characteristic	Measurement levels
General company information	
Number of employees	0–9 employees, 10–49 employees, 50–250 employees
Organization's revenue	0–2 Million, 2–10 Million, 10–50 Million
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 x 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 5.5 Organisational Characteristics and Measurement Levels in CHOISS (Mijnhardt et al., 2016)

5.4 Empirical study: Multi-stakeholder Workshop

To address SRQ2, the workshop "Cybersecurity Standards: What impacts and gaps for SMEs" was co-organised by the StandICT.eu and SMESEC EU funded Horizon 2020 projects.

StandICT.eu (Supporting European Experts Presence in International Standardisation Activities in ICT) is an H2020 project that addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene ("About StandICT.Eu," 2018). SMESEC (Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework) is an H2020 project proposed by an international group of experts as a response to the cyber-security challenges of SMEs with limited background on cybersecurity and a restricted budget (SMESEC, 2017).

The workshop was hosted by CEN and CENELEC, supported by ECSO and the Digital SME Alliance, and gathered the key stakeholders described in Table 5-4 together. In the workshop, there were 12 talks followed by a total of 28 participants including the presenters. This section presents the design of the workshop, workshop stakeholder groups and participants, information about the workshop including the aim and the structure of the workshop. The stakeholders' contributions and the outcomes of the workshop are also presented in this section,

5.4.1 Set-up

Before organising the workshop, and based on Freeman's (Freeman, 2010) definition of a stakeholder–*any group or individual who can affect or is affected by the achievement of the organization's objectives*–, the authors asked the most experienced

members (in SMEs and standardisation processes) of the StandICT.eu and SMESEC consortia to identify key stakeholders for SME cybersecurity standardisation. As a result, five key stakeholder groups were identified:

1. Policymakers, influencers, regulators
2. Standards Developing Organisations (SDOs)
3. SME Alliances
4. Cybersecurity Organisations and
5. EU funded research projects related to cybersecurity for SMEs and ICT standardisation.

After identifying the stakeholder groups, the organisers–the StandICT.eu and SMESEC projects–of the workshop ("Workshop Cybersecurity Standards," 2019) have informed several organisations from each stakeholder group about the aim of the workshop and invited them to participate in the workshop. The majority of the stakeholders were interested in the workshop and at least one stakeholder from each group agreed to participate. After the workshop, the authors analysed the stakeholders' contributions during the workshop. This paper categorises the findings by stakeholder groups as presented in Table 5-4.

5.4.2 Workshop Participants

The authors analysed the types of the stakeholders using the IT standardisation stakeholder typology presented in (de Vries et al., 2003) since it was specifically defined for IT standardisation processes and was illustrated by an information security management standard case study. In (Mitchell, Agle, & Wood, 1997), the authors present the attributes of stakeholders as power, legitimacy and urgency. Using these attributes, they propose a stakeholder typology based on the number of attributes possessed by the stakeholders. In the typology proposed, there are seven types of stakeholders namely, dormant, dominant, dangerous, definitive, discretionary, demanding and dependent. de Vries et al. (2003) present the definition of these stakeholder types adapted to the standardisation processes. In the workshop, there were stakeholders of definitive, dominant, discretionary and dependent types. The definitions of these types adapted to the standardisation processes are presented in Table 5-3 (de Vries et al., 2003).

Stakeholder Type	Definition
Definitive	Definitive stakeholders have the power to affect the standardisation process, they consider the standard to be important, and their involvement is indisputable.
Dominant	Like the discretionary stakeholder, the dominant stakeholder itself does not see immediate interest in participating, while its participation is considered desirable from the perspective of the standardisation process.
Discretionary	Discretionary stakeholders do not have the resources to affect the standardisation process and feel no urgent need to participate.
Dependent	The dependent stakeholders are important for the general support of a standard and they see the need to participate in the standardisation process.

Table 5-3 Stakeholder Types and Definitions (de Vries et al., 2003)

Accordingly, SMEs can be categorised as either discretionary or dependent stakeholders, depending on their level of security awareness. SMEs that do see the need for information security belong to dependent stakeholder category. Dependent stakeholders in many cases lack resources to properly participate in the standardisation process. SMEs require financial support, access to technical expertise and other types of assistance to be involved in the standardisation process (de Vries et al., 2003).

The stakeholder groups and the matching workshop participants are listed in Table 5-4 together with their stakeholder types. In the workshop, SMEs were represented by two SME alliances as presented in Table 5-4. The stakeholders listed in *Table 5-4* interact with each other, establish liaisons, coordinate and collaborate their activities in several settings. There are initiatives such as joint technical committees (CEN-CENELEC, 2019a) ("ETSI - Cyber Security," 2019), working groups (ECSO, 2019a) (ECSO, 2019b), workshops (CEN-CENELEC, 2019b), publications (Manso et al., 2015), surveys (Cyberwatching.eu, 2018), and meetings to ensure the harmonisation of these stakeholders' efforts for cybersecurity standardisation for SMEs.

Stakeholder Group	**Workshop Participant Organisation**	**Number of Participants (per group)**	**Stakeholder Type**			
			Definitive	**Dominant**	**Discretionary**	**Dependent**
Policymakers, influencers, regulators	• European Commission (EC)	4	X	X		
Standard Developing Organisations (SDOs)	• CEN (European Committee for Standardization) • CENELEC (European Committee for Electrotechnical Standardization) • ETSI (European Telecommunications Standards Institute)	2	X			
SME Alliances	• Small Business Standards (SBS) • Digital SME Alliance	3			X	X
Cybersecurity Organisations	• European Cyber Security Organisation (ECSO)	1	X	X		
EU funded research projects related to cybersecurity for SMEs and ICT standardisation	• SMESEC.eu • StandICT.eu	5	X		X	X

Table 5-4 Workshop Stakeholder Groups, Participants and Their Types

In addition to the stakeholders given in Table 5-4, three ICT standardisation experts, one government representative, two independent researchers, and seven private sector members participated in the workshop.

5.4.3 Structure of the Workshop

The workshop comprised of a keynote, three panels and a wrap-up session that are elaborated upon as follows. The Keynote introduced the EU Cybersecurity Package and the Innovation & Research Plan towards Horizon Europe. Panel 1 set the scene of cybersecurity standardisation impacting SMEs. The panel's speakers were the key representatives from the Standard Developing Organisations (SDOs) on achievements to date and future challenges. Panel 2 gave a voice to SMEs. In this panel, there were two speakers from EU funded H2020 projects and one speaker from ECSO WG4 (Working Group 4) (ECSO, 2019b). Panel 3 provided a voice from SMEs, providing an opportunity for the SMEs to report on gaps and needs on cybersecurity standards and best practices. At the end of the workshop, a wrap-up was presented to synthesise the findings and final words could be expressed by the participants. Every stakeholder expressed their willingness to collaborate in helping SMEs with their cybersecurity standardisation challenges. The next section elaborates on the workshop sessions, organised by stakeholder groups.

5.4.4 Workshop Contributions Categorised by Stakeholder Groups

5.4.4.1 Policymakers, Influencers, Regulators

The EC representative gave a policy level talk and introduced the EU Cybersecurity Package and the Innovation & Research Plan towards Horizon Europe. The speaker expressed that the Cybersecurity Package will enable a more robust response to cyber-attacks by:

- Encouraging a Single Cybersecurity Market
- Pooling and shaping research efforts in Cybersecurity
- Fostering NIS (Network and Information Security) Directive implementation
- Proposing a reformed ENISA
- EU Cybersecurity Certification
- Coordinating an emergency response

The EC representative also addressed the key topic for SDOs as certification. According to the EC representative, for the cybersecurity domain, certification will evolve similar to the energy and aviation domains. A participant from the EC pointed out that EU funded H2020 projects have standardisation as a task and can allocate resources, on the other hand, SDOs lack resources. There is no link between these two. Some action should be taken to tighten the connection that will benefit both sides.

5.4.4.2 Standards Developing Organisations (SDOs)

The CEN - CENELEC JTC (Joint Technical Committee) 13 (CEN-CENELEC, 2019a) representative addressed the main objective of the JTC 13 as the transposition of international standards to European standards. The scope of activities of the JTC 13 is the development of standards for cybersecurity and data protection covering all aspects of the evolving information security. JTC 13 has several liaisons including JTC 8 Privacy management and ETSI TC (Technical Committee) Cyber. The current activities of JTC 13 are twofold. First, the transposition of international standards (27 standards in total) like the ISO/IEC 27K series and others such as the ISO/IEC 29100 Privacy framework, and ISO/IEC 19790 Security requirements for cryptographic modules. Second, feasibility studies include the feasibility study on Small Business Standards (SBS) ISO 27001 Guide for SMEs, lightweight evaluation methods (other than as proposed by ISO/IEC 15408), a data protection interface and data protection professional profiles. The JTC 13 representative concluded that SME needs are a strong driver to ease the knowledge and use of International and European standards.

The ETSI TC Cyber representative who gave an overview of the committee and described the diverse scope of areas they are working on. The speaker pointed out the BSI / PETRAS white paper (BSI, 2019) which reports on the following:

- Opportunities and challenges that IoT (Internet of Things) SMEs and start-ups face when developing connected products.
- SME's priority areas for standardisation.
- Accessible summary of the IoT policy and standards landscape.

The ETSI TC Cyber representative addressed the ETSI technical specification 103 645 - Cyber Security for Consumer Internet of Things as the first globally-applicable industry standard on consumer IoT security (ETSI, 2019). It is agreed to transpose TS 103 645 into a European Standard (EN). A European Standard (EN) automatically becomes a national standard in each of the 34 CEN-CENELEC member countries. In addition, a test specification is being considered to sit alongside TS 103 645. The speaker informed the attendees that there is an opportunity for SMEs and ETSI members to contribute to these documents.

A CEN-CENELEC participant pointed out there is no or poor follow up for the standardisation proposals. According to the participant, a reason for this might be it is being a prolonged process.

5.4.4.3 SME Alliances

The representative from Digital SME alliance introduced the alliance that is the first European association in the ICT sector exclusively focused on SMEs. The speaker gave some figures regarding cybersecurity statistics for SMEs as follows (Mansfield, 2017):

- 43% of cyberattacks target small business.
- 14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
- 60% of small companies go out of business within six months after a cyberattack.

The speaker pointed out their important publication "SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management" (SBS, Digital SME Alliance, 2018) which is currently under consideration for adoption by CEN-

CENELEC. More ideas on cybersecurity standards for SMEs were introduced by the speaker as follows:

- Preparing a GDPR (General Data Protection Regulation) Guide for SMEs.
- Preparing a guide for SMEs on a consumer standard for IoT.
- Expanding the ISO27001 guide for SMEs (after review).
- Lightweight cyber schemes for SMEs, guide on specific IoT.

The representative from SBS joined the workshop remotely and presented the goals of SBS as to represent and defend SMEs' interests in the standardisation process at European and international levels, to raise the awareness of SMEs about the benefits of standards, and to encourage them to get involved in the standardisation process. The speaker commented that regarding the cyber domain and standardisation, all cybersecurity aspects are covered (i.e. no significant gaps), but the following issues do exist:

- There are too many standards, and many are not actionable or particularly useful (entry barrier for SMEs).
- There is a need to converge toward useful, interoperable sets of standards.
- If not freely available on-line, constantly evolving, and well-versioned, there is a risk of low practical value.
- There is a need for broad industry & society, public-private support and adoption (multi-stakeholder holistic approach).
- The speaker pointed out SBS's position at ETSI TC CYBER for translating the standards for SMEs and proposed the following options for SDOs adapting standards for SMEs.
    - Evolution – new versions with specific levels to existing standards ("maturity levels"), adapted and applicable to SMEs.
    - Lightweight standard/requirements/recommendation – amend a special section for SMEs as "minimum requirements".
    - Develop new, specific standards for SMEs.
    - Combined requirements (or "guidelines/recommendations") – a "security pack" (cyber hygiene).

5.4.4.4 Cybersecurity Organisations

The representative from ECSO WG1 Standardisation, certification, labelling and supply chain management (ECSO, 2019a) gave an overview of ECSO which has 251 member organisations among which 20-25% are SMEs. It was stated that ECSO unites and represents European cyber security industry players, as well as national public administrations, research centres, SMEs, regions, and academia. The speaker pointed out ECSO's publication, the State of the Art Syllabus (SoTA) - Overview of existing cybersecurity standards and certification schemes (ECSO, 2017) which includes 290 standards and schemes, and is currently under

revision. There is currently a call for contribution to update this document. Furthermore, it is important to note that ECSO WG1 is collaborating with ETSI, CEN, CENELEC, ENISA and others.

The representative from ECSO WG4 (ECSO, 2019b) presented the strategy, objectives and achievements of their working group. ECSO WG4 focuses on the following:

- Support the development of SMEs, start-ups and high growth companies.
- Develop coordinated activities between clusters (both business-oriented and triple helix), regions and local bodies (for local implementation of solutions and educations).
- Development of East and Central EU public and private sectors dealing with cybersecurity.

The speaker introduced the ECSO SME HUB as a unique platform promoting "Cybersecurity Made in Europe" and the ECSO label as a private marketing tool fostering the claim of quality and security of European companies. It was pointed out that this label is not a certification tool, but aims to reflect three key messages: "made in Europe", "created and developed by ECSO" and "issued by a qualified organisation". The eligibility criteria to acquire this label were also presented.

5.4.4.5 EU Funded Projects Related to Cybersecurity for SMEs and ICT Standardisation

The SMESEC project's two-dimensional perspective was presented to the workshop attendees. These dimensions are the technical solution and the human and organisational context. The representative introduced the contribution opportunities for the SMESEC project to cybersecurity standardisation for SMEs by liaising and coordinating with relevant stakeholders.

In the SMESEC project, the CySME maturity model (SMESEC, 2018) is being developed as part of the framework. This maturity model will make self-assessment of cybersecurity capabilities for SMEs possible in a standards-transparent way. CySME questionnaires, which are a coherent collection of SME-specific quick scans on all SME-relevant cybersecurity focus areas with corresponding security controls and best practices from all existing cybersecurity-related standards, including ISO and ETSI, are being implemented by the CYSEC tool (Shojaifar, Fricker, & Gwerder, 2018). The CYSEC tool is also being developed as part of the SMESEC framework positioned as a self-reliant capability assessment, training and awareness platform for SMEs. The CySME maturity model (SMESEC, 2018) will help SMEs with their initiatives for self-assessing and improving cybersecurity capabilities in a standards-transparent way.

The SMESEC project aims to deliver a cybersecurity standardisation guide for SMEs that will facilitate their awareness.

The objectives of the StandICT.eu project were described as follows:

- Supporting the participation of EU experts in international ICT standardisation activities.
- Ensuring the promotion of European requirements and interests.
- Raising awareness on the advantages of adopting ICT Standards.

- Building strong motivation to businesses and SMEs, in addition to researchers, to contribute to the shaping of ICT Standards.

The StandICT.eu representative explained the tool "Standards Watch" (StandICT.eu, 2019) which monitors the status of ICT standards at the international level, mapping critical areas such as Cybersecurity, 5G, Cloud Computing, IoT, Big Data and Artificial Intelligence. The speaker also presented the latest figures, such as the number of funded applications, 154 for their first five open calls; 53 of these funded applications were related to cybersecurity.

Three StandICT.eu funding grantees presented their experiences. These three professionals fully engaged in the cybersecurity domain who showcased the European Gaps & Priorities addressed by their work with the support of the initiative.

5.4.5 Outcomes of the Workshop

The five most important cybersecurity standards gaps and needs identified at the workshop –along with the stakeholder group that raised the needs– can be summarised as follows.

1. SMEs need guides for implementing existing cybersecurity standards (SDOs and SME Alliances).
2. The cost of acquiring and implementing standards is a problematic issue for SMEs (SME Alliances).
3. SMEs would benefit from standards with maturity levels applicable to SMEs (SME Alliances)
4. SME-specific standards can be considered as an option to fulfil the needs of SMEs (SME Alliances).
5. EU funded research projects have standardisation as a task and can allocate resources, on the other hand, SDOs lack resources. There is no link between these two. Some action should be taken to tighten the connection that will benefit both sides (Policymakers, Influencers, Regulators).

As a result of the presentations and discussions during the workshop, the following were the additional highlights.

- CEN-CENELEC JTC13 is considering the adoption of SBS's guide for implementing ISO/IEC 27001 for SMEs.
- ETSI has recently published TS 103 645 - Cyber Security for Consumer Internet of Things impacting SMEs.
- During the workshop, ECSO announced that the new version of the SoTA syllabus document (ECSO, 2017) is being prepared and contributions are expected from the relevant parties.
- As the workshop helped establish the expectations of different stakeholders, an important proposed activity can be the contribution of the related stakeholders to the

revision of the two aforementioned documents (ECSO, 2017) (ETSI, 2019) as requested by ECSO and ETSI respectively.

- In addition, the SMESEC and StandICT.eu projects had the opportunity to gather insights from the participants to steer their future works. The outcomes of the workshop and planned and ongoing work are promising in the sense that will help to move the collective efforts forward.

5.5 Research agenda: Cybersecurity Standardisation for SMEs

The top 5 cybersecurity standards gaps and needs that the authors identified below result from both the multivocal literature searches and the workshop.

To build the research agenda, we performed a thematic analysis within the suggessions for the needs and gaps on cybersecurity standardisation for SMEs. Thematic analysis is used for identifying, analysing and reporting recurrent threads that emerge as important in describing a certain phenomenon (Braun & Clarke, 2006). In total, five themes were identified each representing a research gap in cybersecurity standardisation for SMEs. Each theme was then broken down to research questions. Figure 5.6 illustrates the process of thematic analysis using the process for one of the themes "Financial barriers of available standards by SMEs" (*Table 5-5*). In Figure 5.6, the first suggestion was identified during the workshop (see Section 5.4.4.3) and the other three suggestions were based on the literature (see Section 5.3.4).

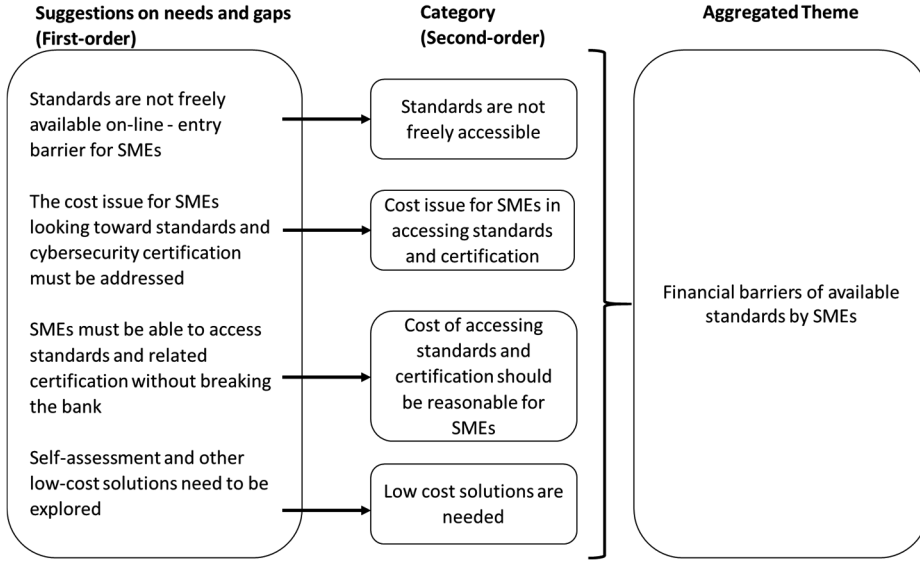


Figure 5.6 Thematic analysis process (example)

As a result of the thematic analysis, to better focus and integrate future research, the authors define corresponding research questions to address these gaps as a research agenda proposition in Table 5-5.

Gaps and Research Questions	
Gap 1: Lack of SMEs' awareness and involvement in standardisation processes	
RQ 1.1	How can SMEs' awareness and involvement in cybersecurity standardisation be improved?
Gap 2: Lack of cybersecurity standards specifically addressing SMEs	
RQ 2.1	How can standards incorporate organisations' maturity levels?
RQ 2.2	How can SME-specific standards be developed?
RQ 2.3	How can organisational characteristics be used in developing standards specifically for SMEs?
RQ 2.4	How do SME cybersecurity requirements differ by their role in the digital ecosystem?
Gap 3: Challenges of adapting existing cybersecurity standards for SMEs	
RQ 3.1	How can maturity levels applicable to SMEs be introduced in standards?
RQ 3.2	What are the barriers for SMEs in adapting standards?
RQ 3.3	How can existing standards be adapted to SME characteristics?
RQ 3.4	How can organisational characteristics be used in adapting existing standards to SMEs?
RQ 3.5	To what extent the extensive number of cybersecurity standards raise a barrier for SME standardisation?
RQ 3.6	How can the need to converge toward useful, interoperable sets of standards be addressed?
Gap 4: Financial barriers of available standards by SMEs	
RQ 4.1	How can SMEs acquire standards and certifications at an affordable price?
RQ 4.2	To what extent do consultancy, implementation and maintenance costs influence SMEs uptake of standards and certifications?
Gap 5: Lack of co-operation between the stakeholders	
RQ 5.1	How can a direct link between EU funded research projects on cybersecurity and SDOs be established?

Table 5-5 Agenda for Future Research

5.6 Conclusion

In standardisation research, prior work has emphasized the challenges and barriers for SMEs in standardisation. The importance of stakeholder identification in standardisation processes has also been pointed out before. This research set out to operationalize these observations by physically gathering the key stakeholders together in a workshop to identify their perspectives on the gaps in cybersecurity standardisation for SMEs.

This paper highlights the trends in the literature, identifies the state of the art in the European landscape, presents the key discussions and outcomes of the workshop and presents the themes, current initiatives, and plans towards cybersecurity standardisation for SMEs.

Furthermore, the SMEs' position regarding cybersecurity standardisation and gaps is presented from the stakeholders' point of views.

The findings from the multivocal literature search and the workshop were formulated to identify the Top 5 gaps in cybersecurity standardisation for SMEs and to propose an agenda for future research. Further research on the posed research questions would be useful to better address SMEs in cybersecurity standardisation.

The workshop also had some practical impacts on the participants. The participants had the opportunity to hear about the current happenings and recently published documents related to cybersecurity standardisation, to discuss the cybersecurity standardisation gaps and needs for SMEs, to hear about successful professionals' experiences working on cybersecurity standardisation, and to get in contact and network with other stakeholders. The participation, involvement and interest of the stakeholders in the workshop indicate their willingness to co-operate to address SMEs in cybersecurity standardisation.

To the best of our knowledge, this workshop was the first of its kind, focusing on cybersecurity standardisation for SMEs by bringing the related parties physically together. It would be beneficial if further workshops were organised to give especially SMEs (as the users of the standards) the opportunity to express their experiences about dealing with the challenges and their expectations regarding cybersecurity standardisation.

Although this research mainly addresses cybersecurity standardisation challenges that SMEs face, the proposed future research focus includes research questions applicable to other standardisation domains due to the generic– not cybersecurity specific– nature of some of the challenges. The literature study in this research presents SME standardisation initiatives of SDOs that are not specific to cybersecurity. The findings show that there are only a few standards that specifically address SMEs. These standards –all published by ISO– are in environmental management, innovation management and human resources management domains. ISO plays a leading role in providing SMEs with guidance on how to adapt existing standards. ETSI, with its recent board decision –to mandate that proposers of new standards describe their relevance to SMEs– has now taken another step forward to better support SME participation in standardisation processes.

Acknowledgements

This work was made possible with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

The authors wish to thank Philippe Cousin and Silvana Muscella for making the workshop possible. Philippe Cousin from the SMESEC project took a leading role in establishing stakeholders' involvement in the workshop and finalising the structure of the workshop. Silvana Muscella from the StandICT.eu project took a leading role in the logistics and organisation of the workshop.

Appendix

The search string S4 in *Table 5-1* resulted in 44 unique publications from Scopus and WoS. The detailed analysis of these publications is presented in *Table 5-2*. The list of relevant publications and non-relevant publications are presented in this appendix as two separate bibliographies as follows.

- The list of relevant unique publications (27 in total) resulting from the search string S4 (*Table 5-2*).

Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L., & Côté, I. (2015). A Pattern-Based and Tool-Supported Risk Analysis Method Compliant to ISO 27001 for Cloud Systems. In Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications (pp. 730–747). Retrieved from www.igi-global.com/article/a-pattern-based-and-tool-supported-risk-analysis-method-compliant-to-iso-27001-for-cloud-systems/123453

Bruderer, R., Villena, M., Tupia, M., & Bruzza, M. (2018). A cybersecurity model for mobile devices aimed at SMEs that use freelancers and BYOD schemes. 129–136. Retrieved from Scopus.

Chapman, D., & Smalov, L. (2004). On information security guidelines for small/medium enterprises. 3–9. Retrieved from Scopus.

Chiu, M., Lin, H. W., Nagalingam, S. V., & Lin, G. C. I. (2006). Inter-operabitity framework towards virtual integration of SMEs in the manufacturing industry. International Journal of Manufacturing Technology and Management, 9(3–4), 328–349. doi: 10.1504/IJMTM.2006.010061

Choez, C. G. P., & Llanos, F. D. C. (2018). Análisis de NIIF 9—Instrumentos Financieros desde una perspectiva industrial. Contabilidad y Negocios, 13(25), 6–19. doi: 10.18800/contabilidad.201801.001

Coles-Kemp, E., & Overill, R. (2007). The design of information security management systems for small-to-medium size enterprises. 47–54. Retrieved from Scopus.

Fagade, T. (2017). Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization. 15(5), 7.

Firoiu, M., & Bacivarov, I. C. (2016). Physical and logical security risk assessment procedure for smes, according to ISO/IEC 27005:2011 and sr iso 31000:2010 standards. Quality - Access to Success, 17(152), 86–98. Retrieved from Scopus.

García-Porras, C., Huamani-Pastor, S., & Armas-Aguirre, J. (2018). Information Security Risk Management Model for Peruvian SMEs. 2018 IEEE Sciences and Humanities International Research Conference (SHIRCON), 1–5. doi: 10.1109/SHIRCON.2018.8592994

Gattiker, U. E. (2008). Early warning system for home users and small- And medium-sized enterprises: Eight lessons learned. International Journal of System of Systems Engineering, 1(1–2), 149–170. doi: 10.1504/IJSSE.2008.018136

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. The TQM Journal, 23(4), 367–376. doi: 10.1108/17542731111139455

Koumpouros, Y., & Georgoulas, A. (2019). A systematic review of mHealth funded R&D activities in EU: Trends, technologies and obstacles. Informatics for Health and Social Care, 45(2), 168–187. doi: 10.1080/17538157.2019.1656208

Lyubimov, A., Cheremushkin, D., Andreeva, N., & Shustikov, S. (2011). Information security integral engineering technique and its application in ISMS design. 585–590. doi: 10.1109/ARES.2011.121

Mangin, O., Barafort, B., Heymans, P., & Dubois, E. (2012). Designing a process reference model for information security management systems. Communications in Computer and Information Science, 290 CCIS, 129–140. doi: 10.1007/978-3-642-30439-2_12

Medve, A. (2012). Model-based framework for integrated evolution of business and IT changes: Integrated evolution of business and IT changes. 255–260. Retrieved from Scopus.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing sme information security maturity. Journal of Computer Information Systems, 56(2), 106–115. doi: 10.1080/08874417.2016.1117369

Muthaiyah, S., & Zaw, T. O. K. (2018). ISO/IEC 27001 implementation in SMEs: Investigation on management of information assets. Indian Journal of Public Health Research and Development, 9(12), 2631–2637. doi: 10.5958/0976-5506.2018.02112.5

Polverini, D., Ardente, F., Sanchez, I., Mathieux, F., Tecchio, P., & Beslay, L. (2018). Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process. Computers & Security, 76, 295–310. doi: 10.1016/j.cose.2017.12.001

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a cyber security label for SMEs: A european perspective. 2018-January, 426–431. Retrieved from Scopus.

Ponsard, Christophe, & Grandclaudon, J. (2019). Survey and Guidelines for the Design and Deployment of a Cyber Security Label for SMEs. In P. Mori, S. Furnell, & O. Camp (Eds.), Information Systems Security and Privacy (pp. 240–260). doi: 10.1007/978-3-030-25109-3_13

Rizzo, C. (2010). ETSI security standardization. 3, 315–320. Retrieved from Scopus.

Rizzo, C. (2011). ETSI security standardization. 633–638. doi: 10.1109/ICRMS.2011.5979345

Sanchez, L. E., Villafranca, D., Fernandez-Medina, E., & Piattini, M. (2007). Developing a model and a tool to manage the information security in small and medium enterprises. 355–362. Retrieved from Scopus.

Sánchez, L. E., Villafranca, D., Fernández-Medina, E., & Piattini, M. (2008). Practical application of a security management maturity model for SMES based on predefined schemas. 391–398. Retrieved from Scopus.

Shojaie, B., Federrath, H., & Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. 2015 10th International Conference on Availability, Reliability and Security, 159–167. doi: 10.1109/ARES.2015.25

Valdevit, T., & Mayer, N. (2010). A gap analysis tool for SMES targeting ISO/IEC 27001 compliance. 3 ISAS, 413–416. Retrieved from Scopus.

Van Akkeren, J., & Harker, D. (2003). The mobile Internet and small business: An exploratory study of needs, uses and adoption with full-adopters of technology. Journal of Research and Practice in Information Technology, 35(3), 205–219.

Retrieved from http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT35/JRPIT35.3.205.pdf

- The list of non-relevant unique publications (17 in total) resulting from the search string S4 (Table 5-2).

6th International Conference on Software Process Improvement, CIMPS 2017. (2018). Advances in Intelligent Systems and Computing, 688, 1–304. Retrieved from Scopus.

20th Americas Conference on Information Systems, AMCIS 2014. (2014). Presented at the 20th Americas Conference on Information Systems, AMCIS 2014. Retrieved from Scopus.

Bozanic, Z., Dirsmith, M. W., & Huddart, S. (2012). The social constitution of regulation: The endogenization of insider trading laws. Accounting, Organizations and Society, 37(7), 461–481. Retrieved from https://ideas.repec.org/a/eee/aosoci/v37y2012i7p461-481.html

EmergiTech (Conference), University of Technology, M., & Institute of Electrical and Electronics Engineers. (2016). 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech): Date, 3-6 Aug. 2016. Retrieved from http://ieeexplore.ieee.org/servlet/opac?punumber=7728913

Flores, Y., Shah, K., Lazcano, E., Hernández, M., Bishai, D., Ferris, D. G., … Morelos HPV Study Collaborators. (2002). Design and methods of the evaluation of an HPV-based cervical cancer screening strategy in Mexico: The Morelos HPV Study. Salud Publica De Mexico, 44(4), 335–344. doi: 10.1590/s0036-36342002000400007

Gervasi, O., Murgante, B., Misra, S., Borruso, G., Torre, C. M., Rocha, A. M. A. C., … Cuzzocrea, A. (2017). Computational Science and Its Applications – ICCSA 2017: 17th International Conference, Trieste, Italy, July 3-6, 2017, Proceedings. Springer.

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019, March 31). Data Protection and Security in SMEs under Enterprise Infrastructure. Retrieved March 13, 2020, from AGRIS on-line Papers in Economics and Informatics website: https://ageconsearch.umn.edu/record/294142

Hölbl, M., & Welzer, T. (2009). Two improved two-party identity-based authenticated key agreement protocols. Computer Standards & Interfaces, 31(6), 1056–1060. doi: 10.1016/j.csi.2008.09.024

Li, L., Xia, Z., Hadid, A., Jiang, X., Zhang, H., & Feng, X. (2019). Replayed Video Attack Detection Based on Motion Blur Analysis. IEEE Transactions on Information Forensics and Security, 14(9), 2246–2261. doi: 10.1109/TIFS.2019.2895212

Oreshkov, V. V., Energy, L. T., Nikolaychuk, A. V., Shevchenko, A. P., Salishchev, A. D., Gnuskov, M. V., … Region, J. T. V. (2018). Forecast for development of methods and means of Russian energy systems management. doi: 10.28999/2541-9595-2018-8-4-469-479

Ponsard, C., & Deprez, J.-C. (2018). Helping SMEs to better develop software: Experience report and challenges ahead. 213–214. doi: 10.1145/3183519.3183553

Proceedings of 12th Australian Information Security Management Conference, AISM 2014. (2014). Presented at the Proceedings of 12th Australian Information Security Management Conference, AISM 2014. Retrieved from Scopus.

Smentkowski, V. S., Ostrowski, S. G., & Keenan, M. R. (2009). A comparison of multivariate statistical analysis protocols for ToF-SIMS spectral images. Surface and Interface Analysis, 41(2), 88–96. doi: 10.1002/sia.2973

Success of a Cervical Cancer Screening Program: Trends in Incidence in Songkhla, Southern Thailand, 1989-2010, and Prediction of Future Incidences to 2030. (2014). Asian Pacific Journal of Cancer Prevention, 15(22), 10003–10008. Retrieved from http://journal.waocp.org/article_30215.html

Thapa, R. B., Matin, M. A., & Bajracharya, B. (2019). Capacity Building Approach and Application: Utilization of Earth Observation Data and Geospatial Information Technology in the Hindu Kush Himalaya. Frontiers in Environmental Science, 7. doi: 10.3389/fenvs.2019.00165

Wang, Y., Hassebrook, L. G., & Lau, D. L. (2010). Data Acquisition and Processing of 3-D Fingerprints. IEEE Transactions on Information Forensics and Security, 5(4), 750–760. doi: 10.1109/TIFS.2010.2062177

Yu, Y., Klauser, F., & Chan, G. (2009). Governing Security at the 2008 Beijing Olympics. The International Journal of the History of Sport, 26(3), 390–405. doi: 10.1080/09523360802602265

6 Cybersecurity Standardisation Essentials for SMEs

The complexity of the cybersecurity domain and abundance of cybersecurity standards entail expertise, cost and complexity challenges for small and medium-sized enterprises (SMEs). This chapter provides SMEs with the main concepts of cybersecurity and introduces a five-step process for establishing cyber-security using standards and frameworks. The chapter addresses and provides guidance for different types of SMEs according to their roles in the digital eco-system. Five widely used standards and frameworks that can be used to reduce the cybersecurity risks are introduced. A comparative analysis of these standards and frameworks is performed. This analysis resulted in 17 unified cybersecurity control categories that serve as a quick reference for SMEs. The five-step process is illustrated by an exemplar SME to facilitate the implementation of the process. The chapter can be used by SMEs as a "where-to-start" guideline for cybersecurity concepts, processes, standards and frameworks to initiate their own implementation.

This work has been accepted for publication as:

Yigit Ozkan, B., & Spruit, M.R. (In press). Cybersecurity Standardisation Essentials for European SMEs. In Fricker, S., Ruiz, J.F., & Tselios, C. (Eds.), *SMESEC: Protecting Small and Medium-sized Enterprises digital technology through an innovative cyberSECurity framework*. Springer.

NB: An extended version has been published by the European Telecommunications Standards Institute (ETSI) as technical report ETSI TR 103 787-1 V1.1.1 (2021-05)

6.1 Introduction

For the organisations that do not have prior cybersecurity experience, it is difficult to find a clue as to where to start their cybersecurity journey. Standards have been a trustworthy resource for individuals, organisations and governments who seek an answer to the question "What's the best way of doing this?" (ISO, 2019d) (ISO, 2019a). The International Standardization Organization[1] (ISO) states several benefits of standards for small to medium sized enterprises (SMEs) (ISO, 2018). According to ISO, standards can help SMEs to build customer confidence that their products are safe and reliable, to meet regulation requirements at a lower cost, to reduce costs across all aspects of their business, and to gain market access across the world.

As in every domain, standards on cybersecurity and information security are built on experience and best practices that may help organisations to cope with cyber threats. It might be difficult for SMEs to get into the almighty world of standards. To date, cybersecurity standardisation of SMEs has received scant attention in the research literature (Ozkan & Spruit, 2019). Nevertheless, the European Standards Developing Organisations (CEN[2], CENELEC[3] and ETSI[4]), SME Alliances (the European Digital SME Alliance[5], SBS[6]) and cybersecurity organisations (ECSO[7], ENISA) are putting in efforts to address the challenges that SMEs are facing.

In this chapter, we provide SMEs with the essential information on where to start establishing cybersecurity by implementing standards and frameworks.

First, we provide information on cybersecurity essentials by introducing the main concepts (i.e. threat, vulnerability, attack, control, risk, etc.) and their relationships. This background information helps SMEs to follow the chapter more easily.

Second, we propose a five-step process that can be followed by SMEs to establish and improve cybersecurity using the standards and frameworks. This process provides SMEs with a quick-starting point. To facilitate the execution of the five-step process for different types of SMEs, we use the SME categories (see Table 6-1) proposed by the Digital SME Alliance according to SMEs' roles in the digital ecosystem. This categorisation was proposed by the Digital SME Alliance in regard to addressing SME requirements in cybersecurity solutions and standards (The European Digital SME Alliance, 2020a).

Third, we introduce the following five well-known cybersecurity standards and frameworks that can be used throughout the five-step process:

1. Cyber Essentials (UK),
2. The Centre for Cyber Security Belgium SME Guide (Belgium),
3. Center for Internet Security (CIS) Controls (USA), ETSI TR 103 305-1 (Europe),
4. NIST Small Business Information Security (USA),

[1] International Standardization Organization (ISO; www.iso.org)

[2] European Committee for Standardization (CEN; https://www.cen.eu/)

[3] European Committee for Electrotechnical Standardization (CENELEC; https://www.cenelec.eu/)

[4] European Telecommunications Standards Institute (ETSI; https://www.etsi.org/)

[5] European Digital SME Alliance (https://www.digitalsme.eu/)

[6] Small Business Standards (SBS; https://www.sbs-sme.eu/)

[7] European Cyber Security Organisation (ENISA; https://ecs-org.eu/)

5. ISO/IEC 27002 Code of practice for information security controls (International).

Fourth, we present a comparative analysis of these five cybersecurity standards and frameworks to provide a unified set of security controls. The granularity of the controls differs in these standards and frameworks. However, by analysing them we present 17 unified control categories that can be applied in organisations for reducing their cybersecurity risks. The comparative analysis helps SMEs to be able to have a unified set of controls from different sources, and enables them to further focus on specific controls by easily referring to the controls in each of the standards and frameworks.

Fifth, we further elaborate on the SME categories (Table 6-1) proposed by the Digital SME Alliance (The European Digital SME Alliance, 2020a). Based on the implementation guidelines provided by CIS (Center for Internet Security, 2020), we present guidance on how to use the comparative analysis and which controls might be applicable for different SME categories. This enables SMEs to get tailored guidance for selecting controls with respect to their role in the digital ecosystem.

Finally, we illustrate (with an exemplar SME) how the five-step process and the five cybersecurity standards and frameworks can be used by SMEs. This enables SMEs to understand the five-step process better. The final section provides an overview of practical impacts and concludes the paper.

SME Category	Description
Digital enablers	SMEs that are active in developing and providing cybersecurity solutions.
Digitally based	SMEs that are highly dependent on digital solutions for their business.
Digitally dependent	SMEs that depend on digital solutions as end users.
Start-ups	SMEs that neglect or are not well aware of cybersecurity and require specific measures and incentives to adopt cybersecurity solutions.

Table 6-1 SME Categories According to Their Roles in the Digital Ecosystem (The European Digital SME Alliance, 2020a)

6.2 Background: What SMEs Need to Know About Cybersecurity?

In this section, firstly, we present the position of cybersecurity and information security with respect to the other disciplines in the security domain. Secondly, we describe the main objectives of cybersecurity and information security. Thirdly, we introduce the concepts of threat, control and risk which are important to better understand what could cause harm to security.

The domains of information security and cybersecurity are quite intertwined. ISO and the International Electrotechnical Commission (IEC) have been developing and publishing many international standards, including the ISO/IEC 27032 guideline for cybersecurity. This standard presents the relationships between cybersecurity, information security and other security domains as shown in Figure 6.1 below.

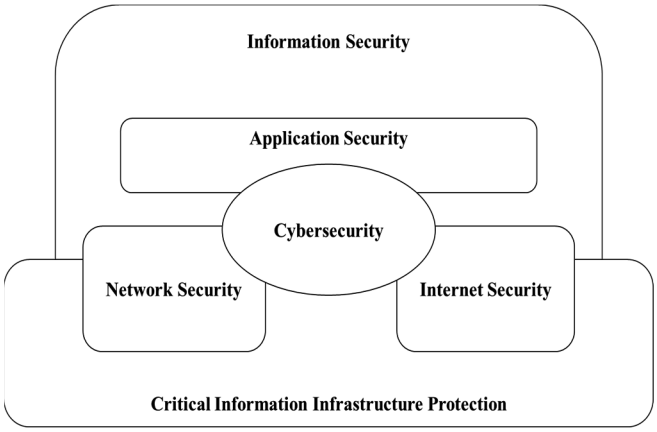


Figure 6.1 Relationships between Cybersecurity and Other Security Domains (redrawn from ISO/IEC 27032 (ISO/IEC, 2012)

The ISO/IEC 27032 standard defines the relationship between cybersecurity and other security domains as follows. Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks. It has a unique scope requiring stakeholders to play an active role in order to maintain, if not improve the usefulness and trustworthiness of the Cyberspace. (ISO/IEC, 2012).

A basic definition of cybersecurity is *"protecting your computer-based equipment and information from unintended or unauthorised access, change, theft or destruction*"(UK Government, 2015). A basic definition of information security is "*preservation of confidentiality, integrity and availability of information*" (ISO/IEC, 2018a). These definitions bring us to the three main objectives of cybersecurity and information security: Confidentiality (C), Integrity (I) and Availability (A). These three objectives (also known as the CIA triad) are described as follows and depicted in Figure 6.2. It is deemed important to know these concepts for any organisation since the principle for establishing security is to make sure these aspects of organisational information are protected.

Confidentiality is protecting the information from disclosure to unauthorised parties. According to ISO/IEC 27000, confidentiality is defined as *property that information is not made available or disclosed to unauthorised individuals, entities, or processes* (ISO/IEC, 2018a).

Integrity is protecting the information from unauthorised modification or destruction. According to ISO/IEC 27000, integrity is defined as a *property of accuracy and completeness* (ISO/IEC, 2018a).

Availability is ensuring that authorised parties are able to access the information when needed. According to the ISO/IEC 27000, availability is defined as *property of being accessible and usable on demand by an authorised entity* (ISO/IEC, 2018a).

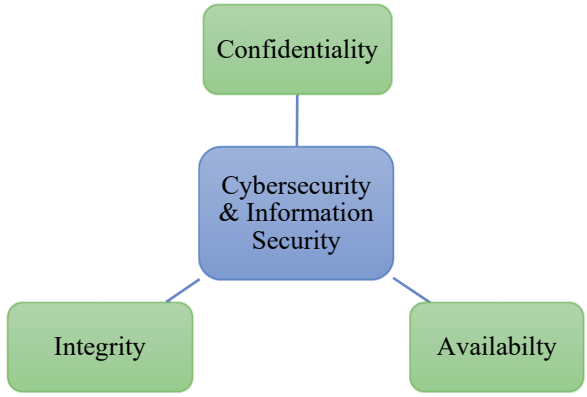


Figure 6.2 Confidentiality, Integrity and Availability (CIA) Triad

The World Economic Forum publishes annual global risk reports. The 2020 report revealed that cyberattacks are in the 7th and 8th place in the Top 10 risks with respect to the likelihood and impact, respectively. In 2021, cybercrime damages are estimated to reach US$6 trillion (World Economic Forum, 2020). Cyberattacks have both short term and long term economic impacts in terms of losses and expenses (Gañán et al., 2017).

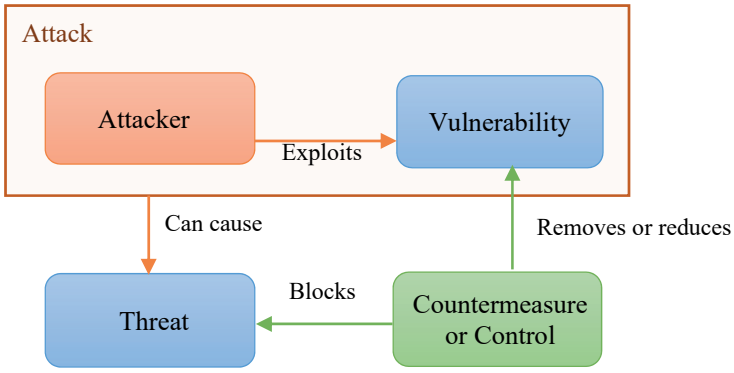


Figure 6.3 Threat-Vulnerability-Control Paradigm (Pfleeger, Pfleeger, & Margulies, 2015)

Cybersecurity and information security are all about risk management. Every company has valuable assets to protect (to protect the CIA of these assets) and assets might have different vulnerabilities contributing to different risks. Since not all risks can be eliminated, the organisations need to decide what risks they can accept and what risks they need to mitigate. The cybersecurity and information security risks that an organisation faces are associated with its operating environment (both external and internal), and the measures should be driven by the needs and expectations of interested parties.

These vulnerabilities of the assets might be exploited by threats. This might cause a risk. Countermeasures (i.e. controls) should be implemented to mitigate the risks. For example, an organisation might have a web server (asset) which is crucial to its business. There could be cyber-attacks (attack) such as a Denial of Service (DoS) targeted to this web server. If the webserver does not have the latest security patches (vulnerability), the attacker may exploit this vulnerability causing a threat to the organisation. The probability of this scenario happening and the impact of it on the organisation constitutes the risk. The organisation has options to reduce or remove the vulnerability of the webserver by applying the latest security patches. Another option might be detecting and blocking the DoS attack. Figure 6.3 illustrates the relationships between a threat, a vulnerability and a control.

6.3 The Five-Step Process to Establish and Improve Cybersecurity for SMEs

The five-step process for establishing and improving cybersecurity in an organisation by using frameworks, standards and certification schemes is depicted in Figure 6.4. These steps are derived from the ISO/IEC 27001 standard's **Planning** clause (ISO/IEC, 2013a). To understand the five-step process better, we encourage the reader to check the illustrative example in the section "Exemplary Application" below.

This five-step process should be considered as the beginning of a long and never-ending journey. New vulnerabilities and threats will always exist given the ever-changing technologies. The aim of the monitor and improve step is to ensure the adaptation of the organisations to emerging security requirements.

The following sections describe the process steps in detail.

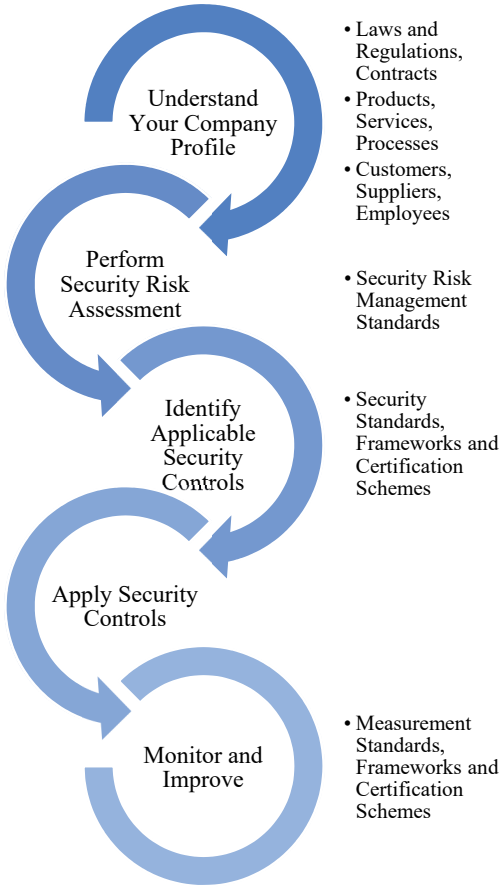


Figure 6.4 The Basic Process for Establishing and Improving Cybersecurity by Using Frameworks, Standards and Certification Schemes (based on the Planning clause of the ISO/IEC 27001 standard (ISO/IEC, 2013a)). There are more steps in this standard clause to fulfil all the requirements of an Information Security Management System (ISMS). Here, the process is simplified for starting a quick implementation to use standards for establishing in-formation security (or cybersecurity).

(Step 1) Understand Your Company Profile

The first step is about understanding the organisation and its context. The internal and external issues play a role in understanding the context of the organisation and its ability to establish and improve cybersecurity. This step is directly related to the **Context of the organisation** clause of the ISO/IEC 27001 standard (ISO/IEC, 2013a).

The following questions can help to understand the internal and external issues:

- How is our organisational structure? What are the main roles in the organisation?
- What products and services do we provide?
- What processes do we have?
- What regulatory and contractual obligations do we have?

- What are our objectives?
- What resources do we have? (Including employees, systems, equipment, etc.)
- Who are our customers and suppliers?
- Who are the interested parties for our cybersecurity efforts?
- What are the needs and expectations of these parties?

In the following paragraphs, we provide resources that aim to address different SMEs according to their organisational context:

In case you provide products and/or services as an SME, you need to ensure that your products and services meet the security requirements. These security requirements may stem from cybersecurity certification schemes. The EU Cybersecurity Act creates a framework (EC, 2017) for European Cybersecurity Certificates for products, processes and services that is valid throughout the EU (EC, 2018). A recent ENISA publication elaborates on standards and the role of Standards Developing Organisations (SDOs) in cybersecurity certification (ENISA, 2020).

Step 2, 3, and 4 of the five-step process are part of the risk management process. The ISO/IEC 27005:2018 standard specifically addresses information security risk management (ISO/IEC, 2018b). There is also a more generic risk management standard published by ISO which is ISO 31000 (ISO, 2018b). ISO/IEC 27000 defines the risk management process as *"the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk"* (ISO/IEC, 2018a). A generic risk management process is depicted in Figure 6.5.

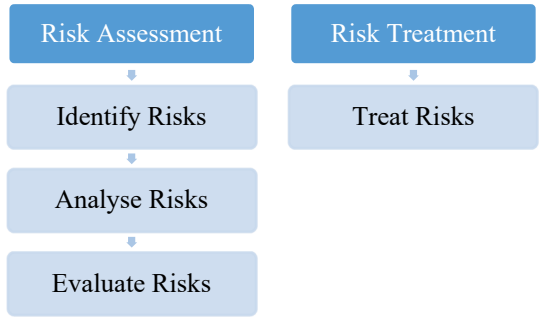


Figure 6.5 Risk Management Process (based on the Planning clause of ISO/IEC 27001(ISO/IEC, 2013a))

(Step 2) Perform Security Risk Assessment

The risk assessment process should follow predefined, repeatable and traceable steps. At this stage, risk acceptance criteria should be identified including the regulatory and contractual requirements and business objectives.

Step 1 - Identify Risks: In this step, the organisation should consider its assets (any item valuable to the organisation), the vulnerabilities of these assets and the likelihood of possible threats. The value of the assets is associated with the way they are used by the business. For example, for an organisation providing e-commerce services to its customers, the computers hosting the e-commerce application are critical assets. Risk owners should be assigned at this stage. Cyber security risk taxonomies (i.e. (Cebula, Popeck, & Young, 2014a)), threat taxonomies (i.e. (Marinos, 2016a)) and risk reports (i.e. (World Economic Forum, 2020)) may help organisations identifying their risks.

Step 2 - Analyse Risks: This step involves assessing the potential impact and realistic probability of the occurrence of the risks. Risk level is determined based on the impact and the probability of the risk. Risk level can be formulated as a function of impact and probability of a security event as follows:

$$R = f(impact \times probability)$$

The impact of a loss of confidentiality, integrity and availability should all be considered. The risk can be quantified using the designated impact and probability.

Step 3 - Evaluate Risks: The quantified risks should be compared against the preset risk acceptance criteria and prioritised by their level for risk treatment.

(Step 3) Identify Applicable Security Controls (Risk Treatment)

Risk treatment is a step in the risk management process (see Figure 6.5). According to ISO/IEC 27000, possible options for risk treatment include (1) reducing the risks by applying controls, (2) accepting risks according to the risk acceptance criteria, (3) avoiding risks by not allowing actions that would cause the risks to occur, and (4) sharing the risks to other parties such as insurers (i.e. cyber insurers) or suppliers. If the organisation decides the first option (reducing the risks), controls (i.e. countermeasures) need to be selected and implemented.

In this chapter, a comparative analysis of five well-known standards and frameworks for cybersecurity controls from different countries and sources is presented to provide a quick reference of control categories (17 in total) for SMEs (see *Table 6-2*). To identify the applicable controls, at this step, we encourage SMEs to refer to section "Four Categories of SMEs in Cybersecurity Context" to identify the category of their company regarding its role in the digital ecosystem. In the aforementioned section, guidance to identify applicable controls per SME category is provided.

There are three types of controls. Physical controls (locks, access-controlled rooms, security guards, etc.), procedural or administrative controls (laws, regulations, policies, contracts, agreements, operational procedures, trainings etc.) and technical controls (firewalls, encryption, malware protection programs, etc.) (Pfleeger et al., 2015).

As described in the previous section, a comparative analysis of 17 control categories from different standards and frameworks are introduced in *Table 6-2*.

(Step 4) Apply Security Controls (Risk Treatment)

An implementation plan can be prepared for the application of identified security controls at the organisation. The CEO can prepare such an implementation plan or they can delegate this to someone in the organisation. The prioritisation of the tasks should be aligned with the prioritisation of the associated risks. There should be people responsible for the implementation of selected controls who are capable in terms of time and knowledge. SMEs might not have the necessary resources to implement the technical controls. In this case, using services from consultancy firms should be considered.

(Step 5) Monitor and Improve

The identified risks should be monitored and reviewed regularly (at least annually). Reviews should be carried out after any change in the organisation that may affect the risks. The necessary risk management steps should be conducted again if required.
To ensure that the security controls are functioning as expected, they need to be monitored and reviewed. This step also contributes to the overall evaluation and improvement efforts to establish cybersecurity. There are several standards that can help in monitoring and improving the controls that are chosen to be applied.
ISO/IEC 27004 explains how to develop and operate measurement processes, and how to assess and report the results of a set of information security metrics. The Center for Internet Security (CIS) Controls Measures and Metrics document presents a list of measures for each control that can be used to monitor and improve the applied controls ("CIS Controls V7 Measures & Metrics," 2018). Although the ISO/IEC/IEEE 15939 standard is focused on systems and software engineering, it provides a generic framework on how to establish a measurement process in an organisation.

Apart from the monitor and improve step, process evaluations, certification and compliance audits are some of the other tools to ensure that the security controls are functioning as expected and the risk management processes are effective.

6.4 Five Cybersecurity Frameworks and Standards for SMEs and their Comparative Analysis

In this section, five different frameworks and standards are introduced. These frameworks and standards provide organisations (some of them specifically focus on SMEs) with security controls that could be applied for risk treatment. The decision of selecting controls to apply should normally be based on the results of risk assessment of the organisations. Some of the standards and frameworks that are presented below include a number of controls that could be applied even before a comprehensive risk assessment. The aim of providing organisations with such a basic set of controls is to support them against the basic threats that they could face. Applying additional controls should be a cost/benefit analysis decision that should be taken by the organisation given their limited resources (especially for start-ups). We will refer to the standards and frameworks (SF) in the given order as SF1, SF2 and so on.

SF1 - Cyber Essentials *(UK)* is a cybersecurity scheme backed by the UK government and operated by National Cyber Security Centre (NCSC) of the UK government. Cyber Essentials provides organisations with a set of fundamental controls against threats coming from the internet (NCSC, 2020).

Cyber Essentials includes two levels of certification as follows. In Cyber Essentials scheme, organisations perform self-assessment against five basic security controls and a qualified assessor verifies the information provided. In the Cyber Essentials Plus scheme, a qualified assessor examines the same controls, testing that they work through a technical audit. To learn more about certification, the IASME consortium website can be visited[8]. The latest self-assessment preparation questionnaire can also be downloaded[9].

SF2 - The Centre for Cyber Security Belgium SME Guide *(Belgium)* was developed by the Centre for Cyber Security Belgium in partnership with the Cyber Security Coalition Belgium for small and medium-sized enterprises [18]. It is based on input and best practices from private and public entities (Centre for Cyber security Belgium, 2017). SMEs can use the list of 12 cyber security topics with basic and advanced cybersecurity recommendations against data breaches and cyber-attacks. The SME guide is freely accessible online[10].

SF3 - Center for Internet Security (CIS) Controls (USA) and **ETSI TR 103 305** (Europe) are published by CIS and ETSI, respectively. The Center for Internet Security (CIS) is a nonprofit organisation based in United States with members including large corporations, government agencies, and academic institutions. The latest version of CIS Controls is freely accessible online[11].

In version 7.1 of the CIS Controls, based on the following three characteristics, three Implementation Groups (IG) are defined:

- Data sensitivity and criticality of services offered by the organization.
- Expected level of technical expertise exhibited by staff or on contract.
- Resources available and dedicated toward cybersecurity activities.

The implementation groups are defined as IG 1, IG 2 and IG 3. The following could be considered as examples of organisations in these IGs.

IG 1: An IG 1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. This group corresponds to the Start-ups SMEs in Table 6-1.

IG 2: An IG 2 organization employs individuals responsible for managing and protecting IT infrastructure. This group corresponds to the Digital Dependent SMEs in Table 6-1.

IG 3: An IG 3 organization employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, and application security).

[8] https://iasme.co.uk/

[9] https://iasme.co.uk/wp-content/uploads/2020/03/Cyber-Essentials-only-question-booklet-v11b.pdf

[10] https://ccb.belgium.be/en/document/guide-sme.

[11] https://learn.cisecurity.org/cis-controls-download

This group corresponds to both the Digital Enabler and Digitally Based SMEs in Table 6-1.

Even though this IG approach provides guidance for prioritizing usage of the CIS Controls, CIS advises that organisations should better base their decisions on their organisation's risk assessment. CIS includes 20 controls and 171 sub-controls. The assignment of controls to IGs is done at the sub-control level. IG 1 includes the minimum set of sub-controls. IG2 has additional sub-controls for IG 2 and the same is valid for IG 3 that includes the full set of 171 sub-controls.

ETSI has published technical report ETSI TR 103 305-1 'The Critical Security Controls V3.1.1' (ETSI, 2018a) that is technically equivalent and compatible with CIS Controls, Version 7.0 of the Center for Internet Cybersecurity.

SF4 - NIST Small Business Information Security (USA) is published by the National Institute of Standards and Technology (NIST) of the USA as a cybersecurity reference guideline for small businesses. The aim of the guideline is to help SMEs establishing and improving cybersecurity in non-technical language which is freely accessible (Paulsen & Toth, 2016). In this guide, recommendations are organised by the five Cybersecurity Framework Core Functions (Identify, Protect, Detect, Respond and Recover). There are 20 recommended actions in total under these categories. In addition, the guide provides 9 other recommendations towards users and employees. This guidance also includes some worksheets to help SMEs on how to conduct risk assessment. Sample policy and procedures statements are also provided in the appendices.

SF5 - ISO/IEC 27002 Code of Practice for Information Security Controls *(International)* provides best practice recommendations on information security controls for initiating, implementing or maintaining information security management systems (ISMS) taking into consideration the organization's information security risk environment(s) (ISO/IEC, 2013b).

The ISO/IEC 27001 standard (ISO/IEC, 2013a) defines the requirements for an Information security management system. In Annex A of this standard, reference control objectives and controls are listed that could be applied to reduce information security risks. The ISO/IEC 27002 standard provides detailed guidelines for implementing these controls. There are 114 controls in 14 clauses included in the ISO/IEC 27002 standard.

6.5 Standards and Frameworks for Security Controls – A Comparative Analysis

In this section a comparative analysis of the five standards and frameworks presented above is given (*Table 6-2*). It should be noted that physical and environmental controls are listed in this analysis only for the Incident and Continuity Management controls. Although, as part of the ISO 27002 standard, physical and environmental controls have 15 sub-controls, the other four standards do not include corresponding controls. This is because physical and environmental controls are not considered as part of cybersecurity. In the last column of *Table 6-2*, "Additional Standards to Consider" are presented. These standards are the specific standards that address the associated controls in detail. The ISO/IEC 27000 series of standards include specific standards that address some of the controls elaborately. All of the standards in this series can be accessed on ISO's standards search webpage[12].

[12]https://www.iso.org/search.html?q=27000&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard

#	Control Category	[1] Cyber Essentials (UK)	[2] The Centre For Cyber Security Belgium SME Guide (Belgium)	[3] Center for Internet Security (CIS) (USA) + ETSI TR 103 305-1 (Europe)	[4] NIST Small Business Information Security (USA)	[5] ISO/IEC 27002 Code of Practice for Information Security Controls	Additional Standards to Consider
1	*Management commitment and policies*		- Involving Top Management - Publish a Corporate Security Policy and a Code of Conduct		- Create policies and procedures for information security	6 Organizing information security 5 Information security policies	
2	*Asset Management*		- Manage Your Key ICT Assets	- Inventory and Control of Hardware Assets - Inventory and Control of Software Assets	- Identify what information your business stores and uses - Determine the value of your information - Develop an inventory - Dispose of old computers and media safely	8 Asset management	
3	*Patch Management*	- Patch Management	- Update All Programs	- Continuous Vulnerability Management	- Patch your operating systems and applications	12 Operations security	
4	*Access Control*	- Access Control	- Manage Access To Your Computers And Networks	- Controlled Use of Administrative Privileges - Controlled Access Based on the Need to Know - Account Monitoring and Control	- Use strong passwords - Limit employee access to data and information - Identify and control who has access to your business information - Require individual user accounts for each employee	9 Access control	
5	*Secure Computers, Servers and Network Configuration*	- Secure Configuration	- Secure Workstations and Mobile Devices - Secure Servers and Network Components	- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	- Use separate personal and business computers, mobile devices, and accounts - Do not connect personal or untrusted storage devices or hardware into your computer, mobile device, or network	12 Operations security 13 Communications security	
6	*Log Management*			- Maintenance, Monitoring and Analysis of Audit Logs	- Maintain and monitor logs	12 Operations security	
7	*Email and Web Security*			- Email and Web Browser Protections	- Set up web and email filters - Be careful downloading software - Watch for harmful pop-ups - Be careful of email attachments and web links - Conduct online business more securely	12 Operations security	
8	*Malware Protection*	- Malware Protection	- Install Antivirus Protection	- Malware Defenses	- Install and update anti-virus, -spyware, and other malware programs	12 Operations security	
9	Network and Communications Security	- Boundary firewalls	- Secure Servers And Network Components - Secure Remote Access	- Limitation and Control of Network Ports, Protocols, and Services - Secure Configuration for Network Devices, such as Firewalls, Routers and Switches - Boundary Defense - Wireless Access Control - Penetration Tests and Red Team Exercises	- Install and activate software and hardware firewalls on all your business networks - Secure your wireless access point and networks	13 Communications security	- ISO/IEC 27033 – Network security

#	Control/ Process	[1] Cyber Essentials (UK) – SF1	[2] The Centre For Cyber Security Belgium SME Guide (Belgium) – SF2	[3] Center for Internet Security (CIS) (USA) + ETSI TR 103 305-1 (Europe) – SF3	[4] NIST Small Business Information Security (USA) – SF4	[5] ISO/IEC 27002 Code of Practice for Information Security Controls – SF5	Additional Standards to Consider
10	*Back-up and Recovery Management*		- Backup All Information	- Data Recovery Capabilities	- Make full backups of important business data/information - Make incremental backups of important business data/information	12 Operations security	
11	*Data Protection and Encryption*			- Data Protection	- Use encryption for sensitive business information	10 Cryptography 18 Compliance	
12	*Awareness and Training*		- Raise Staff Awareness of Cyber Risks	- Implement a Security Awareness and Training Program	- Train your employees - Do not give out personal or business information	7 Human resource security	
13	*Secure Development*			- Application Software Security		14 System acquisition, development and maintenance	- ISO/IEC 27034: Application security, OWASP Top 10, PSI Security Standards
14	*Incident and Continuity Management*		- Have a Business Continuity and an Incident Handling Plan	- Incident Response and Management	- Install Surge Protectors and Uninterruptible Power Supplies (UPS) - Develop a plan for disasters and information security incidents - Consider cyber insurance	11 Physical and environmental security 16 Information security incident management 17 Information security aspects of business continuity management	- ISO/IEC 2703: Incident management - ISO 22301: Business continuity management
15	*Human Resource Security*				- Conduct Background Checks - Pay attention to the people you work with and around	7 Human resource security	
16	*Improvement and Compliance*				- Make improvements to processes / procedures / technologies	16 Information security incident management 18 Compliance	- ISO/IEC 27035: Incident management - ISO/IEC 27004: Measure ment - ETSI TR 103 305 2: Measurement and auditing - ISO/IEC/IEEE 15939: Measurement process
17	*Supplier Relationships*					15 Supplier relationships	- ISO/IEC 27036: Information security for supplier relationships

Table 6-2 Standards and Frameworks for Security Controls – a Comparative Analysis

6.6 Four Categories of SMEs in Cybersecurity Context

As mentioned in the Introduction section, the European Digital SME Alliance recently published their position paper on the EU Cybersecurity Act and the role of standards for SMEs (The European Digital SME Alliance, 2020a). In this section, we further explain the four categories of SMEs within a cybersecurity context. ECSO's State of the Art Syllabus (ECSO, 2017) presents an overview of cybersecurity standards categorised by industry, products, components and services that might be useful for all categories of SMEs.

Digital Enabler SMEs are less likely to face challenges in adopting cybersecurity standards. Since they develop or provide cybersecurity solutions, they might focus on the certification of their products and/or services. Apart from developing and providing cyber secure solutions, these types of SMEs should protect their assets. They need to consider the security of their processes and of their information. Intellectual property rights (IPR) should be another aspect to consider for these type of SMEs as they might be working on innovative cybersecurity solutions.

According to the Center for Internet Security (CIS) criteria presented in section "Center for Internet Security (CIS) (USA) and ETSI TR 103 305 (Europe)", Digital Enabler SMEs correspond to the CIS's Implementation Group 3 (IG 3). The services offered by Digital Enabler SMEs are critical for the security of other organisations as well. These SMEs should refer to IG 3 of the CIS Controls and expand their implementation with the comparative analysis that we provide in *Table 6-2*. There is also another document of the CIS that provides sub-control level mapping of CIS Controls to ISO 27001 Annex1 and therefore ISO 27002 controls (CIS, 2019).

Digitally Based SMEs depend on digital solutions to run their businesses, according to their domain of operation (e.g. health, finance, critical infrastructures, e-government). Therefore they should be aware of related standards available and they need to adhere. According to the Center for Internet Security (CIS) criteria presented in section "Center for Internet Security (CIS) (USA) and ETSI TR 103 305 (Europe)", Digitally Based SMEs correspond to the Implementation Group 3 (IG 3). The business model of Digitally Based SMEs is dependent on digital solutions provided by their vendors. These SMEs should refer to IG 3 of the CIS Controls and expand their control implementation with the comparative analysis that we provide in *Table 6-2*. There is also another document of the CIS that provides sub-control level mapping of CIS Controls to ISO 27001 Annex1 and therefore ISO 27002 controls (CIS, 2019).

Digitally Dependent SMEs depend on ICT to run their businesses, according to their domain of operation (e.g. health, finance, critical infrastructures, e-government). Therefore, they should be aware of related standards available and they need to adhere. According to the Center for Internet Security (CIS) criteria presented in section "Center for Internet Security (CIS) (USA) and ETSI TR 103 305 (Europe)", Digitally Dependent SMEs correspond to the Implementation Group 2 (IG 2). The business model of Digital Dependent SMEs are dependent on ICT provided by their vendors. These SMEs should refer to IG 2 of the CIS Controls and expand their control implementation with the comparative analysis that we provide in *Table 6-2*.

Start-ups are defined as a sub-group of the first or second category (The European Digital SME Alliance, 2020a). Security has a low priority for the SMEs in this category. According to the alliance, this category of enterprises requires specific measures and incentives to adopt security standards. According to the Center for Internet Security (CIS) criteria presented in section "Center for Internet Security (CIS) (USA) and ETSI TR 103 305 (Europe)", Start-ups correspond to the Implementation Group 1 (IG 1). These SMEs should refer to IG 1 of the CIS Controls and expand their control implementation with the comparative analysis that we provide in *Table 6-2*.

6.7 Exemplary Application: Cybersecurity Essentials for SME "UP"

We encourage SMEs to read the background information provided in this chapter first to get familiar with the cybersecurity concepts. The next step is to follow the five-step process (Figure 6.4).

In this section, we will consider an exemplar SME which we will refer to as "UP" to present some tips on how to use the recommended five-step process presented in Figure 6.4. We would like to use our exemplar SME to help the reader better understand the provided cybersecurity essentials in a more actionable manner.

Our exemplar SME, UP, has a main business of providing an online platform for e-trainings. The CEO of the SME has read the annual risk reports (i.e. (World Economic Forum, 2020)) and was concerned about the security of her organisation and its online platform. She then reads this chapter. After understanding some basic terminology about cybersecurity (see Introduction), she follows the steps presented in Figure 6.4. We will follow the five-step process with the CEO.

Step 1: Understand Your Company Profile

To understand her company's profile, she answers the questions provided in the related section (see section 6.3, Step 1). She considers the following with respect to UP's profile. UP hosts an online training platform on a company-owned application server in an office they have in a science park. The online platform was developed internally by the UP software engineers. Currently, they have four servers and all employees use company-owned laptops to perform their daily work. UP has one human resources (HR) team member who is responsible for all HR related work. They do not have a deep hierarchical structure. A CEO (Chief Executive Officer), a CFO (Chief Financial Officer), three team leaders (Business Development Team, Pre-Sales and Customer Support Team and Development Team), nine team members report to these three team leaders and one HR employee. Their current customers are the companies that work in the same science park with them but UP wants to expand its business. She now has a better understanding of her company in terms of external (i.e. customers, suppliers.) and internal factors (i.e. employees, processes.) that may affect its cybersecurity.

Step 2: Perform Security Risk Assessment

She considers the online platform they provide to their customers, the threats they might have for this platform and the vulnerabilities that the software running on their application server might have. She then identifies the following risks associated with the threats and vulnerabilities she has thought of.

She thinks that an attacker can guess their application server administrator's password and shut their server down. She believes this risk has a low likelihood and a high impact.

She thinks that there might be vulnerabilities in the software that could allow DDoS (Distributed Denial of Service) attacks. *The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed* (OWASP Foundation, 2020). She believes this risk has a medium likelihood and a high impact.

Step 3: Identify Applicable Security Controls

Then, she wants to identify which controls she can apply to reduce these risks. She follows the guidance given at this step and she refers to section "Four Categories of SMEs in Cybersecurity Context" to identify the category of her company regarding its role in the digital ecosystem. She considers the presented categorisation of the Digital SME alliance and identifies her company as "Digitally Based".

Furthermore, she checks the recommendations for "Digitally Based" SMEs and understands that her company is in Implementation Group 3 (IG 3). In this recommendation, she is advised to implement all controls present in the Center of Information Security (CIS) Controls. She reads the comparative analysis of the standards and frameworks (*Table 6-2*) and gets familiar with them. In the comparative analysis, she identifies two control categories related to the risks that she has identified. The control category "Access Control" is related to strong passwords and "Secure Development" control category is related to application software security. She decides to investigate these controls deeper using the presented standards and frameworks. She easily finds the corresponding controls in the standards and frameworks using the comparative analysis provided in *Table 6-2*.

Step 4: Apply Security Controls

Risk #	Control Category	Control	Control Source (Table 6-2)	Task	Deadline	Responsible
1	Access Control	Use strong passwords	SF4	Ensure that the administrator passwords are strong.	01/08/2020	B.Y. Ozkan
2	Secure Development	System security testing	SF5	Ensure that security testing is performed.	01/09/2020	M.R. Spruit

Table 6-3 Control Implementation Plan Example

As advised in this step, she prepares an implementation plan for the controls that she has selected from the related standards and frameworks based on her risk assessment and prioritisation of the risks. An implementation plan example is shown in *Table 6-3*.
In the comparative analysis of the standards and frameworks (*Table 6-2*) She notices that there are specific standards and frameworks dedicated to application security (see the last column in *Table 6-2*). She decides that it might be good to investigate those; as she wants to expand her business and she wants to be sure that, their online training platform is cyber-secure. Figure 6.6 illustrates the asset, vulnerability, threat, and control relationship for the risks of the exemplar SME UP.

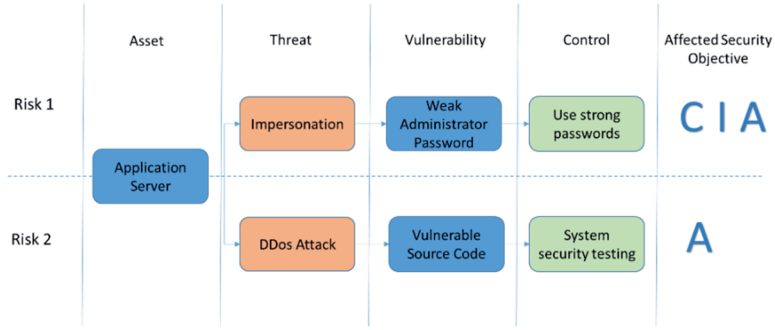


Figure 6.6 Asset, Threat, Vulnerability, Control Relationship for the Risks of SME "UP".

Figure 6.6 shows the asset at risk, vulnerabilities of the asset, the threats that may exploit those vulnerabilities to cause harm and the controls that are chosen to reduce the risks. The conceptual relationships between the assets, vulnerabilities, threats and controls are presented in Figure 6.3. The CIA triad is presented in Figure 6.2. Figure 6.6 presents the affected CIA objectives for the two risks identified for the exemplar SME UP. The cybersecurity risks of UP are certainly more than those two risks presented above. We highlighted these two risks to illustrate how to use the five-step process (Figure 6.4) presented in this chapter to start working on cybersecurity using standards and frameworks.

Step 5: Monitor and Improve

In this step, the CEO checks the status of the task in the implementation plan (*Table 6-3*) to take any necessary actions and decides to review the status of the two risks once every six months to see if any other controls are required. SME UP has a plan to migrate its platform to another operating system. The CEO acknowledges that this is a change that might affect the risks. She decides to review the risks before the migration takes place.

6.8 Conclusion

This chapter presents the essentials of cybersecurity standardisation for European SMEs to address the challenges of getting started with cybersecurity standardisation. In this chapter, we introduce the main concepts in the cybersecurity domain. We propose a five-step process for establishing and improving cybersecurity using standards and frameworks. We introduce five widely used standards and frameworks for SMEs from different countries and sources for reducing cybersecurity risks. The security controls present in these standards and frameworks are compared and unified in 17 control categories to provide SMEs with a quick reference.

Since cybersecurity is closely associated with the roles of the SMEs in the digital ecosystem, we discuss four different SME categories (digital enablers, digitally based, digitally dependent, and start-ups) and provide SMEs with tailored guidance on the implementation of the controls. Although the selection of controls should be based on the risks that are specific to the organisation, the basic controls that are applicable to almost every organisation can also be considered for direct implementation.

We illustrate the use of the essentials presented in this chapter through an exemplar SME to help SMEs further to get practically started. The chapter uses a holistic approach by integrating the main concepts, processes, security controls derived from the standards and frameworks, and a focus on different SME categories to present the cybersecurity essentials for SMEs.

SECTION 3 INTEGRATING ADAPTIVE CYBERSECURITY MATURITY ASSESSMENT AND STANDARDISATION

7 Adaptable Security Maturity Assessment and Standardization for Digital SMEs

Small and Medium-sized Enterprises (SMEs) constitute a very large part of every country's economy and play an essential role in economic growth and social development. SMEs are frequent targets of cyberattacks, just like large enterprises. However, unlike large enterprises, SMEs generally have limited capabilities regarding cybersecurity practices. Assessment and improvement of cybersecurity capabilities are crucial for SMEs to survive and sustain their operations with limited resources. Despite the availability of maturity assessment models and standards to assess and improve cybersecurity capabilities, SMEs' specific requirements and roles in the digital ecosystem are often neglected. This paper presents high-level SME requirements regarding cybersecurity maturity assessment and standardization and translates them into an Adaptable Security Maturity Assessment and Standardization (ASMAS) framework to address this gap. Adopting the Design Science Research approach, the framework is demonstrated by an online and user-friendly software prototype that shows how the framework can be used in practice by implementing 194 controls, 251 capabilities from 5 standards and frameworks. In the Technology Acceptance evaluation study of the ASMAS framework that is conducted with 6 SMEs, using a Likert scale (1-5), we obtained positive evaluation results as average scores 4.29 for perceived usefulness, 4.14 for perceived ease of use, and 3.62 for intention to use evaluation constructs.

This work has been submitted for publication as:

Yigit Ozkan, B., & Spruit, M. Adaptable Security Maturity Assessment and Standardization for Digital SMEs.

7.1 Introduction

Information security and cybersecurity deal with ensuring confidentiality (C), integrity (I), and availability (A) of information. Other information properties such as authenticity and reliability can also be involved. According to the ISO/IEC 27032 standard, cybersecurity is preserving those properties in cyberspace. In contrast, information security is not limited to cyberspace and is preserving the CIA in general (ISO/IEC, 2012). Having made this distinction, our focus in this paper is all-encompassing. Thus, we investigate cybersecurity and information security in conjunction and refer to them as security.

According to the World Bank, small and medium-sized enterprises (SMEs) represent 90% of businesses and more than 50% of employment worldwide (World Bank, 2021). As SMEs are the backbone of every country or region's economy and digitalization is no longer optional, their resilience to malicious attacks and dependability are increasingly important. SMEs often share a business ecosystem by providing services to large enterprises. An OECD report on the digital transformation of SMEs states that during the ongoing pandemic, SMEs are increasingly using online platforms (OECD, 2021). The prior security challenges for SMEs remain but amplified with the surge of teleworking and the need for operating remotely (Lanz & Sussman, 2020; OECD, 2021). Malicious actors exploit these difficult times for their objectives, and governments issue alerts for individuals and organizations to warn them and increase awareness (UK National Cyber Security Centre, 2020). Having weak security practices has a twofold effect on SMEs. On the one hand, it can create a barrier for them to engage with large businesses. On the other hand, it can make them targets for attacks as a gateway to penetrate their alliances. SMEs can build trust in their existing or target business ecosystem by establishing good security practices. By doing so, they will have the advantage of pursuing new engagement opportunities (OECD, 2021). "Digital technology and security" is identified as one of the dimensions of digitally enabled growth in SMEs (North, Aramburu, & Lorenzo, 2019).

The European Digital SME Alliance represents about twenty thousand digital SMEs in Europe. Their position paper on Covid-19 economic recovery proposes the key areas in which quick actions are needed for recovery, one of which is cybersecurity & standards. They emphasize the heterogeneity of SMEs, thus the need for tailored and practical solutions and ensuring SMEs access to and awareness of standards (European Digital SME Alliance, 2020). Both security maturity assessments and security standardization help organizations to improve their security capabilities and processes (Le & Hoang, 2016; Siponen & Willison, 2009). We refer to standardization as adopting existing standards (international, regional, or national). Despite the challenges faced by SMEs, research on cybersecurity considering SMEs has been scant in literature (Yigit Ozkan & Spruit, 2019b).

Originating from the software engineering domain, organizations have used maturity models to assess and improve their capabilities for a couple of decades. Maturity modeling has attracted researchers' attention in various domains (Wendler, 2012). Information security and cybersecurity domains were no exception (Rabii et al., 2020; Spruit & Roeling, 2014; Yigit Ozkan, van Lingen, & Spruit, 2021).

Cybersecurity or information security needs, goals, and requirements depend on the organizational context (ISO/IEC, 2013a). Therefore, the adaptivity of security solutions, including maturity models and standards, to varying organizational contexts is essential. In

security maturity assessment literature, researchers have investigated organizational context and adaptivity of the assessment models from various angles. An information security maturity assessment and process improvement tool has been proposed for SMEs (Cholez & Girard, 2014). This tool is in the form of a standards-based questionnaire conducted by the researchers. However, there is no information in the published work about how the questionnaire is adapted to different organizational contexts (Cholez & Girard, 2014). Mijnhardt et al. (2016) approaches the organizational characteristics in two ways. First, as some indicators such as the number of employees, revenue. Second, as the nature of business processes such as outsourcing of or complexity in information technologies. Yigit Ozkan and Spruit (2020) have investigated the design requirements for an information security maturity model adaptable to SMEs by focusing on internal characteristics of SMEs, such as lack of organizational capabilities, short-term vision, and orientation.

In cybersecurity standardization literature, gaps and needs for SMEs have been identified in a research agenda that points out the adaptivity issues within several research questions (Yigit Ozkan & Spruit, 2019b). Barlette and Fomin (2008) state the need for future research on the creation and adoption of simplified security methods or standards dedicated to SMEs. Manso et al. (2015) recommend that "standards applicable by SMEs should incorporate maturity levels with different sets of requirements to facilitate a phased implementation" to facilitate the implementation of security standards by SMEs. Inspired by these research gaps in the literature regarding adaptivity issues in security maturity assessment and standardization, and adoption challenges of SMEs, we state our research objective as *"To integrate security maturity assessment and standardization in an adaptive instrument to support concurrent implementation efforts of digital SMEs"*.

To address this research objective, we employ a Design Science Research approach. We investigate the needs, goals, and requirements of SMEs and propose a design artefact as a solution. Our design artefact is the Adaptable Security Maturity Assessment and Standardization (ASMAS) framework for digital SMEs. The framework builds on a set of high-level SME requirements, is adaptable to the different roles SMEs take in digital ecosystems, and embeds security risk management and standardization concepts. The artefact is developed to support SMEs establishing, improving and demonstrating security maturity and standardization concurrently. The framework may also guide researchers and practitioners in the development of security maturity assessment models for SMEs.

The remainder of the paper is structured as follows. Section 2 provides the relevant background information. In Section 3, we explain our research approach and methodology. Section 4 introduces the high-level SME requirements regarding security maturity assessment. Section 5 presents the ASMAS framework and its aspects that address the high-level requirements. In Section 6, we describe the software prototype. Section 7 presents the evaluation of the framework and the evaluation results. Finally, conclusions are drawn, and potential areas for future research are proposed.

7.2 Background

7.2.1 SME characteristics and categories

Several researchers investigated how SME characteristics are different from larger companies (Cocca & Alberti, 2009; Hudson, 2001; Storey, 1994). The implications of SME characteristics on information security have been investigated at single SME and cluster levels (Mayer, 2010; Mijnhardt et al., 2016; Yigit Ozkan et al., 2019). Furthermore, the effect of SME characteristics on the design of information security maturity models has been investigated, and the design requirements to be considered have been reported (Yigit Ozkan & Spruit, 2020). The question of what approach to take for categorizing SMEs according to their security requirements has been a pertinent one. The European Digital SME Alliance has proposed SME categories with respect to SMEs' role in the digital ecosystem in their position paper on the European Union Cybersecurity Act and the role of standards for SMEs (The European Digital SME Alliance, 2020a). Table 7-1 presents these categories.

SME Category	Description
Digital enablers	SMEs that are active in developing and providing cybersecurity solutions.
Digitally based	SMEs that are highly dependent on digital solutions for their business.
Digitally dependent	SMEs that depend on digital solutions as end-users.
Start-ups	SMEs that neglect or are not well aware of cybersecurity and require specific measures and incentives to adopt cybersecurity solutions.

Table 7-1 SME Categories According to Their Roles in the Digital Ecosystem (The European Digital SME Alliance, 2020a)

The European Digital SME Alliance focuses on two challenges of SMEs: cybersecurity and standardization that are to be addressed by distinguishing the SME categories (The European Digital SME Alliance, 2020a). The categorization in Table 7-1 takes into account different security requirements of digital SMEs that originate from their various roles in the digital ecosystem. As our research aim is to support digital SMEs in their security and standardization efforts, in this research, we opted to use these categories presented in Table 7-1. SMEs' security and standardization requirements depend on and are shaped by their roles in the digital ecosystem. The Start-ups category in this categorization does not refer to the stage of the operation of a company, as described in Table 7-1, these SMEs are the ones that neglect or not well aware of cybersecurity.

7.2.2 Security standardization and SMEs

Despite SMEs' challenges in security standardization (The European Digital SME Alliance, 2020a), there are no information security or cybersecurity standards available specifically for SMEs (Yigit Ozkan & Spruit, 2019b). Barlette and Fomin (2008) state that few information security standards are theoretically suitable for SMEs, but given the cost, the skills

needed, and the language issues, it can be assumed that there is no method that can help SMEs to improve their security. This hasn't changed in time; however, there are guidelines, technical reports, and frameworks that can help SMEs in security standardization (ETSI, 2021; Paulsen & Toth, 2016; SBS, Digital SME Alliance, 2018). Security standardization produces opportunities but also presents challenges for SMEs.

7.2.3 Security maturity assessment

Maturity models in different domains have been developed and used since they became popular after the introduction of the Capability Maturity Model of the Software Engineering Institute of Carnegie Mellon University (Paulk et al., 1993). There is abundant research related to security maturity modelling (Akinsanya, Papadaki, & Sun, 2019; Le & Hoang, 2016; Rabii et al., 2020).

The list of SME characteristics that influence their security maturity proposed by Mijnhardt et al. (2016) are indicators (e.g., number of employees, revenue) to distinguish between a wide variety of different organizations. Following a similar categorization, Sánchez et al. (2006) proposed a maturity model for information security management within SMEs. In another study, researchers investigated how to address internal SME characteristics for designing information security maturity models (Yigit Ozkan & Spruit, 2020). Benz and Chatterjee (2020) proposed a cybersecurity assessment tool specifically for SMEs. The tool is based on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) (NIST, 2018), and uses a subset of activities of the NIST CSF that are chosen as applicable to or feasible for SMEs. Although the proposed tool provides SMEs with a tool for assessing their cybersecurity capabilities concerning (a subset of) a reference model, it does not take the SMEs' different roles in the digital ecosystem and their different needs that emerge out of their roles (Benz & Chatterjee, 2020).

Although research has been carried out on security maturity models targeting SMEs, or the adaptability of existing models to SMEs, no studies have considered the different roles SMEs take in the digital ecosystem.

7.3 Research methodology

We followed the Design Science Research (DSR) methodology consisting of the following steps: identify problem and motivate, define objectives of a solution, design and development, demonstration, evaluation and communication (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007b). Accordingly, our research includes realizing a problem situation, identifying high-level SME requirements (objectives of a solution), developing the framework, demonstrating and evaluating the use of the framework with a prototype, and communicating the research results. Our research process is presented in Figure 7.1.

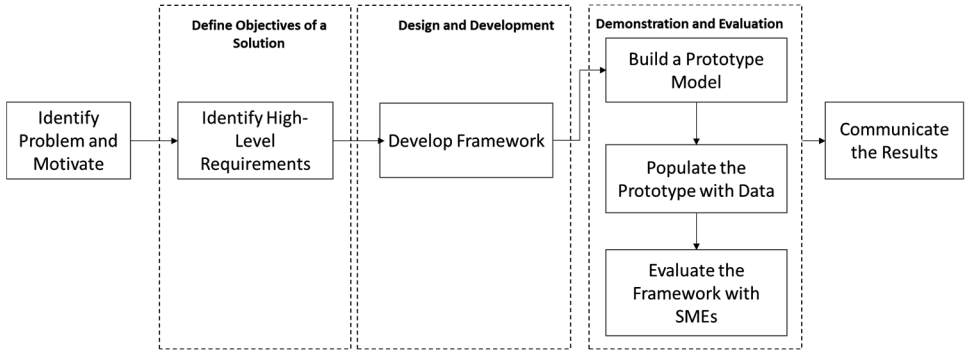


Figure 7.1 The Research Process (Peffers et al., 2007b).

As discussed in the introduction and background sections, we reviewed the literature to identify the problem and motivate our research. The problem identification and motivation step provided the input for setting the high-level requirements for security maturity modeling and standardization for SMEs. These requirements serve as objectives for the design and development step to be addressed by the framework (i.e., design artefact) aspects and components. The framework was developed by assembling the aspects and components to address the requirements.

To evaluate our framework, we adapted the "Prototyping" evaluation pattern for DSR artefacts, and hence we provide an implementation of the solution through a prototype (Sonnenberg & vom Brocke, 2012). We created a knowledge base in the prototype to demonstrate the aspects included in the framework. Pries-Heje et al. (2008) investigate the strategies for DSR evaluation and propose a framework that encompasses both ex-ante and ex-post orientations in naturalistic settings or artificial settings for DSR evaluation. We adapted evaluation constructs from the Technology Acceptance Model (TAM) (Davis, 1989) to evaluate our framework with SMEs for predicting how likely our design artefact is to be adopted in practice (Hevner et al., 2004). Our evaluation study was conducted with practitioners from real SMEs after the artefact was constructed; therefore, our evaluation is ex-post. We evaluated the ASMAS framework by conducting interviews with SMEs, which is accompanied by an evaluation form.

7.4 High-level requirements

In the DSR, understanding the problem space is crucial to propose useful artefacts to real-world problems (Hevner et al., 2004). There are four key concepts to understand and define the problem space: needs, goals, requirements, and stakeholders (Maedche et al., 2019). The stakeholders in our research are SMEs. On the one hand, being non-homogeneous, SMEs have different needs regarding cybersecurity and standardization that depend on their organizational context (i.e., their role in the digital ecosystem). On the other hand, SMEs' goal (intended outcome) is to secure their organization against cyber threats. We derived a set of high-level requirements (HLRs) regarding security maturity modeling and security standardization for SMEs to address this goal.

SMEs lack resources (time, money, and expertise) to establish security capabilities and security standardization (Cocca & Alberti, 2009; de Vries et al., 2009). The existing security

maturity models and standards are costly and complex. Lack of financial resources is a barrier for SMEs to get external support to help with cybersecurity (Kertysova, et al., 2018). Self-assessment is a means by which an organization assesses compliance to a selected reference model or module without requiring a formal method (Blanchette & Keeler, 2018). Ritchie and Dale (2000) summarize the benefits of self-assessment from a quality management perspective. Most of the benefits are also applicable from a security management perspective. The following are critical for SMEs with a security perspective: self-assessment helps keep costs down, raises understanding and awareness on security, and develops a holistic approach to security. The Cyberwatching.eu project surveyed cybersecurity standardization gaps. Their white paper summarizes the findings and recommendations and states the need to explore self-assessment and other low-cost solutions (Cyberwatching.eu, 2018). Consequently, we derive the following HLR:

HLR1- Easy to use, self-assessment, do-it-yourself. Assessment and improvement planning should be easily realized by SMEs, requiring minimal extra resources.

Digitalization brings security as a critical element in business model scaling, and it is both a necessity and an enabler for SMEs (Westerlund, 2020). Depending on the digitalization level, SMEs' needs for cybersecurity dramatically differ. None of the available security models addresses this situational aspect. In design science research, artefact mutability –the adaptability of DSR artefacts– is proposed as one of the components of design theories (Jones & Gregor, 2007). The design of adaptable artefacts is referred to as situational artefact construction (SAC). SAC allows the researcher to develop artefacts which are adaptable to different design problems within a problem class, and to understand the relevant design situations within this class (Winter, 2011). As the costs for adapting a more generic solution artefact to a specific design problem are higher than those for adapting the more specific solution artefact, developing situational artefacts reduces the cost of adaptation (Winter, 2011). Understanding the organization's context is the primary step when establishing information security or cybersecurity (ISO/IEC, 2013a). SMEs are not homogenous, and they differ in their requirements for security. The difference between SMEs can be characterized by their role in the digital ecosystem (The European Digital SME Alliance, 2020a; Westerlund, 2020). Consequently, we derive the following HLR:

HLR2 - Situational awareness. The assessment model should provide customized guidance and implementation plan according to SME categories.

In standard development, SMEs are often neglected and require financial support, access to technical expertise, and assistance to be active stakeholders (de Vries et al., 2003). Maturity models have the basic design principle of "Definition of central constructs related to the application domain" (Pöppelbuß & Röglinger, 2011). If the application domain has achieved a level of maturity to have published standards by standards developing organizations, these standards can be used as sources for defining domain specific constructs of the maturity model (Shrestha et al., 2018). A maturity assessment model having constructs based on standards in the application domain can help organisations in both their maturity improvement and standardization efforts simultaneously by integrating maturity assessment and standardization in the same tool (design artefact). Organizations using the maturity assessment model to improve their cybersecurity would be able to adhere to (or adopt) the standards in the

application domain. While establishing security capabilities, SMEs can improve their adherence to security standards. This can be accomplished by using standards as the primary source for maturity model capabilities. Consequently, we derive the following HLR:

HLR3 - Support for standardization and standards-transparency. The framework should support the ability to adhere to related standards on security. The relation between security capabilities and standards should be transparent.

SMEs' awareness of security and related standards is low. This partly stems from the lack of resources and the security domain's perceived complexity (Paulsen, 2016). SMEs' level of security awareness might differ according to their role in the digital ecosystem. By considering human actors as part of the solution rather than the problem regarding security (Zimmermann & Renaud, 2019), awareness of the organizations' employees and managers has critical importance. Consequently, we derive the following HLR:

HLR4 - Provide security awareness. The model should help increase security awareness concerning the assessed capabilities by considering SME categories.

Given the ever-changing and dynamic nature of security threats, and risks, it is crucial to incorporate emerging security capabilities and standards. This will ensure the maintainability of the assessment model and support it to be future-proof. In design science research, this phenomenon is referred to as “mutability-in-use”, a strategy that takes into account the future needs that may emerge when the artefact is in use (Sjöström et al., 2011). Consequently, we derive the following HLR:

HLR5 - Maintainability and adaptability by design. New standards, threats, risks, capabilities should easily be included in the assessment model.

We propose an adaptable security maturity assessment and standardization framework to address the HLRs in the following section.

7.5 The Adaptable Security Maturity Assessment and Standardization (ASMAS) Framework

The ASMAS framework integrates five aspects: organization, standardization, risk management, assessment and measurement, and improvement. Figure 7.2 illustrates the meta-model of the ASMAS framework.

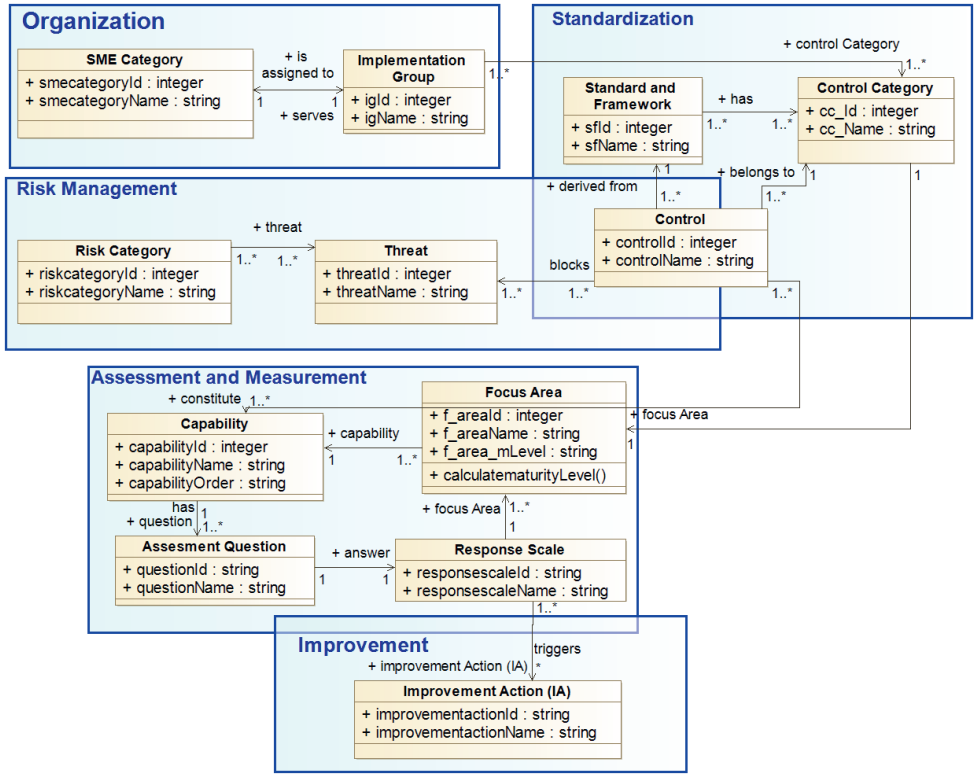


Figure 7.2 Meta-model of the Adaptable Security Maturity Assessment and Standardization (ASMAS) Framework

In the following subsections, we elaborate on the aspects and components of the framework to address the high-level requirements presented in Section 7.4. The framework addresses the SME categories shown in Table 7-1. The Organization aspect presented in Section 7.5.1 elaborates on how this is accomplished. A mapping of the high-level requirements and the aspects that address them is presented in Section 7.5.6.

7.5.1 Organization aspect

The Organization aspect comprises the SME categories and Implementation Groups (IGs). IGs are composed of Control Categories. Each control category (1 to n) has several controls populated from standards and frameworks. IGs are constructed according to SME categories and provide SMEs in each category with a tailored perspective on the controls and capabilities relevant to their organizational profile. The Organization aspect enables SMEs to explore and use the framework according to their IG. Figure 7.3 illustrates the Control Categories, IGs, and the associations between the SME categories and the IGs.

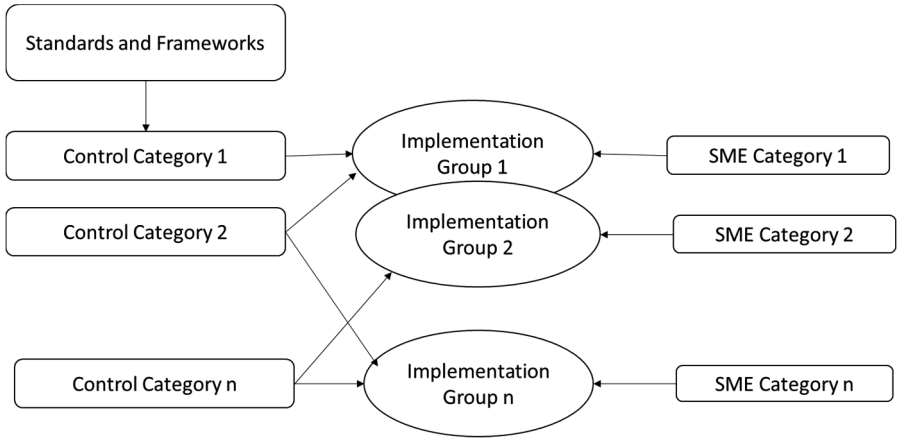


Figure 7.3 Control Categories, Implementation Groups, and Their Associations with the SME Categories.

The Organization aspect addresses the "self-assessment" HLR(#1) and the "situational awareness" HLR(#2) by using a designated implementation group per SME category. The Organization aspect introduces configuration parameters for artefact mutability (Pöppelbuß & Goeken, 2015).

7.5.2 Standardization aspect

The Standardization aspect comprises standards and frameworks. Standards and frameworks are the sources of security controls in the Risk Management aspect. Controls are the sources for capabilities and assessment questions in the Assessment and Measurement aspect. The Standardization aspect addresses HLR(#3) (support for standardization and standards-transparency), and HLR(#5) (maintainability and adaptability by design) by facilitating the inclusion of new standards and frameworks (mutability-in-use).

Overlapping controls in the standards and frameworks should be taken into account to eliminate duplicate end-user efforts. This is accomplished by deriving the capabilities (see Section 7.5.4) by considering all the controls from relevant standards and frameworks for each control category.

The Standardization aspect introduces best practices from standards and enables the integration of maturity assessment and standardization in one framework.

7.5.3 Risk management aspect

The Risk Management (RM) aspect introduces the core concepts of security risk management and comprises threats, risks, and controls. Ontologies and taxonomies can be used as sources for threats and risks. Control categories and controls are to be derived from standards and frameworks. Control categories are considered as a group of controls that have common objectives. The RM aspect enables SMEs to explore and use the framework according to their threats and risks. The RM aspect addresses “the situational awareness” HLR (#2) (by the association of implementation groups and controls). As the RM aspect incorporates risks and threats, it addresses the "provide security awareness" HLR (#4). The RM aspect also addresses "the maintainability and adaptability by design” HLR (#5) by enabling the inclusion of emerging threats, risks, and controls (mutability-in-use).

For specific SMEs, we presume that a security risk analysis will yield more appropriate controls than those assigned per SME category through implementation groups. The concern is to provide SMEs with a quick start to security that can be improved upon. The RM aspect in the framework is for supporting SMEs to have a risk-based view on the controls.

7.5.4 Assessment and measurement aspect

One of the purposes of using a security maturity model is the assessment of existing capabilities and measuring performance (Le & Hoang, 2016; Mettler, 2009, 2011; Pöppelbuß & Röglinger, 2011). This purpose of use is referred to as “descriptive purpose of use” (Pöppelbuß & Röglinger, 2011). The Assessment and Measurement (A&M) aspect comprises the following: capabilities, assessment questions, measurement mechanism, focus areas, response scale, and maturity levels. To assess the current maturity level of a functional domain, measures must be defined for each of the capabilities. This can be done by formulating assessment questions for each capability. Formulation of the questions is usually based on the descriptions of the capabilities, experience, and practices (Steenbergen et al., 2010).

A measurement mechanism is required for measuring the current level of an organization's capabilities. Although a two-level scale (Implemented–Not-implemented) might be used, a four-level scale will give higher precision.(CMU/SEI, 2006) Focus areas are the areas that have to be developed to achieve maturity in a functional domain (Steenbergen et al., 2010). In our framework, control categories in the Standardization aspect correspond to focus areas in the A&M aspect. Given the answers to the assessment questions, a maturity level per control category (i.e. focus area) can be calculated according to the desired measurement mechanism. The function calculatematurityLevel() function in Figure 7.2 is to be developed to achieve this purpose. Together with the Organization aspect, the A&M aspect addresses the self-assessment HLR(#1) and situational awareness HLR(#2). SMEs will face the applicable assessment questions associated with their organizational profile (mutability-in-design). Measurement of the maturity is based on the answers provided to the assessment questions.

7.5.5 Improvement aspect

Another purpose of using maturity models is improving capabilities to the desired level on the scale. This purpose of use is referred to as “prescriptive purpose of use” (Pöppelbuß & Röglinger, 2011). The Improvement aspect comprises improvement actions.

When the SME performs self-assessment using the assessment questionnaire, based on the given answers, the capabilities that are not currently fully implemented can be used to formulate a customized improvement plan that also facilitates standardization efforts.

The standards transparency HLR(#3) is addressed by the Improvement aspect, which ensures that SMEs have a quick reference for the capabilities (that are derived from standards and frameworks), increase their standards awareness and adherence to standards. Together with the Organization and Risk Management aspect, the Improvement aspect addresses the situational awareness HLR(#2). Personalized improvement plans can be prepared by selecting controls that are designated according to the SME categories. Both the Organization aspect (by implementation groups) and the Risk Management aspect (by the association of implementation groups and controls) play a role in accomplishing this. As part of the Improvement aspect, providing security awareness addresses another HLR(#4).

7.5.6 Mapping of high-level requirements and aspects

Table 7-2 shows the mapping of the high-level requirements and the aspects that address the corresponding requirement. The rationale for these mappings is discussed in Section 7.5.1 – 7.5.5.

#	Requirement	Aspects
HLR1	Easy to use, self-assessment, do-it-yourself	Assessment and Measurement, Organization
HLR2	Situational awareness	Organization, Risk Management, Improvement
HLR3	Support for standardization and standards-transparency	Standardization, Improvement
HLR4	Provide cybersecurity awareness	Improvement, Risk Management
HLR5	Maintainability and adaptability by design	Risk Management, Standardization

Table 7-2 Mapping of the High-level Requirements (HLRs) and the Framework Aspects.

The ASMAS framework addresses all high-level requirements by integrating the aspects that are described above and visually presented in the meta-model (Figure 7.2). Given the challenges faced by SMEs, the ASMAS framework proposes a "one-stop-shop" for SMEs to start with security and standardization.

7.6 The software prototype and the knowledge base

A prototype is implemented to demonstrate the ASMAS framework as a web-based application using a low-code software development tool –Mendix Studio Pro 9.0.2 platform– (free version) (Mendix, 2021). The screenshots of the prototype are presented in the Appendix. A short video demonstrating the prototype can be accessed through https://tinyurl.com/yc5b63cw. Figure 7.4 presents the conceptual model of the prototype.

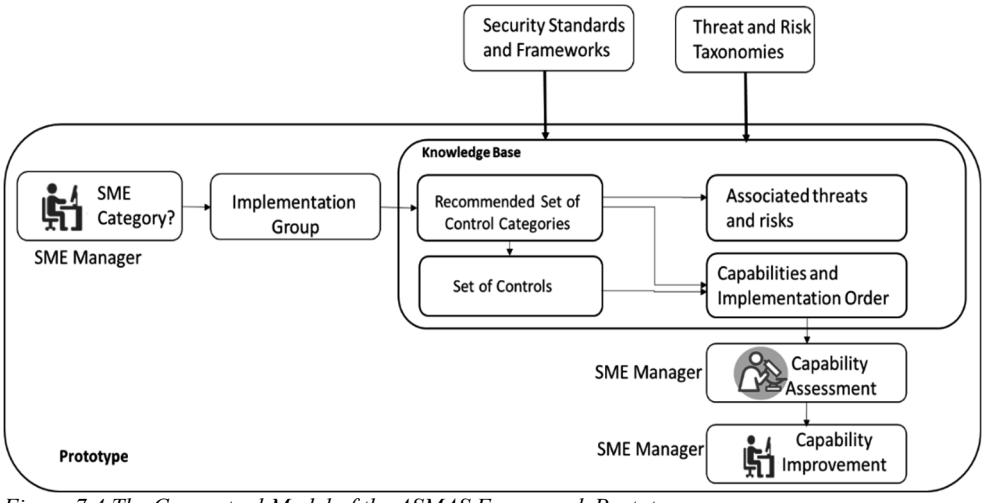


Figure 7.4 The Conceptual Model of the ASMAS Framework Prototype

As shown in Figure 7.4, the prototype includes a knowledge base of the framework components (e.g., control categories, controls, standards, risks, threats). The knowledge base was populated from five standards and frameworks (control sources) (ETSI, 2021). These standards and frameworks are as follows: Cyber Essentials from the UK (National Cybersecurity Centre, 2017), The Centre for Cyber Security Belgium SME Guide (Centre for Cyber security Belgium, 2017), Center for Internet Security Controls from the USA (Center for Internet Security, 2018), and ETSI (global) (ETSI, 2015), NIST Small Business Information Security from the USA (Paulsen & Toth, 2016), and ISO/IEC 27002:2013 (ISO/IEC, 2013b). We analyzed these standards and frameworks and put forward a union set of control categories (see Section 7.5.3). We used the SME categories presented in Table 7.1. to identify the SME profiles (Implementation Groups) in the prototype. We populated the knowledge base with the threat taxonomy of ENISA (European Union Agency for Cybersecurity) (Marinos, 2016b), and with the taxonomy of operational cybersecurity risks from the Carnegie Mellon University, USA (Cebula, Popeck, & Young, 2014b).

The knowledge base's content implemented in the prototype is summarized in Table 7-3 and Table 7-4.

Standard/ Framework (Control Source)	**# of Controls**
Cyber Essentials	5
The Centre for Cyber Security Belgium SME Guide	13
Center for Internet Security (CIS) Controls	20
NIST Small Business Information Security	33
ISO/IEC 27002	123
Total # of Controls	194
Total # of Control Categories	18

Table 7-3 The Summary of Control Related Content of the Knowledge Base

Data	**Total #**
Capabilities	251
Risk Classes	4
Risk Sub-Classes	13
Risks	57
Threat Categories	8

Table 7-4 The Summary of Capability, Risk, and Threat-related Content of the Knowledge Base

In the prototype, the process starts with the SME manager identifying their organization's category according to Table 7-1. Subsequently, the prototype assigns an implementation group for the SME, and the SME manager can view the recommended set of controls for their category.

Table 7-5 presents the functions implemented in the software prototype.

Functions	Description
Definitions	This function is used to populate the knowledge base. Using this function it is possible to add new entities and items (e.g., new controls, new control categories, new risks) to the knowledge base (mutability-in-use).
Company	This function is used to define the company names for demonstration purposes. Using the "Company-Capability" sub-function, it is possible to view the controls assigned to each company.
Views	This function has three sub-functions. The “SME Category-Control” is used to query the controls associated with an SME category. The “Threat view on Controls” enables the user to query all the associated controls with a threat category. Using the “Risk view on Controls”, the user can query the related controls by choosing a risk class and a risk sub-class.
Search	This function is used for querying the controls. The user can select a control category and a control source and query the associated controls. If no control category or control source is chosen, then all the controls in the knowledge base are listed.
Assessment	This function is for performing capability assessments and viewing the results. The user can enter the implementation status for the capabilities. The capability order and capability level are displayed while performing the assessment.

Table 7-5 The Functions in the ASMAS Framework Prototype

7.7 Evaluation of the framework

In this section, we present the evaluation of the ASMAS framework by instantiating and demonstrating the framework using the software prototype and the evaluation results. We have conducted seven evaluation sessions with 6 SMEs. Each session has consisted of an approximately one-hour online interview. In each session, one of the researchers has presented the conceptual framework and then demonstrated the framework using the software prototype. This was followed with a discussion. At the end of each interview session, we sent out evaluation forms to the participants to obtain their feedback on the utility of the proposed framework.

To understand and predict the acceptance our design artefact, we have focused on the constructs perceived usefulness, ease of use, and intention to use in line with the Technology Acceptance Model (TAM) core constructs (Davis, 1989; Hevner et al., 2004). Perceived usefulness refers to the user's perception concerning how the design artefact enables the user to enhance their performance in a given context. Perceived ease of use entails the user's perception concerning the degree to which use of the artefact would not require physical or mental effort. Intention to use explains user acceptance of the design artefact (Davis, 1989). We used these three constructs to guide the further design of our evaluation interviews and questionnaires. Table 7-6 presents the set of questions in the evaluation form to evaluate each

construct. We used three statements per evaluation construct to evaluate the framework resulting in 9 statements.

Evaluation Construct	#	Statement
Perceived usefulness	1	I think this framework contributes to supporting SMEs to assess and improve their information security and cybersecurity.
	2	I think this framework contributes to helping SMEs increase awareness of information security and cybersecurity security.
	3	I think this framework contributes to helping SMEs increase awareness of information security and cybersecurity security standardization.
Perceived ease of use	4	I think this framework is easy to use to assess and improve my company's information security and cybersecurity.
	5	I think this framework is easy to use to improve my company's awareness of information security and cybersecurity security.
	6	I think this framework is easy to use to improve my company's awareness of information security and cybersecurity security standardization.
Intention to Use	7	I would use this framework to assess and improve my company's information security and cybersecurity.
	8	I would use this framework to improve my company's awareness of information security and cybersecurity security.
	9	I would use this framework to improve my company's awareness of information security and cybersecurity security standardization.

Table 7-6 Set of Questions Used to Evaluate the Utility of the ASMAS Framework

In the evaluation form, we used a 5-point Likert scale to understand the level of agreement of the interviewee concerning each statement, for which 1 represents 'strongly disagree' and 5 represents 'strongly agree'.

We also gathered the characteristics of the SMEs and the interviewees via the evaluation form. These characteristics are presented in Table 7-7.

SME #	Country	Category(The European Digital SME Alliance, 2020a)	# of Employees	Interviewee's # of Years Security Experience	Interviewee's Role*	SME Size(European Commission, 2016)
1	United Kingdom	Digital Enabler	<10	23	CEO	Micro
2	Egypt	Digitally Based	<10	2	CEO	Micro
3	Netherlands	Digital Enabler	<250	4	Security Specialist	Medium
4	Switzerland	Digitally Based	<10	1	CEO	Micro
5	Switzerland	Digitally Dependent	<10	20	CISO	Micro
6	Italy	Digitally Based	<50	5	CTO	Small

Table 7-7 Evaluation Study Participants' Characteristics

*CEO: Chief Executive Officer, CISO: Chief Information Security Officer, CTO: Chief Technology Officer

7.1 Evaluation Results

The results of the evaluation survey are presented in Table 7-8. We elaborate on the findings per evaluation criteria and present quotes from the participants in the following paragraphs.

Evaluation Construct	Statement	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly agree (5)	Average Score
Perceived usefulness	1	0%	0%	14,3%	28,6%	57,1%	4.43
	2	0%	0%	28,6%	42,9%	28,6%	4.00
	3	0%	0%	14,3%	28,6%	57,1%	4.43
						Average score per construct	4.29
Perceived ease of use	4	0%	0%	14,3%	28,6%	57,1%	4.14
	5	0%	0%	28,6%	42,9%	28,6%	4.00

Evaluation Construct	Statement	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly agree (5)	Average Score
	6	0%	0%	28,6%	14,3%	57,1%	4.29
						Average score per construct	4.14
Intention to Use	7	0%	14,3%	14,3%	42,9%	28,6%	3.57
	8	0%	14,3%	28,6%	28,6%	28,6%	3.43
	9	0%	14,3%	14,3%	14,3%	57,1%	3.86
						Average score per construct	3.62

Table 7-8 Responses to the Evaluation Survey

We also included optional open-ended questions in our survey to gather more insights on the perception of the framework. Not every SME preferred to answer those questions. We also present and discuss the answers we gathered for the open-ended questions in the following paragraphs.

Perceived usefulness

Regarding the perceived usefulness, the majority of the participants considered the ASMAS framework as useful, given the high responses associated with the corresponding statements (statements 1, 2, and 3).

The answers to the open questions support the findings as follows.

"The framework can also be used to support standard compliance efforts." [Participant 1]

"Provides order, structure, guidance, helps SMEs get started, extensible, can be used or adopted by practitioners" [Participant 3]

"Having a single place where all the major standards/frameworks are collected without having to look for them in many different places is certainly a strong point. Prioritization of the different gaps is also a strong point." [Participant 7]

Perceived ease of use

Most of the participants considered the ASMAS framework easy to use regarding the perceived ease of use, given the high responses associated with the corresponding statements (statements 4, 5, and 6). The answers to the open questions support the findings as follows.

"Easy to use, particularly if a minimal level of proficiency is already present. Great for figuring out different standards and requirements." [Participant 4]

"Despite being easier to use than the standards that are incorporated, it may still be useful to provide a tutorial/"getting started" for SMEs in order to get them started using the framework." [Participant 4]

"Although it provides a very good introduction into the topic, SME might be overwhelmed by the number of questions and tasks." [Participant 5]

Intention to Use

The participants had diverse responses associated with the corresponding statements (statements 7, 8, and 9) regarding the intention to use the framework. The answers to the open questions support the findings as follows.

"It's really interesting and definitely, I would use it if it's available." [Participant 2]
"I would consider using this tool, but now am getting more familiar with ISO 27001 every day and may not be in the target audience anymore." [Participant 4]

One SME disagreed with all of the statements that were designed to evaluate the intention to use the framework. This SME defines their business as follows: "Provider of a SaaS Solution for Internal Control, Audit Management, ISMS, Governance Risk and Compliance". As their security maturity is relatively high and they provide security services consultancy, their intention to use the framework is low.

Other Feedback and Discussions

"The framework could also support subcategories of SMEs under the given categorization" [Participant 1]

We discussed this feedback with the participant; it refers to more tailoring for SME categorization. For example, subcategories might be introduced according to other characteristics for an SME category (i.e., digitally dependent) (e.g., number of employees).

"We have the experience that even if SMEs want to take care of the topic, business needs always have priority, and since they are short on resources, this topic often gets the least attention. Not good, but the reality." [Participant 5]

This feedback is relatively straightforward, and it supports the high-level requirements that we pointed out in Section 7.4.

"It would be nice if the framework could give an indication of the initial status of the SME (good - sufficient - bad for example, or a scoring system) and update this each time a new assessment is performed. SMEs might not be able to cope with all the gaps identified by the framework due to lack of time so maybe you could reduce the gaps to just the ones which are more important and leave the less important ones as simple "suggestions"". [Participant 7]

This feedback is about complexity as the participant suggests categorizing the capabilities as mandatory/suggestion. The implementation of the capability levels from A-D in the

prototype was designed to help reduce the implementation complexity for SMEs. This can be interpreted as level A capabilities being mandatory to implement and followed by B, C, and D level capabilities.

To summarize, we demonstrated the framework aspects and the high-level requirements by using a software prototype. Concerning validity, the prototype addresses HLR2, HLR3, HLR4, and HLR5. The HLR1 (Easy to use, self-assessment, do-it-yourself) is partially addressed by the Assessment and Measurement aspect, and the Organization aspect in the prototype as the SMEs are exposed to the components (i.e., controls, control categories, and capabilities) of the framework according to their profile that makes the framework easier to use. The demonstration of the perceived ease of use as part of the HLR1 requires SMEs' involvement as the framework's end-users. Concerning the technical feasibility, the development of the software prototype shows that the framework can be operationalized. The answers to the open-ended questions and the feedback gathered during the interviews support the high-level requirements presented in Section 7.4.

7.8 Conclusion

Emerging cyber threats, standards, and regulatory requirements place organizations under pressure to implement security measures and provide assurance to regulators promptly. Organizations can establish and improve their security and compliance using maturity assessments and standards. We have formulated our research objective to support organizations to accomplish this with an adaptive instrument. We have proposed an Adaptable Security Maturity Assessment and Standardization (ASMAS) framework to address our research objective. We have presented the high-level requirements of such a framework by adopting an SME perspective. Since SMEs are not homogenous, and their cybersecurity needs differ, we augmented our framework by incorporating SMEs' roles in the digital ecosystem. We then presented the five aspects of the framework: Organization, Standardization, Risk Management, Assessment and Measurement, and Improvement that facilitate a novel approach to security maturity assessment and standardization through a meta-model and a software prototype. We pointed out how the aspects support the five high-level requirements and integrated the aspects to construct a software prototype that demonstrates the validity and applicability of the framework.

We conducted seven evaluation interviews with six SMEs from five countries. We used the evaluation constructs based on the Technology Acceptance Model to explain and predict the utility of the ASMAS framework. The evaluations using a Likert scale (1-5) resulted in average scores 4.29 for perceived usefulness, 4.14 for perceived ease of use, and 3.62 for intention to use evaluation constructs. When we specifically look into the perceived usefulness of the framework for increasing the awareness of cybersecurity standardization, 85.7% of the interviewees responded positively (agree and strongly agree). The same result has been achieved for the perceived usefulness of the framework for supporting SMEs to assess and improve their information security and cybersecurity. This results show that SMEs can benefit

from the approach of integrating cybersecurity maturity assessment and standardization in the same framework.

This holistic and integrated approach of a multi-aspect security assessment framework that facilitates both standardization and risk management adopting an SME perspective is the first of its kind. Given the challenges faced by SMEs with limited resources, we believe our holistic approach can facilitate and consolidate SMEs' security assessment and standardization efforts.

By conducting maturity assessments based on the ASMAS framework, SMEs can assess their security capabilities, identify areas of improvement and increase adherence to standards. SMEs can also use the high-level requirements and the framework to evaluate any maturity model proposed for their use.

A real-world implementation of the framework should include security functions (e.g., users, roles, authorizations). Future research can implement these security functions, and a more naturalistic evaluation can be carried out in a real organizational context. Although further research could be conducted to validate the high-level requirements, the evaluation sessions conducted with SMEs support the validity of the requirements. The findings from the evaluation study show that regarding the utility of the framework, generally positive results have been obtained. This research has shown that security maturity assessment and standardization frameworks such as ASMAS provide a much-needed and feasible foundation for a more secure future for SMEs, guided by established best practices.

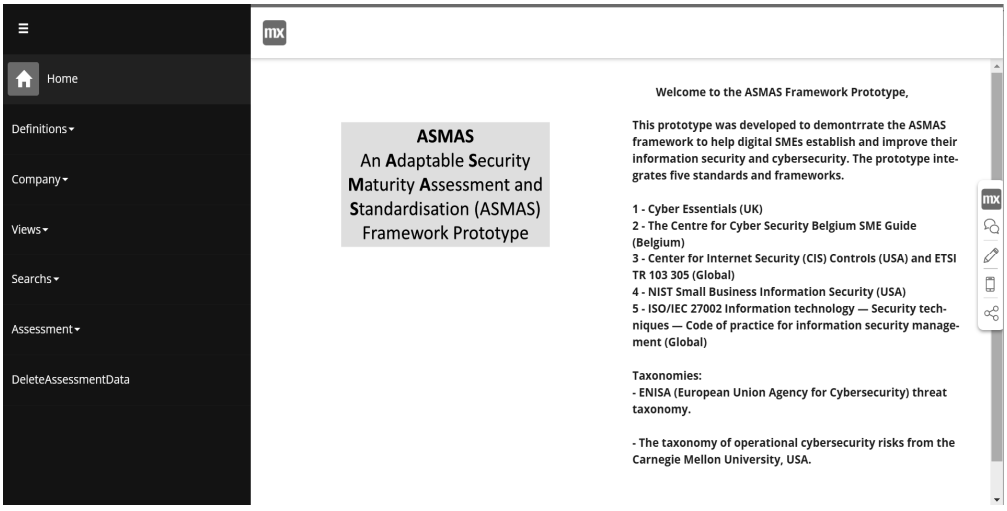
Acknowledgement

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.

Appendix: Screenshots of the ASMAS Framework Prototype

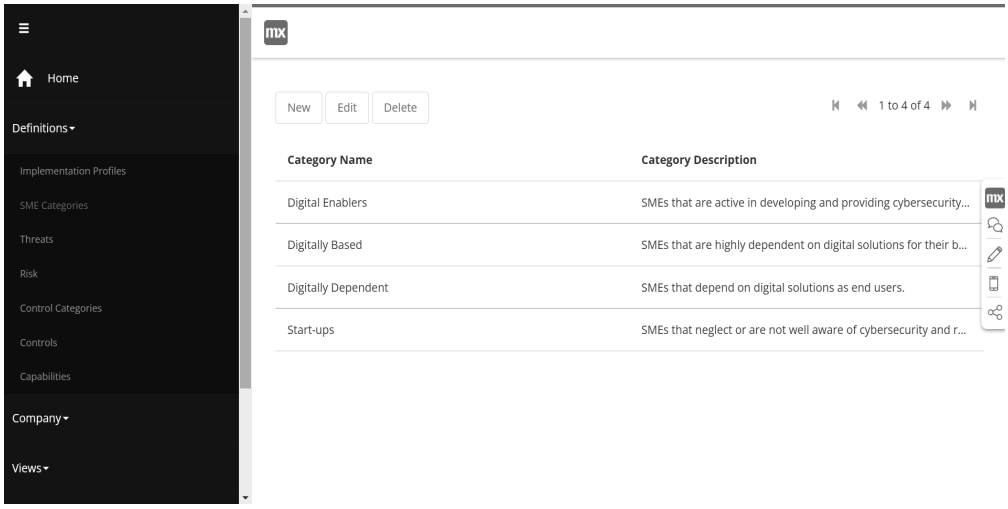
Home Screen:

In the Home screen, we see an introduction text that explains the standards, frameworks and taxonomies included in the knowledge base of the prototype. In the navigation menu on the left side of the screen, there are the menu items that correspond to the functions implemented in the prototype.



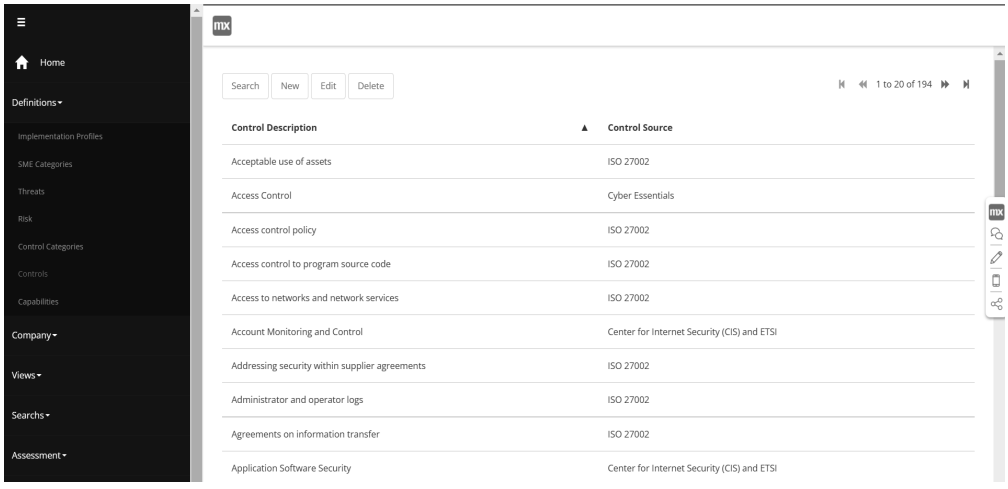
Definitions: SME Category

Using this function, the SME categories and the definitions of the SME categories can be defined. As can be seen here, it is always possible to add more categories or change/delete the existing ones. This is ensued by maintainability by design high-level requirement.



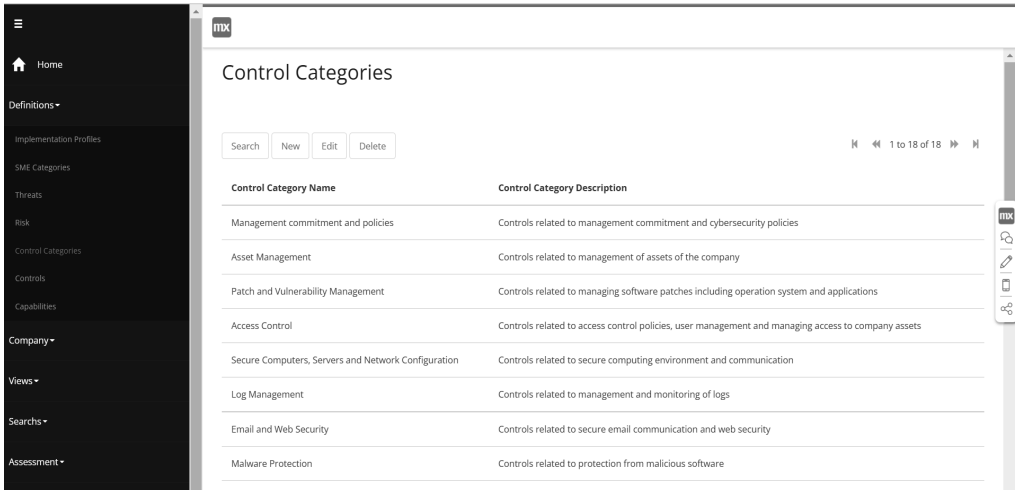
Definitions: Controls

Using this function, controls from standards and frameworks can be defined. Control Source is the name of the standard or the framework.



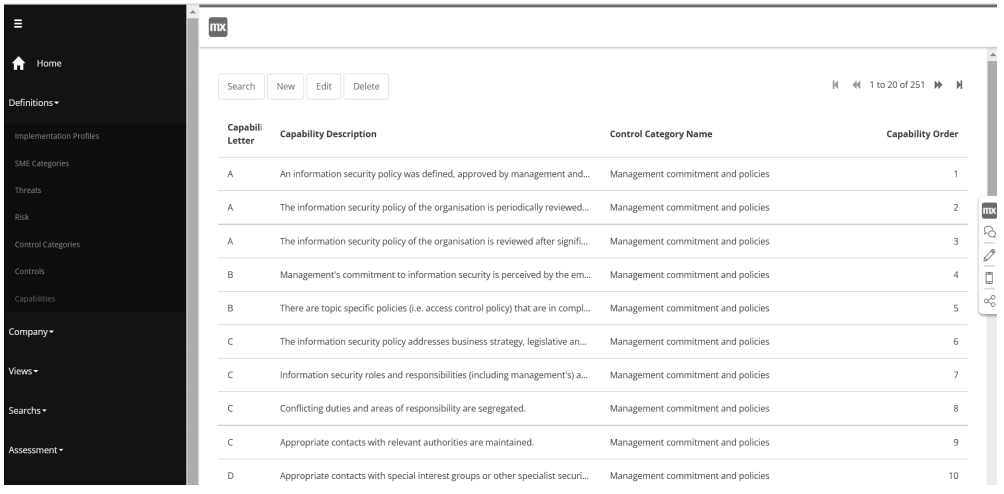
Definitions: Control Categories

Using this function, controls categories from standards and frameworks can be defined. Every control belongs to a control category.



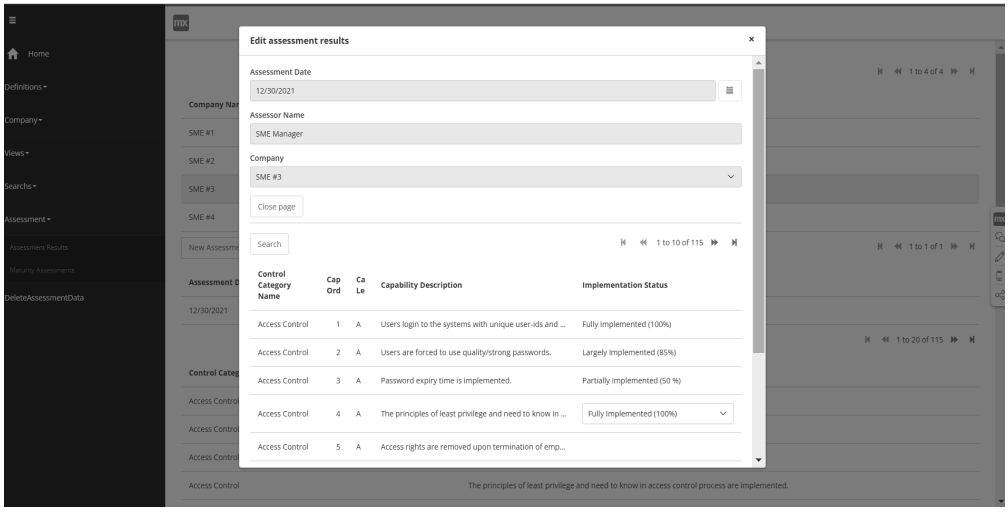
Definitions: Capabilities

Using this function, capabilities per control category can be defined. Capabilities are derived from the implementation guidance presented in standards and frameworks. Capabilities belong to a Level characterised by a letter (i.e. A, B, C, D, E) and an implementation order characterised by Capability Order. The Capability Order is the implementation order of the capabilities associated with a control category.



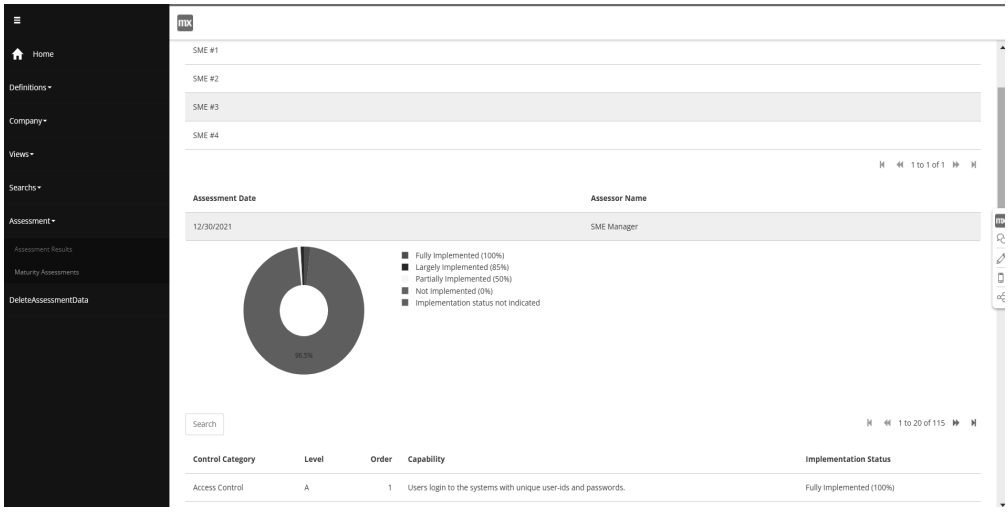
Maturity Assessment

With this function, organisations can assess their cybersecurity maturity by evaluating the capabilities that are applicable to their organisational profile. The assessment is done by giving ratings to the implementation status of the capabilities. Implementation status can be “Fully Implemented”, “Largely Implemented”, “Partially Implemented” or “Not Implemented”. A capability can also be “Not applicable” to an organisation. In the screenshot, we also see the information about the assessment (i.e. Assessment date, assessor, company name and the category). Several assessments can be performed and saved in the prototype.



Maturity Assessment Results

In this screen, organisations can review their previously done assessment’s results. The pie chart illustrates the implementation status percentages. Although current implementation in the prototype presents the whole assessment in one pie chart, a pie chart per control category can also be prepared.


Home
Definitions
Company
Views
Searchs
Assessment
Assessment Results
Maturity Assessments
DeleteAssessmentData
SME #1
SME #2
SME #3
SME #4
1 to 1 of 1
Assessment Date
Assessor Name
12/30/2021
SME Manager
Fully Implemented (100%)
Largely Implemented (85%)
Partially Implemented (50%)
Not Implemented (0%)
Implementation status not indicated
96.5%
Search
1 to 20 of 115
Control Category
Level
Order
Capability
Implementation Status
Access Control
A
1
Users login to the systems with unique user-ids and passwords.
Fully Implemented (100%)

8 Conclusion

In this final chapter, we conclude and reflect on our work by revisiting our research questions and explaining how we have addressed them. We discuss the practical and scientific relevance of our research outputs, and the limitations of our research. Furthermore, we identify the research gaps and directions for future research. Finally, we conclude the dissertation with a personal reflection.

Digital connectivity and dependency continues to raise apace, and brings with it cyber risks. Our approach to supporting organisations to help them improve their cybersecurity was twofold. First, we considered cybersecurity maturity assessment as a means of improvement that enables organisations to evaluate their as-is cybersecurity capabilities and, subsequently, plan for development of the required capabilities. Second, we considered cybersecurity standardisation as a means of improvement by adopting and implementing best practices (standards) published by standards developing organisations. Therefore, our research objective was t*o support the improvement of organizations' cybersecurity through maturity assessment and standardisation*.

Using a maturity assessment model or a standard to improve cybersecurity is not an easy undertaking. It is rather quite complicated. It requires commitment and a diverse set of resources, including technical knowledge as well as cybersecurity management skills. The challenge is even greater for SMEs which have limited resources. We tackled the problem with various approaches to address SMEs' needs and requirements. We investigated the opportunity to adapt an existing maturity model to SMEs and developed a method (Chapter 2). We designed a situation-aware assessment instrument that adapts itself accordingly during the course of the assessment (Chapter 3). We proposed design requirements for designing information security maturity models for SMEs (Chapter 4). We identified the gaps in the literature and proposed a research agenda for cybersecurity standardisation to guide future research (Chapter 5). We developed the cybersecurity standardisation essentials guideline for SMEs that is published by a European standardisation body (Chapter 6). Finally, we integrated the maturity assessment and standardisation into an adaptable framework for SMEs. We elaborate on our contributions in Section 8.1.

In Figure 8.1, we revisit the problem space, solution space (Section 1.2), our knowledge contributions (*Table 1-3*) and present our prescriptive knowledge contributions. We discussed our knowledge contributions in detail in Section 1.6. Drechsler & Hevner (2018) point out two sub-categories of as prescriptive knowledge contributions: solution design knowledge (e.g., technological rules, requirements, principles, features of design artifacts) and solution design entities (e.g., meta-artifacts, artifacts).

In Figure 8.1, we present our solution design knowledge contributions as ***SDK***, and our solution design entities as ***Artifact***.

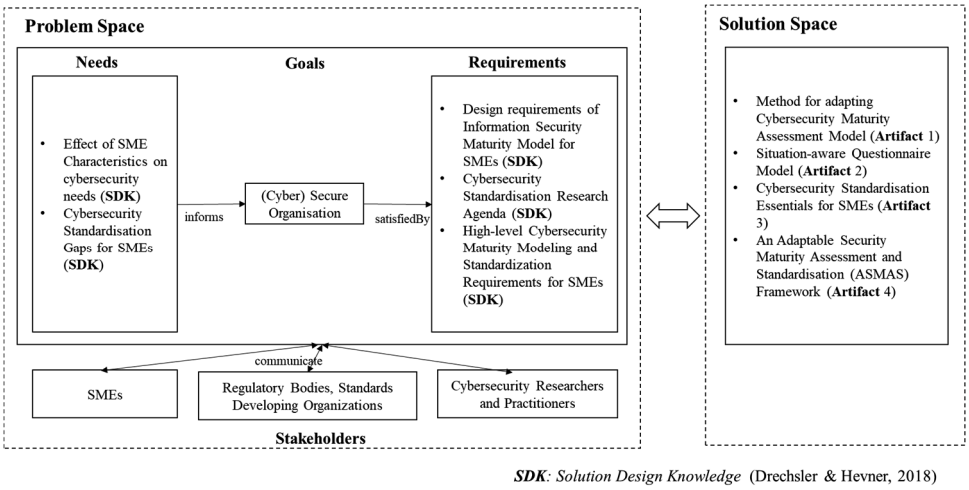


Figure 8.1 Problem Space, Solution Space, and Contributions based on (Maedche et al., 2019)

We have presented the stakeholders for our research in Section 1.2. As can be seen in Figure 8.1, our stakeholders were SMEs, regulatory bodies, standards developing organizations, cybersecurity researchers and practitioners. Our interactions that took place in the course of our research with the stakeholders are as follows.

SMEs: We interacted with SMEs in case studies and workshops, standards developing organizations (ETSI Technical Committee (TC) Cyber) workgroup meetings. We also conducted evaluation interviews with SMEs. The conferences and conference workshops that we attended and presented our work also enabled interactions with SMEs. Our work in the EU H2020 SMESEC project (SMESEC, 2017) helped us interact with SMEs.

Regulatory Bodies: We interacted with regulatory bodies during the Standardization Gaps and Needs workshop (Ch. 5) and conferences.

Standards Developing Organizations (SDOs): We interacted with the SDOs bodies during the Standarzisation Gaps and Needs workshop (Ch. 5). In addition, we participated in ETSI TC Cyber as a member, and we worked as the rapporteur of a work item that was published as a technical report by ETSI.

Cybersecurity Researchers and Practitioners: The conferences and conference workshops that we attended and presented our work and standards developing organizations (ETSI Technical Committee (TC) Cyber) workgroup meetings enabled interactions with cybersecurity researchers and practitioners. Our work in the EU H2020 SMESEC project (SMESEC, 2017) enabled us to interact with cybersecurity researchers and practitioners.

Revisiting our research scope (Section 1.4) and knowledge contributions (*Table 1-3*), Figure 8.2 presents our research contributions per research focus area.

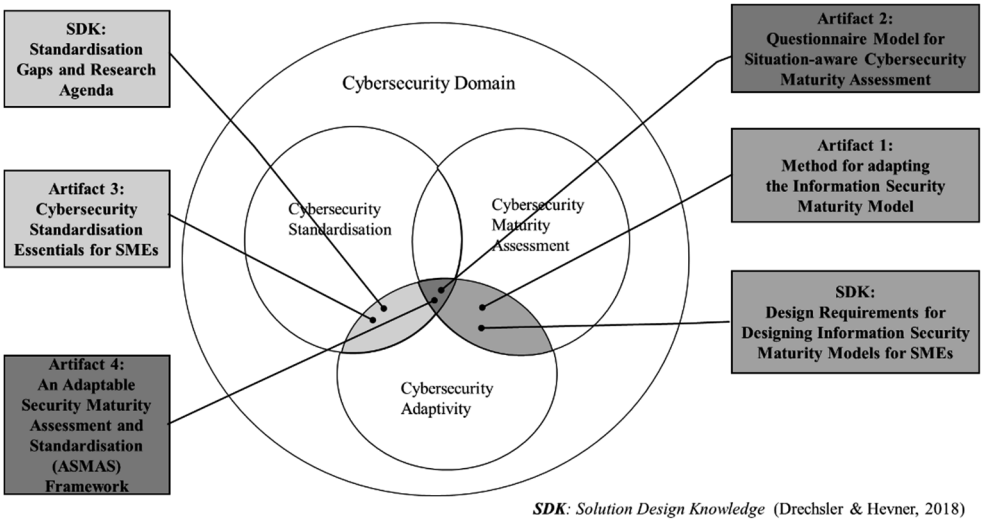


Figure 8.2 Research Contributions per Research Focus Area

We investigated the effect of organisational characteristics on establishing and improving cybersecurity. Organisational characteristics and context determine the cybersecurity requirements and needs that shape the form and function of the possible solutions. For our research objective, this means there needs to be an adaptable solution, as organisations do not have the same characteristics and context. To achieve our research objective, we posed the following main research question.

MRQ: *How can we integrate cybersecurity maturity assessment and cybersecurity standardisation to provide tailored support for organisations in their cybersecurity improvement efforts?*

We used the Design Science Research (DSR) paradigm to answer this research question as our research approach. Our research framework is presented in Section 1.5.

To help answer the MRQ, we posed seven research questions. We investigated these research questions in Chapters 2 – 7. We will discuss the MRQ in two parts. First, we will tackle the "tailored support for organisations in their cybersecurity improvement efforts" part, then the "integrate cybersecurity maturity assessment and cybersecurity standardisation" part. This discussion will allow us to connect the research we have done to answer our MRQ and how the concepts in the MRQ was investigated and addressed. As the MRQ seeks an answer to integrate maturity assessment and standardisation to provide tailored support to organisations to improve their cybersecurity, we will discuss how exactly this was achieved.

Tailored support for organisations is tied to the artifact mutability (i.e., adaptivity) concept as discussed in the Introduction section. We addressed the adaptivity of cybersecurity maturity assessment in Chapter 2 by means of identifying maximum maturity levels applicable to organisational context and provided a method for accomplishing this through a case study in an SME cluster. The adaptivity approach here is mainly indicator-based (i.e. number of employees, revenue). Chapter 3 investigated a situation-aware assessment instrument that

enables adaptation of cybersecurity maturity assessments to organisational contexts and proposed a questionnaire model. Artifact adaptivity in this assessment instrument is an example of mutability-in-design (Pöppelbuß & Goeken, 2015). This assessment instrument can support any type of adaptivity approach. The demonstration of the assessment instrument was done via a critical infrastructure example where we used configuration parameters (i.e. situational questions) to understand the criticality of the infrastructure and the answers to the situational questions were used to configure the assessment instrument for the infrastructure in question. Chapter 4 investigated the design requirements of an information security maturity model that addresses SMEs as its target audience. This research builds on existing design theory (i.e. the design principles of maturity models (Pöppelbuß & Röglinger, 2011)) and proposes design requirements for designing information security maturity models adaptable to SMEs. The adaptivity approach used in this research is based on the internal characteristics of organisations (i.e. SMEs). Design requirement (DR) #15 "Tailored advice for adapting the improvement measures should be provided for different categories of SMEs" addresses the adaptivity requirement. Chapter 5 investigated the cybersecurity standardisation gaps for SMEs and proposed a research agenda to address the gaps. In this research, the workshop findings showed the need for adaptivity in cybersecurity standards. Research gaps was presented to further the research on adaptive cybersecurity standards for SMEs. In Chapter 6, we proposed the cybersecurity standardisation essentials for SMEs. This research incorporates guidance on adaptivity to SMEs according to their roles in the digital ecosystem to provide tailored support.

With regard to the integration of cybersecurity maturity assessment and standardisation part of our MRQ, Chapter 3 was our first attempt to identify the application domain specific constructs (i.e. capability assessment questions) of a maturity assessment model based on the standards in the domain to support standardisation in addition to maturity assessment and improvement of organisations. In Chapter 4, DR #5 "The central constructs that are recognised and well-perceived by SMEs' stakeholders (i.e. standards) should be provided to facilitate the usage of adequate language and understandability of the maturity model." can help SMEs in their standardisation efforts while utilizing the maturity assessment models for improving their cybersecurity. Chapter 7 proposed an integrated cybersecurity maturity assessment and standardisation meta-model, a framework, and a prototype. We evaluated the proposed framework and presented the evaluation results. Artifact adaptivity in this framework is an example of mutability-in-design (Pöppelbuß & Goeken, 2015). The demonstration of the framework was done via a software prototype where we used configuration parameters (i.e. organisational profiles based of organisations' roles in the digital ecosystem) to enable adaptivity to cybersecurity needs of the organisations. As the assessment instrument proposed in Chapter 2, the framework proposed in Chapter 7 incorporated cybersecurity standards and frameworks for the domain specific constructs of the maturity assessment framework. These constructs are capabilities, controls, control categories. This approach made the integration of cybersecurity maturity assessment and standardisation possible. In addition to the use of domain specific standards to support standardisation, the prototype also incorporates risk and threat taxonomies that are used in the application domain. Evaluation of the utility of the framework through interviews and demonstrations showed positive results for the perceived usefulness, ease of use and intention to use the framework. The participants' comments during the interview showed that they recognize how the framework can support standardisation and awareness in addition to maturity assessment.

8.1 Contributions

To answer the main research question, we posed seven research questions. Here, we revisit these questions and briefly review the contributions of each chapter to answer these research questions and formulate a conclusion for each of them. Together, they form an answer to the main research question.

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

To investigate the adaptivity of the focus area maturity model in information security, we conducted research at the Port of Rotterdam in the Netherlands. We profiled the characteristics of an SME cluster in the port area and proposed a method for tailoring a maturity model to the profile of the target cluster. We calculated the maximum maturity levels per focus area that correspond to the cluster profile by applying the method. These tailored target maturity levels help save the scarce resources that SMEs have. The proposed method for this tailoring process was found successful compared with the tailoring made manually by the experts in the field.

Conclusion 1: The focus area maturity model in information security can be methodologically adapted to the organisational characteristics profiles of an SME cluster that eventually will result in focused maturity improvement. The target SMEs can use the cluster-adapted model to assess and capture their information security-related capabilities. 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-implementing information security capabilities for SMEs with scarce resources.

RQ2: *How can we design an instrument for the assessment and improvement of cybersecurity capabilities with implementation guidance and taking into account the organizational characteristics?*

We have designed an assessment instrument that can be adapted to organisational characteristics and provides implementation guidance at the same time. The assessment instrument proposes two different sets of assessment questions. The focus area questions are for assessing the domain (security) capabilities, and the situational questions are for determining the organizational characteristics. The two types of questions interact such that the answers given to the situational questions trigger a pre-planned change in the focus area questions. This includes specific focus area questions being applicable in the case of particular answers to situational questions. As such, this adaptive behaviour of the focus area questions enables a tailored assessment according to the organizational characteristics. We developed the assessment instrument in the SMESEC project, and we adapted the instrument for the cybersecurity assessment of critical infrastructures (Yigit Ozkan & Spruit, 2019a). As described in the chapter, the questionnaire model was successfully operationalized for SMEs in the SMESEC project (SMESEC, 2017) (Shojaifar, Fricker, & Gwerder, 2020). The SMESEC project proposed a lightweight cybersecurity framework for protecting SMEs. One of the SMESEC partners, the University of Applied Sciences Northwestern Switzerland (FHNW), developed a cybersecurity coaching tool named CYSEC. The tool aimed to guide

SMEs with capability improvements and monitor adherence to the recommendations. The questionnaire model was adopted in the CYSEC tool and disseminated as part of the SMESEC framework.

Conclusion 2: We have demonstrated how cybersecurity capability assessment can consider organizational characteristics and adapt accordingly. Organizations are asked more relevant and applicable assessment questions during the assessments that use our instrument. The conceptual thinking (an assessment instrument that incorporates standards, capabilities, improvement actions) originating in this research paved the way to the integrated maturity assessment and standardization framework as described in Chapter 7.

RQ3: *What information security maturity model design requirements can be drawn by considering SME characteristics and the design principles of maturity models?*

We investigated the effect of SME characteristics on the design of information security maturity assessment models and proposed 16 design requirements to be addressed by maturity models attuned to SMEs (see *Table 4-5*). The literature search yields different approaches to identify SME characteristics. This research adopted an approach that considers internal SME characteristics such as having limited resources and short-term vision and orientation instead of an indicator-based approach that considers general organizational attributes such as the number of employees or annual revenue. We argue that using the former approach, the context of the organisations can be better understood as the internal characteristics influence the success of improvement initiatives such as information security improvement programs.

Conclusion 3: SMEs' internal characteristics affect how SMEs should use and adapt maturity models. SME specific information security maturity model design requirements can be identified by considering SMEs' internal characteristics. The 16 information security maturity model design requirements proposed (*Table 4-5*) and mapped to 9 design principles for maturity models can help researchers and practitioners design usable and applicable information security maturity models for SMEs. SMEs can use the design requirements to assess the applicability of available maturity models for their use.

RQ4: *What are the gaps in cybersecurity standardisation for SMEs?*

In this research, we organized a workshop with relevant stakeholders (SMEs, policymakers, regulators, standards developing organizations, cybersecurity researchers, and practitioners) to identify the gaps in cybersecurity standardization for SMEs. As a result of the literature search and the findings from the workshop, a research agenda for SME cybersecurity standardization was proposed.

Conclusion 4: There are gaps in cybersecurity standardization for SMEs that can be grouped into the following five categories:

- lack of SMEs' awareness and involvement in standardization processes,
- lack of cybersecurity standards specifically addressing SMEs,
- challenges of adapting existing cybersecurity standards for SMEs,
- financial barriers of available standards by SMEs, and
- lack of co-operation between the stakeholders.

The corresponding research questions that are proposed (*Table 5-5*) to address these gaps can guide future research.

RQ5: *What are the cybersecurity standardisation essentials for SMEs considering their diverse roles in the digital ecosystem?*

We investigated five standards and frameworks that are applicable to SMEs and proposed a unified set of control categories derived from those standards and frameworks. These standards and frameworks are as follows:

- Cyber Essentials from UK (National Cybersecurity Centre, 2017),
- The Centre for Cyber Security Belgium SME Guide from Belgium (Centre for Cyber security Belgium, 2017),
- Center for Internet Security (CIS) Controls from USA (Center for Internet Security, 2018), and ETSI (global) (ETSI, 2015),
- NIST Small Business Information Security from USA (Paulsen & Toth, 2016), and
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (ISO/IEC, 2013b).

A one-stop guide for SMEs was proposed, including a five-step process with an exemplar scenario walkthrough and guidance for implementation for different SME roles in the digital ecosystem. The ETSI TC Cyber members endorsed an extended version of the proposed guide as a technical report which enabled broader dissemination.

Conclusion 5: Although information security or cybersecurity should be based on risk assessment, we argue that risk assessment might be a complex and resource-demanding process for SMEs with scarce resources. SMEs often do not know where to start to progress towards a secure organisation. A guide that explains the basic terminology, maps several standards and frameworks in a unified and comparable way, and proposes a set of recommended controls according to roles SMEs take in the digital ecosystem can support SMEs in their initiatives to establish and improve cybersecurity or information security.

RQ6: *How can security maturity assessment and standardisation be integrated into an adaptive instrument to support concurrent implementation efforts of digital SMEs?*

In this research, we identified the high-level requirements of an adaptive instrument to address the research question. We proposed an adaptable security maturity assessment and standardization (ASMAS) framework. The proposed framework encompasses five different aspects: Organization, Standardization, Risk Management, Assessment and Measurement, and Improvement. These aspects include SMEs' roles in the digital ecosystem, standards, and frameworks, risks, threats, controls, capabilities, and order of the capabilities. We developed a user-friendly web-based software prototype to demonstrate the ASMAS framework. The successful construction of the prototype shows that the framework is technically feasible. The prototype includes a knowledge base populated with five standards and frameworks, 194 controls, 251 capabilities, 8 threat categories, and 57 risks.

Conclusion 6: An adaptable security maturity assessment and standardization framework combining Organization, Standardization, Risk Management, Assessment and

Measurement, and Improvement aspects in an integrated way can help SMEs establish and improve their security. As SMEs mostly lack security and standard awareness, a framework that incorporates the important aspects, and provides tailored guidance can help them achieve quick results.

We focused on improving organisations' cybersecurity posture to increase protection against cyber-attacks. As the cost of cyber-attacks can be significant for organisations, they increasingly use cyber insurance carriers to transfer cyber risk and to accelerate recovery in the wake of an event. Cyber insurance is not for protection but recovery. Being able to recover is also part of operational resilience. Cyber insurance companies take into account the current cybersecurity measures and the capabilities in place to decide on the amount of the premiums. Cybersecurity maturity assessment and standardisation frameworks such as ASMAS can help SMEs evaluate their cybersecurity posture when negotiating with their cyber insurance carriers.

RQ7: *What is the perceived usefulness, ease of use, and intention to use such an integrated cybersecurity maturity assessment and standardisation framework for SMEs?*

We have conducted with SMEs to evaluate the proposed framework to address the RQ6. The evaluation study incorporated the evaluation criteria from the Technology Acceptance Model (TAM) to explain and predict the framework's utility. The feedback of the SMEs regarding the evaluation constructs (perceived usefulness, ease of use, and intention to use) have been gathered during interview sessions complemented by a survey. The evaluations using a Likert scale (1-5) resulted in average scores of 4.29 for perceived usefulness, 4.14 for perceived ease of use, and 3.62 for intention to use with respect to our evaluation constructs. When we specifically look into the perceived usefulness of the framework for increasing the awareness of cybersecurity standardisation, 85.7% of the interviewees responded positively (agree and strongly agree). The same result has been achieved for the perceived usefulness of the framework for supporting SMEs to assess and improve their information security and cybersecurity. These results show that SMEs can benefit from the approach of integrating cybersecurity maturity assessment and standardisation in the same framework.

Conclusion 7: The ASMAS framework was found to be useful and easy to use. The SMEs were interested in using the prototype should it be available as a tool in the future for either their organizations or their customers. The findings suggest that adaptable security maturity assessment and standardization frameworks such as ASMAS provide a much-needed and feasible foundation for a more secure future for SMEs, guided by established best practices.

Having its roots in the science of the artificial, DSR is a problem-solving paradigm that deals with real world problems by creating design knowledge and novel artifacts (Hevner et al., 2004). Here, we summarise and make explicit how our research and our design entities contribute to existing bodies of knowledge (scientific/research and practical/societal contributions).

Scientific/Research Contributions: In Chapter 2, we build on existing design entity (i.e. ISFAM model) and propose a method for adapting this design entity. Although researchers investigated cybersecurity maturity assessment and its adaptivity to organisational characteristics (Sánchez et al., 2006), (Cholez & Girard, 2014), (Mijnhardt et al., 2016), and (Benz & Chatterjee, 2020), the organisations' role in the digital ecosystem has not been

touched upon as an adaptivity approach (i.e. configuration parameter). In Chapter 3, the situational assessment instrument operationalised as a situation-aware questionnaire model is generic and can be used for any type of adaptivity approach. The interactive nature of focus area (domain specific) assessment questions and situational questions enables the model to use any configuration parameter (e.g. criticality of a critical infrastructure, roles in the digital ecosystem, organisation's size.). In Chapter 4, we build on existing design theories (Pöppelbuß & Röglinger, 2011) (Chandra et al., 2015) and contribute with the proposed design requirements. In Chapter 5, by identifying the stakeholders' perspectives and the trends in the literature, we propose a research agenda for SME standardisation research.

Practical/Societal Contributions: Next to contributions to research, this work has several contributions to practice. The proposed design artefacts address the challenge of SMEs (as our key stakeholders) cybersecurity assessment, improvement and standardisation issues. In Chapter 2, the proposed method can practically be used by SMEs or cluster of SMEs and can support collective learning in the cluster. The situational assessment instrument proposed in Chapter 3 has already been operationalised for SMEs in the SMESEC project (SMESEC, 2017) as part of a lightweight cybersecurity product suite for SMEs. The design requirements proposed in Chapter 4 can be used by researchers and practitioners (as our research's stakeholders) in developing security maturity models for SMEs. Chapter 5 presents gaps in cybersecurity standardisation for SMEs that can be addressed by researchers, standards developing organisations, and can be promoted by cybersecurity and SME organisations (as our research's stakeholders). In Chapter 6, we propose adaptable cybersecurity guidelines for SMEs that builds on exiting standards and frameworks. As discussed in (Shrestha et al., 2018), using standards in DSR projects improves the external validity of the artifacts in terms of practical relevance. As the extended version of this work was published by ETSI as a technical report freely available on their website, we expect a broader reach for this research. The ASMAS framework can be used by researchers and practitioners to design and develop SME adaptable security maturity assessment models that support security standardisation. By doing future research, the software prototype that demonstrates the framework can be developed into a maturity model that can be used in real world. We have recently presented the ASMAS framework prototype to the European Digital SME alliance standardisation experts. The alliance represents over 20.000 digital SMEs. As they were quite interested in the ASMAS framework, they invited us to present our work to a broader audience in their Standardisation working group.

8.2 Research Validity and Limitations

Our research incorporates multiple stakeholder types in cybersecurity and information security that ensures the multivocality of the findings. The stakeholders included in our research were SMEs, regulatory bodies, standards developing organizations, cybersecurity researchers and practitioners. Nevertheless, we acknowledge several limitations to this work as follows.

In Chapter 2, the research is based on a single case study in an SME cluster that constitutes a limitation for the generalizability of the findings. 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 than information security. Second, the proposed method can be used to adapt the demonstrated FAMM (ISFAM) to other target SME clusters in different sectors than transport, logistics and packaging sector.

In Chapter 3, although the questionnaire model was operationalized in a tool and evaluated through case studies in the SMESEC project by one of the project partners (FHNW), we have not participated in their evaluation research. The researchers at FHNW who conducted the case studies published their findings. One of their findings, "The assessment questionnaires and recommendations need to adapt to each specific Small and Medium-sized Businesses (SMB) to increase autonomy" (Shojaifar et al., 2020), supports the importance of situation-aware assessment models.

The SME specific design requirements for information security maturity models (Chapter 4) have been partly addressed in the ASMAS framework. As the ASMAS framework is not a maturity model but a theoretical framework, not all the maturity model design requirements were applicable. Some of the requirements, such as *"DR11 – The assessment methodology should enable the configuration of the criteria according to different categories of SMEs' according to their role in the digital ecosystem."*, were addressed in the ASMAS framework and implemented in the prototype. The constructs that are not addressed in ASMAS but considered important for a maturity model are discussed in the future work section.

We have proposed cybersecurity standardisation gaps for SMEs and a research agenda to fill in these gaps (Chapter 5). The lack of explicit inclusion criteria of the agenda items might be considered a limitation for this research. Although the research agenda items were not traced back to their sources explicitly, we based our proposition on our literature search and workshop findings by performing a thematic analysis.

In Chapter 6, cybersecurity standardisation essentials have been proposed as a design artifact. The extended version of this design artifact has been published by the European Telecommunications Standards Institute (ETSI) as a technical report. The author of this dissertation acted as the rapporteur in discussions and publication of the technical report in the Technical Committee (TC) Cyber of ETSI. Although the technical report publication process is transparent and inclusive (TC Cyber members include public and private organisations, including SMEs), there is no information regarding SMEs' actual use of the technical report. ETSI publishes technical reports and other work items as freely accessible to anyone globally, which we consider a bolster for disseminating our research's output.

The number of evaluation sessions for the ASMAS framework (Chapter 7) we were able to conduct was 7. However, we conducted evaluation interviews with SMEs that differ in the country of origin, size, and role in the digital ecosystem. According to our evaluation design, during the evaluation sessions, the participating SME representatives drew on their intuition to assess whether the framework was usable or easy to use without using the tool in a real-world organisational context. It remains uncertain whether our proposed framework would bring forth similar utility in a more naturalistic evaluation setting, hampering the generalisability of our findings. However, all of the interviewed SMEs were interested in using the prototype should it be available as a tool in the future for either their organizations or their customers.

8.3 Future Research

In this dissertation, we approached the cybersecurity maturity assessment and standardisation topics from various angles to address stakeholders' goals, needs, and requirements, including adaptivity, usability, and applicability. We organized workshops, conducted interviews and case studies, and investigated the literature to understand the problem space. Our design (meta-) artifacts and design artifacts aim to provide novel solutions to the identified problems.

The design requirements proposed in Chapter 4 constitute solution design knowledge for information security maturity models targeting SMEs. These requirements have not been fully validated in the scope of this dissertation. The validation of these requirements and their use in information security maturity models development for SMEs remains a possible future research area. As discussed in Section 8.2, some of the design requirements have been addressed in the ASMAS framework, implemented in the software prototype, and evaluated as part of the framework.

We have proposed a research agenda including gaps in cybersecurity standardisation for SMEs (Chapter 5). We believe the research questions to address the research gaps deserve researchers' and standard developing organizations' attention as future areas. Especially, the research questions related to Gap 3, "Challenges of adapting existing cybersecurity standards for SMEs," have the potential to help SMEs tackle their ongoing challenges in cybersecurity standardisation.

In Chapter 6, cybersecurity standardisation essentials have been proposed as a design artifact. The extended version of this design artifact has been published by the European Telecommunications Standards Institute (ETSI) as a technical report. ETSI Technical Committee (TC) CYBER considers this technical report the first part of a series of standards for SMEs. The research gaps identified in Chapter 5 can guide the development of new standards in the TC CYBER. For instance, an SME-specific cybersecurity standard with different maturity levels for implementation can be considered.

The ASMAS framework and prototype demonstrating the framework are design (meta-) artifacts (Chapter 7). Although the prototype has been developed as a design (meta-) artifact, it has most of the functionalities of a possible design artifact. The design artifact should include security functions (e.g., users, roles, authorisations) needed for a real-world implementation. Future research can implement these security functions, and a more naturalistic evaluation can be carried out in a specific organizational context. The ASMAS

framework can evolve into a cybersecurity maturity model based on standards by incorporating the additional required constructs such as a maturity scoring mechanism and SME-oriented documentation. A further study could investigate how a method can be developed to guide researchers and practitioners to design and build adaptable cybersecurity maturity models based on standards. The ASMAS framework was developed to address the five high-level requirements drawn from the literature. Although the evaluation study findings support the validity of these requirements, future research can be designed to validate them. The ASMAS framework's perceived usefulness for supporting SMEs to assess and improve their information security and cybersecurity and perceived usefulness for helping SMEs increase awareness of information security and cybersecurity security standardization was evaluated. Although we can relate the positive results (85.7 %) for these evaluations to the framework's ability to integrate cybersecurity maturity assessment and standardisation, future research should focus on evaluating the usefulness of integrating cybersecurity maturity assessment and standardisation directly. Future research can focus on the suitability of the ASMAS framework for SMEs in different categories (e.g., digital enablers, digitally dependents).

8.4 Personal Reflection

Finally, I would like to take the opportunity to briefly reflect on my Ph.D. journey on both academic and personal levels in these paragraphs.

Many years of working as a practitioner in the information security domain broadened my experience on organizations' challenges on establishing information security maturity and adopting information security standards. This industry experience, alongside my academic background, enabled me to understand the domain more broadly while pursuing the Ph.D. degree. My experience in the maturity models in the software engineering domain helped me better understand the process and the challenges of building maturity in organisations. As a computer engineer and knowledgeable in the technical aspects of cybersecurity, I have always been interested in the governance structures that provide the direction for improving organizational cybersecurity maturity.

Being part of a European project with international partners was a privilege that enabled and facilitated stakeholder engagement and collaboration in my research. Being part of Utrecht University and the Department of Information and Computing Sciences helped me gain new research and teaching capabilities (e.g., lesson planning, managing student expectations) and enabled collaboration with my colleagues.

I hope my studies can make a positive contribution to organisations struggling with responding to the cybersecurity challenges in practice and eventually help make the world a safer place for individuals and the societies.

Bibliography

About StandICT.eu. (2018, March 30). Retrieved June 20, 2019, from StandICT.eu website: https://www.standict.eu/about-standicteu

About the Business Process Maturity Model Specification Version 1.0. (n.d.). Retrieved August 26, 2018, from https://www.omg.org/spec/BPMM/

Akinsanya, O. O., Papadaki, M., & Sun, L. (2019). Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud? *CERC*, 211–222. New Delhi, India.

Alves, J. F. A. (2013). *Finding Maturity Evolution Paths for Organisational use of Information* (Master Thesis, Instituto Superior Técnico). Instituto Superior Técnico, Portugal. Retrieved from https://fenix.tecnico.ulisboa.pt/downloadFile/395145528220/DMEIC-57552-Joana-Alves.pdf

Baars, T., Mijnhardt, F., Vlaanderen, K., & Spruit, M. (2016). An analytics approach to adaptive maturity models using organizational characteristics. *Decision Analytics*, *3*(1), 1–26. doi: 10.1186/s40165-016-0022-1

Balaji, S., & Murugaiyan, M. S. (2012). Waterfall vs. V-Model vs. Agile: A comparative study on SDLC. *International Journal of Information Technology and Business Management*, *2*(1), 26–30.

Barlette, Y., & Fomin, V. V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 308–308. Hawaii. doi: 10.1109/HICSS.2008.167

Baskerville, R., & Pries-Heje, J. (2014). Design Theory Projectability. In B. Doolin, E. Lamprou, N. Mitev, & L. McLeod (Eds.), *Information Systems and Global Assemblages. (Re)Configuring Actors, Artefacts, Organizations* (pp. 219–232). Springer Berlin Heidelberg.

Baskerville, R., & Pries-Heje, J. (2019). Projectability in Design Science Research. *Journal of Information Technology Theory and Application (JITTA)*, *20*(1), 53–76. Retrieved from https://aisel.aisnet.org/jitta/vol20/iss1/3

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. doi: 10.1007/s12599-009-0044-5

Belzunegui-Eraso, A., & Erro-Garcés, A. (2020). Teleworking in the Context of the Covid-19 Crisis. *Sustainability*, *12*(9), 3662. doi: 10.3390/su12093662

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. doi: 10.1016/j.bushor.2020.03.010

Bititci, U. S., Garengo, P., Ates, A., & Nudurupati, S. S. (2015). Value of maturity models in performance measurement. *International Journal of Production Research*, *53*(10), 3062–3085. doi: 10.1080/00207543.2014.970709

Blanchette, S., & Keeler, J. K. L. (2018). *Self Assessment and the CMMI-AM – A Guide for Government Program Managers* (p. 41). USA: Carnegie Mellon University. Retrieved from Carnegie Mellon University website: https://doi.org/10.1184/R1/6583784.v1

Braue, D. (2021, September 10). Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. Retrieved October 31, 2021, from Cybercrime Magazine website: https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. doi: 10.1191/1478088706qp063oa

BSI. (2019). Navigating and Informing the IoT Standards Landscape | BSI Group. Retrieved June 21, 2019, from https://www.bsigroup.com/en-GB/navigating-and-informing-the-iot-standards-landscape/

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014a). *A Taxonomy of Operational Cyber Security Risks Version 2:* Fort Belvoir, VA: Defense Technical Information Center. doi: 10.21236/ADA609863

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014b). *A Taxonomy of Operational Cyber Security Risks Version 2:* Fort Belvoir, VA: Defense Technical Information Center. doi: 10.21236/ADA609863

CEN. (2016). E-CF overview | European e-Competence Framework. Retrieved August 26, 2018, from https://ecfexplorer.itprofessionalism.org/

CEN-CENELEC. (2019a). CEN/CLC/JTC 13. Retrieved June 20, 2019, from https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B

CEN-CENELEC. (2019b). Cybersecurity standardization—CEN-CENELEC Workshop. Retrieved June 20, 2019, from https://www.cencenelec.eu/news/events/Pages/EV-2019-001.aspx

CEN-CENELEC. (2019c, July 11). SME Standardization Toolkit. Retrieved November 7, 2019, from https://www.cencenelec.eu/sme/SMEST/Pages/default.aspx

CEN-CENELEC. (2019d, November 7). Standards eSME. Retrieved November 7, 2019, from http://www.standards-esme.eu/

Center for Internet Security. (2018). CIS Controls. Retrieved August 31, 2018, from https://learn.cisecurity.org/20-controls-download

Center for Internet Security. (2020). Download the CIS Controls. Retrieved April 15, 2020, from https://learn.cisecurity.org/cis-controls-download

Centre for Cyber security Belgium. (2017, January 20). Guide for SME. Retrieved April 15, 2020, from Centre for Cyber security Belgium website: https://ccb.belgium.be/en/document/guide-sme

Chandra, L., Seidel, S., & Gregor, S. (2015). Prescriptive Knowledge in IS Research: Conceptualizing Design Principles in Terms of Materiality, Action, and Boundary Conditions. *2015 48th Hawaii International Conference on System Sciences*, 4039–4048. HI, USA: IEEE. doi: 10.1109/HICSS.2015.485

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. doi: 10.1002/smr.1609

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., & Dolan, T. (2014). *Cybersecurity capability maturity model (C2M2)* (pp. 1–76).

CIS. (2019, July). CIS Controls and Sub-Controls Mapping to ISO 27001. Retrieved April 19, 2020, from CIS website: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/

CIS Controls V7 Measures & Metrics. (2018, March). Retrieved April 18, 2020, from CIS website: https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/

CMU/SEI. (2006). *Standard CMMI® Appraisal Method for Process Improvement (SCAMPISM) A, Version 1.2: Method Definition Document*. Retrieved from https://resources.sei.cmu.edu/asset_files/Handbook/2006_002_001_14630.pdf

Cocca, P., & Alberti, M. (2009, June 14). *SMEs' Three-step Pyramid: A new Performance Measurement Framework for SMEs*. 13. Göteborg, Sweden.

Cronholm, S., & Göbel, H. (2018). Guidelines Supporting the Formulation of Design Principles. In *Australasian Conference on Information Systems 2018*. University of Technology, Sydney. doi: 10.5130/acis2018.ak

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

Curado, C. (2006). Organisational learning and organisational design. *The Learning Organization*, *13*(1), 25–48. doi: 10.1108/09696470610639112

Curtis, B., Hefley, B., & Miller, S. (2009). *People Capability Maturity Model (P-CMM) Version 2.0, Second Edition*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST. Retrieved from CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST website: https://apps.dtic.mil/sti/citations/ADA512354

Cybersecurity Capability Maturity Model (C2M2) | Department of Energy. (n.d.). Retrieved July 19, 2018, from https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

Cyberwatching.eu. (2018). *Cybersecurity Standard Gaps Analysis*. Retrieved from https://cyberwatching.eu/sites/default/files/White-Paper-Cybersecurity-Standard-Gaps-Analysis_Cyberwatching.eu-October2018.pdf

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. doi: 10.2307/249008

de Bruin, T., Freeze, R., Kulkarni, U., & Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *ACIS 2005 Proceedings*, 11. Sydney. Retrieved from https://aisel.aisnet.org/acis2005/109/

de Vries, H., Blind, K., Mangelsdorf, A., & Verheul, H. (2009). *SME access to European standardization*. 95. Retrieved from https://www.unms.sk/swift_data/source/dokumenty/technicka_normalizacia/msp/SME-AccessReport.pdf

de Vries, H., Jakobs, K., Egyedi, T. M., Eto, M., Fertig, S., Kanevskaia, O., … Scaramuzzino, G. (2018). Standardization: Towards an Agenda for Research. *International Journal of Standardization Research (IJSR)*, *16*(1), 52–59. doi: 10.4018/IJSR.2018010104

de Vries, H., Verheul, H., & Willemse, H. (2003). *Stakeholder identification in IT standardization processes*. 12–14. USA.

Dekker, M., Liveri, D., Europäische Union, & Agentur für Netz- und Informationssicherheit. (2015). *Cloud security guide for SMEs cloud computing security risks and opportunities for SMEs*. Heraklion. Retrieved from https://doi.org/10.2824/508412

Digital SME Alliance. (2017). *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*. Retrieved from

https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf

Drechsler, A., & Hevner, A. R. (2018). Utilizing, Producing, and Contributing Design Knowledge in DSR Projects. In S. Chatterjee, K. Dutta, & R. P. Sundarraj (Eds.), *Designing for a Digital and Globalized World* (pp. 82–97). Cham: Springer International Publishing. doi: 10.1007/978-3-319-91800-6_6

EC. (2016, April 19). Communication on ICT Standardisation Priorities. Retrieved December 11, 2019, from ICT Standardisation Priorities for the Digital Single Market website: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0176&from=EN

EC. (2017, September 19). The EU cybersecurity certification framework [Text]. Retrieved April 12, 2020, from Shaping Europe's digital future—European Commission website: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

EC. (2018). Cybersecurity Act [Text]. Retrieved April 12, 2020, from European Commission website: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

EC. (2019). *2019 Rolling Plan for ICT Standardisation*. Retrieved from https://ec.europa.eu/docsroom/documents/34788/attachments/1/translations/en/renditions/native

ECSO. (2017). *ECSO State of the Art Syllabus v2*. Retrieved from http://www.ecs-org.eu/documents/uploads/updated-sota.pdf

ECSO. (2019a). European Cyber Security Organisation—Work Group 1. Retrieved June 20, 2019, from ECSO - European Cyber Security Organisation website: https://ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management

ECSO. (2019b). European Cyber Security Organisation—Work Group 4. Retrieved June 20, 2019, from ECSO - European Cyber Security Organisation website: https://ecs-org.eu/working-groups/wg4-support-to-smes-coordination-with-countries-and-regions

ENISA. (2020). Standardisation in support of the Cybersecurity Certification [Report/Study]. Retrieved April 12, 2020, from https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i

ETSI. (2011). *Participation of SMEs in Standardization*. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/WP_No_6_SME_FINAL.pdf

ETSI. (2015). *ETSI TR 103 305 CYBER; Critical Security Controls for Effective Cyber Defence*.

ETSI. (2018a). *CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls*. Retrieved from https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf

ETSI. (2018b). *ETSI TR 103 305 .CYBER; Attribute Based Encryption for Attribute Based Access Control*.

ETSI. (2019). ETSI TS 103 645—Cyber Security for Consumer Internet of Things. Retrieved June 21, 2019, from https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

ETSI. (2021). *CYBER; Cybersecurity for SMEs; Part 1: Cybersecurity Standardization Essentials*. ETSI. Retrieved from https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf

ETSI - Cyber Security. (2019). Retrieved June 20, 2019, from https://www.etsi.org/committee/1393-cyber

ETSI TC CYBER. (2021). *CYBER; Cybersecurity for SMEs; Part 1: Cybersecurity Standardization Essentials* (Technical Report No. ETSI TR 103 787-1). Retrieved from https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf

European Commission. (2016, July 5). SME definition [Text]. Retrieved August 10, 2021, from Internal Market, Industry, Entrepreneurship and SMEs—European Commission website: https://ec.europa.eu/growth/smes/sme-definition_en

European Digital SME Alliance. (2020). *DIGITAL SME Recommendations on COVID-19-Recovery*. Brussels. Retrieved from https://www.digitalsme.eu/digital/uploads/DIGITAL-SME-Recommendations-on-COVID-19-Recovery.pdf

European Network and Information Security Agency. (2016). *Guidelines for SMEs on the security of personal data processing*. ENISA.

Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science*, *2*(1), 15–24. doi: 10.1007/s13753-011-0002-y

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge University Press.

Gañán, C. H., Ciere, M., & van Eeten, M. (2017). Beyond the pretty penny: The Economic Impact of Cybercrime. *Proceedings of the 2017 New Security Paradigms Workshop*, 35–45. Santa Cruz, CA, USA: ACM Press. doi: 10.1145/3171533.3171535

Goldkuhl, G. (2004). Design Theories in Information Systems—A Need for Multi-Grounding. *Journal of Information Technology Theory and Application (JITTA)*, *6*(2). Retrieved from https://aisel.aisnet.org/jitta/vol6/iss2/7

Gregor, S. (2002). Design Theory in Information Systems. *Australasian Journal of Information Systems*, *10*(1). doi: 10.3127/ajis.v10i1.439

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Q.*, *37*(2), 337–356. doi: 10.25300/MISQ/2013/37.2.01

Gregor, S., & Iivari, J. (2007). Designing for Mutability in Information Systems Artifacts. In D. Hart & S. Gregor (Eds.), *Information Systems Foundations: Theory, Representation and Reality* (1st ed.). ANU Press. doi: 10.22459/ISFTRR.11.2007.01

Hayes, W., & Zubrow, D. (1995). *Moving On Up: Data and Experience Doing CMM-Based Process Improvement* (Technical Report No. CMU/SEI-95-TR-008; p. 41). Pittsburgh, Pennsylvania, USA: Software Engineering Institute, Carnegie Mellon University. Retrieved from Software Engineering Institute, Carnegie Mellon University website: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1995_005_001_16391.pdf

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*(6), 1285–1305. doi: 10.1007/s10796-019-09959-1

Helgesson, Y. Y. L., Höst, M., & Weyns, K. (2012). A review of methods for evaluation of maturity models for process improvement. *Journal of Software: Evolution and Process*, *24*(4), 436–454. doi: 10.1002/smr.560

Hevner. (2007). *A Three Cycle View of Design Science Research*. *19*, 7.

Hevner, A., & Chatterjee, S. (2010). A Science of Design for Software-Intensive Systems. In A. Hevner & S. Chatterjee (Eds.), *Design Research in Information Systems: Theory and Practice* (pp. 63–77). Boston, MA: Springer US. doi: 10.1007/978-1-4419-5653-8_6

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Q.*, *28*(1), 75–105. Retrieved from http://dl.acm.org/citation.cfm?id=2017212.2017217

Hudson, M. (2001). *Introducing integrated performance measurement into small and medium sized enterprises* (Research Theses, University of Plymouth). University of Plymouth, UK. Retrieved from https://pearl.plymouth.ac.uk/handle/10026.1/400

ISO. (2018a). ISO 30414:2018 Human resource management—Guidelines for internal and external human capital reporting. Retrieved March 6, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/93/69338.html

ISO. (2018b). ISO 31000:2018 Risk management—Guidelines. Retrieved March 20, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/56/65694.html

ISO. (2018). ISO and Small & Medium Enterprises. Retrieved September 2, 2018, from https://www.iso.org/iso-and-smes.html

ISO. (2019a). Benefits of standards. Retrieved June 8, 2019, from ISO website: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/benefits-of-standards.html

ISO. (2019b). ISO 14005:2019 Environmental management systems—Guidelines for a flexible approach to phased implementation. Retrieved March 6, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/23/72333.html

ISO. (2019c). ISO 56003:2019 Innovation management—Tools and methods for innovation partnership—Guidance. Retrieved March 6, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/89/68929.html

ISO. (2019d, May 14). Standards. Retrieved May 14, 2019, from ISO website: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards.html

ISO. (2021). ISO - ISO/IEC JTC 1—Information technology. Retrieved August 17, 2021, from https://www.iso.org/committee/45020/x/catalogue/

ISO/IEC. (2003). ISO/IEC 15504-2:2003—Information technology—Process assessment—Part 2: Performing an assessment. Retrieved September 28, 2018, from https://www.iso.org/standard/37458.html

ISO/IEC. (2012). ISO/IEC 27032:2012—Information technology—Security techniques—Guidelines for cybersecurity. Retrieved December 14, 2017, from https://www.iso.org/standard/44375.html

ISO/IEC. (2013a). *ISO/IEC 27001:2013—Information technology—Security techniques—Information security management systems—Requirements*. Retrieved from https://www.iso.org/standard/54534.html

ISO/IEC. (2013b). *ISO/IEC 27002:2013—Information technology—Security techniques—Code of practice for information security controls*. Retrieved from https://www.iso.org/standard/54533.html

ISO/IEC. (2016). ISO/IEC Guide 17:2016 Guide for writing standards taking into account the needs of micro, small and medium-sized enterprises. Retrieved August 17, 2021, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/73/67340.html

ISO/IEC. (2018a). ISO/IEC 27000:2018. Retrieved March 20, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73906.html

ISO/IEC. (2018b). ISO/IEC 27005:2018 Information security risk management. Retrieved March 20, 2020, from ISO website: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html

ISSA UK. (2018). ISSA UK Home Page. Retrieved December 11, 2019, from https://www.issa-uk.org/

JAMK University of Applied Sciences. (2020). FINCSC – Finnish Cyber Security Certificate. Retrieved March 3, 2020, from Finnish Cyber Security Certificate website: https://www.fincsc.fi/en/services/

Jones, D., & Gregor, S. (2007). The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, *8*(5). doi: 10.17705/1jais.00129

Kayworth, T., & Whitten, D. (2012). *Effective Information Security Requires a Balance of Social and Technology Factors* (SSRN Scholarly Paper No. ID 2058035). Rochester, NY: Social Science Research Network. Retrieved from Social Science Research Network website: https://papers.ssrn.com/abstract=2058035

Kertysova, K., Bhattacharyya, K., Frinking, E., Dool, K. van den, Maričić, A., & 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. Retrieved from https://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

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5–7. doi: 10.1016/S1361-3723(15)30017-8

Lanz, J., & Sussman, B. I. (2020). Information Security Program Management in A COVID-19 World. *The CPA Journal*, *90*(6), 28–36. Retrieved from http://go.gale.com/ps/i.do?p=AONE&sw=w&issn=07328435&v=2.1&it=r&id=GALE%7CA632049489&sid=googleScholar&linkaccess=abs

Lawson, C., & Lorenz, E. (1999). Collective Learning, Tacit Knowledge and Regional Innovative Capacity. *Regional Studies*, *33*(4), 305–317. doi: 10.1080/713693555

Le, N. T., & Hoang, D. B. (2016). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 1–7. USA. doi: 10.1109/PCCC.2016.7820663

Lowry, P. B., Dinev, T., & 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*, *26*(6), 546–563. doi: 10.1057/s41303-017-0066-x

Maedche, A., Gregor, S., Morana, S., & Feine, J. (2019). Conceptualization of the Problem Space in Design Science Research. In B. Tulu, S. Djamasbi, & G. Leroy (Eds.), *Extending the Boundaries of Design Science Theory and Practice* (pp. 18–31). Cham: Springer International Publishing. doi: 10.1007/978-3-030-19504-5_2

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2012). Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids. *IEEE Transactions on Engineering Management*, *59*(1), 138–159. doi: 10.1109/TEM.2010.2077289

Mansfield, M. (2017, January 3). Cyber Security Statistics: Numbers Small Businesses Need to Know. Retrieved June 25, 2019, from Small Business Trends website: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & 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.* Heraklion: ENISA. Retrieved from http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Marinos, L. (2016a). *ENISA Threat Taxonomy*. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

Marinos, L. (2016b). *ENISA Threat Taxonomy* (p. 24). Greece: ENISA.

Mayer, N. (2010). A Cluster Approach to Security Improvement according to ISO/IEC 27001. *Proceedings of the 17th European Systems & Software Process Improvement and Innovation Conference (EUROSPI'10)*. Presented at the EUROSPI 2010, Grenoble, France.

McLennan, M., & Group, S. (2021). *The Global Risks Report 2021 16th Edition* (p. 97). Retrieved from http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Mendix. (2021). Mendix—Go Make It. Retrieved March 26, 2021, from Mendix website: https://www.mendix.com/

Mettler, T. (2009). *A Design Science Research Perspective on Maturity Models in Information Systems—Alexandria* (No. BE IWI/HNE/03; p. 13). Switzerland: Institute of Information Management, Universtiy of St. Gallen. Retrieved from Institute of Information Management, Universtiy of St. Gallen website: https://www.alexandria.unisg.ch/214531/

Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science*, *3*(1/2), 81. doi: 10.1504/IJSSS.2011.038934

Mettler, T., & Rohner, P. (2009). Situational Maturity Models As Instrumental Artifacts for Organizational Design. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 22:1-22:9. New York, NY, USA: ACM. doi: 10.1145/1555619.1555649

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems*, *56*(2), 106–115. doi: 10.1080/08874417.2016.1117369

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review*, *22*(4), 853–886. doi: 10.2307/259247

Morgan, S. (2019, June 10). Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021. Retrieved October 31, 2021, from Cybercrime Magazine website: https://cybersecurityventures.com/cybersecurity-market-report/

Mori, I. (2021). *Cyber Security Breaches Survey 2021: Statistical Release*. 66.

National Cybersecurity Centre. (2017, September 26). National Cybersecurity Centre—CyberEssentials (UK). Retrieved December 11, 2019, from Cyber Essentials website: https://www.cyberessentials.ncsc.gov.uk/

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST Cybersecurity White Paper). Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.CSWP.02122014

NCSC. (2020). About Cyber Essentials. Retrieved April 15, 2020, from https://www.ncsc.gov.uk/cyberessentials/overview

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST CSWP 04162018; p. NIST CSWP 04162018). Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.CSWP.04162018

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, *5*(1), 14–37. Retrieved from http://www.jstor.org/stable/2635068

North, K., Aramburu, N., & Lorenzo, O. J. (2019). Promoting digitally enabled growth in SMEs: A framework proposal. *Journal of Enterprise Information Management*, *33*(1), 238–262. doi: 10.1108/JEIM-04-2019-0103

OECD. (2017). *Enhancing the Contributions of SMEs in a Global and Digitalised Economy*. Paris, France. Retrieved from https://www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf

OECD. (2021, February 3). The Digital Transformation of SMEs [Text]. Retrieved August 19, 2021, from http://www.oecd.ilibrary.org/industry-and-services/the-digital-transformation-of-smes_bdb9256a-en

OMG. (2017). Unified Modeling Language Specification Version 2.5.1. Retrieved November 24, 2018, from https://www.omg.org/spec/UML/

OWASP Foundation. (2020). Denial of Service Software Attack. Retrieved June 22, 2020, from https://owasp.org/www-community/attacks/Denial_of_Service

Ozkan, B. Y., & Spruit, M. (2019, July 1). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. Retrieved June 26, 2020, from International Journal of Standardization Research (IJSR) website: www.igi-global.com/article/cybersecurity-standardisation-for-smes/253856

Parkin, S., Fielder, A., & Ashby, A. (2016). Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes. *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, 69–80. New York, NY, USA: Association for Computing Machinery. doi: 10.1145/2995959.2995967

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability Maturity Model, Version 1.1. *IEEE Software; Los Alamitos*, *10*(4), 18–27. doi: http://dx.doi.org/10.1109/52.219617

Paulsen, C. (2016). Cybersecuring Small Businesses. *Computer*, *49*(8), 92–97. doi: 10.1109/MC.2016.223

Paulsen, C., & Toth, P. (2016). *Small Business Information Security: The Fundamentals* (No. NIST IR 7621r1; p. NIST IR 7621r1). USA: National Institute of Standards and Technology. doi: 10.6028/NIST.IR.7621r1

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

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007b). A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst.*, *24*(3), 45–77. doi: 10.2753/MIS0742-1222240302

People CMM: A Framework for Human Capital Management (SEI Series in Software Engineering Series) | ISBNdb. (n.d.). Retrieved August 26, 2018, from https://isbndb.com/book/9780321553904

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (Fifth edition). Upper Saddle River, NJ: Prentice Hall.

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*. doi: 10.17705/1CAIS.02927

Pöppelbuß, J., & Goeken, M. (2015). Understanding the Elusive Black Box of Artifact Mutability. *Wirtschaftsinformatik Proceedings 2015*. Retrieved from https://aisel.aisnet.org/wi2015/104

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. *ECIS 2011*. Presented at the ECIS, Finland.

Porter, M. E. (2000). Location, Clusters, and Company Strategy. In *The Oxford Handbook of Economic Geography* (pp. 253–274). Oxford: Oxford University Press. Retrieved from https://www.hbs.edu/faculty/Pages/item.aspx?num=5432

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. doi: 10.1002/itl2.247

Pries-Heje, J., Baskerville, R., & Venable, J. (2008). Strategies for Design Science Research Evaluation. *ECIS 2008 Proceedings*. Presented at the Ireland. Ireland. Retrieved from https://aisel.aisnet.org/ecis2008/87

Purao, S. (2013). Truth or Dare: The Ontology Question in Design Science Research. *Journal of Database Management*, *24*(3), 51–66. doi: 10.4018/jdm.2013070104

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information & Computer Security*, *28*(4), 627–644. doi: 10.1108/ICS-03-2019-0039

Rainer, A., & Hall, T. (2002). Key success factors for implementing software process improvement: A maturity-based analysis. *Journal of Systems and Software*, *62*(2), 71–84. doi: 10.1016/S0164-1212(01)00122-4

Ritchie, L., & Dale, B. G. (2000). Self-assessment using the business excellence model: A study of practice and process. *International Journal of Production Economics*, *66*(3), 241–254. doi: 10.1016/S0925-5273(99)00130-9

Rosemann, M., & Bruin, T. (2005). Towards a Business Process Management Maturity Model. *ECIS 2005 Proceedings*. Retrieved from https://aisel.aisnet.org/ecis2005/37

Sánchez, L. E., Villafranca, D., & Piattini, M. (2006). Developing a Maturity Model for Information System Security Management within Small and Medium Size Enterprises: *Proceedings of the 4th International Workshop on Security in*

Information Systems, 256–266. Paphos, Cyprus: SciTePress - Science and and Technology Publications. doi: 10.5220/0002502602560266

Sánchez, L. E., Villafranca, D., & Piattini, M. (2007). MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs: *Proceedings of the 5th International Workshop on Security in Information Systems*, 233–244. Funchal, Madeira, Portugal: SciTePress - Science and and Technology Publications. doi: 10.5220/0002430402330244

Sanchez-Puchol, F., & Pastor-Collado, J. A. (2017). Focus Area Maturity Models: A Comparative Review. In M. Themistocleous & V. Morabito (Eds.), *Information Systems* (pp. 531–544). Springer International Publishing.

SBS. (2016). *Small Business Standards User Guide for European SMEs on ISO 26000 Guidance on Social Responsibility*. SBS. Retrieved from https://www.sbs-sme.eu/sites/default/files/publications/SBS%20SME%20ISO%20User%20Guide%202016_FINAL.pdf

SBS. (2021). SBS SME | Small Business Standards. Retrieved August 17, 2021, from https://www.sbs-sme.eu/

SBS, Digital SME Alliance. (2018). *SME Guide for the implementation of ISOIEC 27001 on information security management*. Small Business Standards. Retrieved from https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management.pdf

Scarfone, K., Benigni, D., & Grance, T. (2009). Cyber Security Standards. In *Wiley Handbook of Science and Technology for Homeland Security* (pp. 1–10). American Cancer Society. doi: 10.1002/9780470087923.hhs439

SCORE. (2018). 43% of Cyberattacks Target Small Businesses. Retrieved October 31, 2021, from https://www.prnewswire.com/news-releases/43-of-cyberattacks-target-small-businesses-300729384.html

Shojaifar, A., Fricker, S. A., & Gwerder, M. (2018). Elicitation of SME Requirements for Cybersecurity Solutions by Studying Adherence to Recommendations. *REFSQ 2018 Joint Proceedings of the Co-Located Events*. Presented at the 24th International Conference on Requirements Engineering: Foundation for Software Quality.

Shojaifar, A., Fricker, S. A., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-case Study. In L. Drevin, S. Von Solms, & M. Theocharidou (Eds.), *Information Security Education. Information Security in Action* (pp. 110–124). Cham: Springer International Publishing. doi: 10.1007/978-3-030-59291-2_8

Shrestha, A., Cater-Steel, A., Toleman, M., & Rout, T. (2018). Benefits and relevance of International Standards in a design science research project for process assessments. *Computer Standards & Interfaces*, *60*, 48–56. doi: 10.1016/j.csi.2018.04.011

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. doi: 10.1016/j.im.2008.12.007

Sjöström, J., Ågerfalk, P., & Lochan, R. (2011). MUTABILITY MATTERS: BASELINING THE CONSEQUENCES OF DESIGN. *MCIS 2011 Proceedings*. Retrieved from https://aisel.aisnet.org/mcis2011/33

Smart Grid Maturity Model, Version 1.2: Model Definition. (n.d.). Retrieved August 26, 2018, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10035

Smedlund, A., & Pöyhönen, A. (2005). Chapter 14 - Intellectual Capital Creation in Regions: A Knowledge System Approach. In A. Bounfour & L. Edvinsson (Eds.), *Intellectual Capital for Communities* (pp. 227–252). Boston: Butterworth-Heinemann. doi: 10.1016/B978-0-7506-7773-8.50017-0

SMESEC. (2017). About SMESEC. Retrieved June 20, 2019, from https://www.smesec.eu/about.html

SMESEC. (2018, June). CySME Maturity Model. Retrieved June 27, 2019, from https://www.smesec.eu/News/180610_SMESecMM_UU.html

Sonnenberg, C., & vom Brocke, J. (2012). Evaluation Patterns for Design Science Research Artefacts. In M. Helfert & B. Donnellan (Eds.), *Practical Aspects of Design Science* (pp. 71–83). Berlin, Heidelberg: Springer. doi: 10.1007/978-3-642-33681-2_7

Spruit, M., & Roeling, M. (2014). ISFAM: The Information Security Focus Area Maturity Model. *Proceedings of the European Conference on Information Systems (ECIS) 2014, June 9-11, 2014*, 15. Tel Aviv, Israel: Association for Information Systems. Retrieved from https://aisel.aisnet.org/ecis2014/proceedings/track14/6

StandICT.eu. (2019). Standards Watch. Retrieved June 21, 2019, from StandICT.eu website: https://www.standict.eu/standards-watch

Staples, M., Niazi, M., Jeffery, R., Abrahams, A., Byatt, P., & Murphy, R. (2007). An exploratory study of why organizations do not adopt CMMI. *Journal of Systems and Software*, *80*(6), 883–895. doi: 10.1016/j.jss.2006.09.008

Steenbergen, M. van, Berg, M. van den, & Brinkkemper, S. (2007). An Instrument for the Development of the Enterprise Architecture Practice. *Proceedings of the Ninth International Conference on Enterprise Information Systems*, *2*, 14–22. Madeira, Portugal. doi: 10.5220/0002362300140022

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2010). The Design of Focus Area Maturity Models. *Global Perspectives on Design Science Research*, 317–332. Switzerland: Springer, Berlin, Heidelberg. doi: 10.1007/978-3-642-13335-0_22

Storey, D. J. (1994). *Understanding The Small Business Sector*. 48.

The European Digital SME Alliance. (2020a). *The EU Cybersecurity Act and the Role of Standards for SMEs*. Brussels. Retrieved from https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf

The European Digital SME Alliance. (2020b, February 7). Standardisation Success Story: "Relevance to SMEs" becomes a priority for new ETSI standards. Retrieved March 6, 2020, from European Digital SME Alliance website: https://www.digitalsme.eu/relevance-to-smes-becomes-a-priority-for-new-etsi-standards/

The Open Group. (2017). *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*. Retrieved from https://publications.opengroup.org/c17b

Thuan, N., Drechsler, A., & Antunes, P. (2019). Construction of Design Science Research Questions. *Communications of the Association for Information Systems*, *44*(1). doi: 10.17705/1CAIS.04420

Tisdale, S. M. (2016). *Architecting a Cybersecurity Management Framework: Navigating and Traversing Complexity, Ambiguity, and Agility - ProQuest* (Doctoral Thesis, Robert Morris University). Robert Morris University, Pennsylvania, USA. Retrieved from https://search.proquest.com/openview/0934ecf7a7afd537d2f2307843e1fdb3/1?cbl=18750&diss=y&pq-origsite=gscholar

TMMi Model. (n.d.). Retrieved August 26, 2018, from TMMI website: https://www.tmmi.org/tmmi-model/

UK Government. (2015, March). Small businesses: What you need to know about cyber security. Retrieved April 16, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf

UK National Cyber Security Centre. (2020, April). Advisory: COVID-19 exploited by malicious cyber actors. Retrieved January 6, 2021, from https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

US Department of Energy. (2014). *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Retrieved from https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

US Department of Homeland Security. (2014). *National Initiative for Cybersecurity Education – Cybersecurity Capability Maturity Model White Paper*. United States. Department of Homeland Security. Retrieved from https://www.hsdl.org/?view&did=798503

van de Weerd, I., & Brinkkemper, S. (2009). Meta-modeling for situational analysis and design methods. In *Handbook of research on modern systems analysis and design technologies and applications* (pp. 35–54). Pennsylvania, USA: IGI Global.

van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I., & Bekkers, W. (2010). The Design of Focus Area Maturity Models. In R. Winter, J. L. Zhao, & S. Aier (Eds.), *Global Perspectives on Design Science Research* (pp. 317–332). Berlin, Heidelberg: Springer Berlin Heidelberg.

van Steenbergen, M., Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2013). Improving IS Functions Step by Step: The Use of Focus Area Maturity Models. *Scandinavian Journal of Information Systems*, *25*(2). Retrieved from http://aisel.aisnet.org/sjis/vol25/iss2/2

Waldt, G. V. der. (2013). Disaster Risk Management: Disciplinary status and prospects for a unifying theory : original research. *Jamba : Journal of Disaster Risk Studies*, *5*(2), 1–11. doi: 10.4102/jamba.v5i2.76

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. doi: 10.1016/j.infsof.2012.07.007

Westerlund, M. (2020). Digitalization, Internationalization and Scaling of Online SMEs. *Technology Innovation Management Review*, *10*(4), 48–57. doi: http://doi.org/10.22215/timreview/1346

Williams, R., & 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*, *23*(1), 1–22. JSTOR. Retrieved from https://www.jstor.org/stable/23207869

Winter, R. (2011). Problem Analysis for Situational Artefact Construction in Information Systems. In A. Carugati & C. Rossignoli (Eds.), *Emerging Themes in Information Systems and Organization Studies* (pp. 97–113). Heidelberg: Physica-Verlag HD. doi: 10.1007/978-3-7908-2739-2_8

Workshop: Cybersecurity Standards: What impacts and gaps for SMEs. (2019, April 15). Retrieved June 20, 2019, from StandICT.eu website: https://www.standict.eu/events/cybersecurity-standards-what-impacts-and-gaps-smes

World Bank. (2021). World Bank SME Finance [Text/HTML]. Retrieved August 17, 2021, from World Bank website: https://www.worldbank.org/en/topic/smefinance

World Economic Forum. (2018). *The Global Risks Report*. World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

World Economic Forum. (2020). *The Global Risks Report 2020*. Retrieved from https://wef.ch/2QfEAR9

Yigit Ozkan, B., & Spruit, M. (2019a). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. In A. P. Fournaris, K. Lampropoulos, & E. Marín Tordera (Eds.), *Information and Operational Technology Security Systems* (pp. 49–60). Heraklion, Crete, Greece: Springer International Publishing, New York, USA. doi: https://doi.org/10.1007/978-3-030-12085-6_5

Yigit Ozkan, B., & Spruit, M. (2019b). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. *International Journal of Standardization Research (IJSR)*, *17*(2), 32. doi: 10.4018/IJSR.20190701.oa1

Yigit Ozkan, B., & Spruit, M. (2020). Addressing SME Characteristics for Designing Information Security Maturity Models. In N. Clarke & S. Furnell (Eds.), *Human Aspects of Information Security and Assurance* (pp. 161–174). Cham: Springer International Publishing. doi: 10.1007/978-3-030-57404-8_13

Yigit Ozkan, B., & Spruit, M. (2021). Cybersecurity Standardisation Essentials for European SMEs. In *SMESEC: Protecting Small and Medium-sized Enterprises digital technology through an innovative cyberSECurity framework*. Springer.

Yigit Ozkan, B., Spruit, M., Wondolleck, R., & Burriel Coll, V. (2019). Modelling adaptive information security for SMEs in a cluster. *Journal of Intellectual Capital*, *21*(2), 235–256. doi: 10.1108/JIC-05-2019-0128

Yigit Ozkan, B., van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. *Journal of Cybersecurity and Privacy*, *1*(1), 119–139. doi: 10.3390/jcp1010007

Yu, D., Xiao, H., & Bo, Q. (2018). The Dimensions of Organizational Character and Its Impacts on Organizational Performance in Chinese Context. *Frontiers in Psychology*, *9*(1049). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6024914/

Zhao, S., Guo, Y., Sheng, Q., & Shyr, Y. (2014). Advanced Heat Map and Clustering Analysis Using Heatmap3. *BioMed Research International*, *2014*, 1–6. doi: 10.1155/2014/986048

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. doi: 10.1016/j.ijhcs.2019.05.005

List of Publications

Internationally refereed publications included in the dissertation

1. Yigit Ozkan, B., Spruit, M., Wondolleck, R., & Burriel Coll, V. (2019). Modelling adaptive information security for SMEs in a cluster. *Journal of Intellectual Capital, 21*(2), 235–256.
2. Yigit Ozkan, B., & Spruit, M (2019). A Questionnaire Model for Cybersecurity Maturity Assessment for Critical Infrastructures. In Fournaris, A., Lampropoulos, K., & Tordera, E. (Eds.), *Lecture Notes in Computer Science (LNCS) 11398 11398*, *Information and Operational Technology Security Systems. First International Workshop, IOSec 2018, CIPSEC Project* (pp. 49–60). IOSec 2018, 13 Sept 2018, Heraklion, Crete, Greece: Springer.
3. Yigit Ozkan, B., & Spruit, M. (2020). Addressing SME Characteristics for Designing Information Security Maturity Models. In Clarke N., Furnell S. (Eds.), *IFIP Advances in Information and Communication Technology: Human Aspects of Information Security and Assurance* (pp. 161–174). HAISA 2020, 8-10 July, Online: IFIP.
4. Yigit Ozkan, B., & Spruit, M (2019). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. *International Journal of Standardization Research, 17*(2), 1–25.
5. Yigit Ozkan, B., & Spruit, M.R. (In press). Cybersecurity Standardisation Essentials for European SMEs. In Fricker, S., Ruiz, J.F., & Tselios, C. (Eds.), *SMESEC: Protecting Small and Medium-sized Enterprises digital technology through an innovative cyberSECurity framework*. Springer. Extended version published by ETSI
6. Yigit Ozkan, B., & Spruit, M.R. (Submitted). Adaptable Security Maturity Assessment and Standardization for Digital SMEs.

Other publications (not included in the dissertation)

1. Yigit Ozkan, B., van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. *Journal of Cybersecurity and Privacy, 1*, 119–140.
2. Haastrecht, M. van, Sarhan, I., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). SYMBALS: A Systematic Review Methodology Blending Active Learning and Snowballing. *Frontiers in Research Metrics and Analytics, 6*, Section Text-mining and Literature-based Discovery.
3. Haastrecht, M. van, Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. *Applied Sciences, 11*(15), Human Factors in the Digital Society, 6909.

Summary

Organisations' cybersecurity requirements have several origins, including the need to protect their business from cyberattacks, comply with laws and regulations, and build trust. Cyber threats and new regulations emerge, thus the need to implement measures and assure compliance. Cybersecurity maturity assessments and cybersecurity standardisation can be used to implement measures and provide assurance for regulators. Therefore, this dissertation investigates cybersecurity maturity assessment and cybersecurity standardisation to improve organisations' cybersecurity. We state our research objective as follows: *To support the improvement of organisations' cybersecurity by means of maturity assessment and standardisation.* To guide our research project, we pose our main research question as *"How can we integrate cybersecurity maturity assessment and cybersecurity standardisation to provide tailored support for organisations in their cybersecurity improvement efforts?".* To answer this main research question, we employ the Design Science Research approach and investigate our problem space by identifying the stakeholders' needs, goals, and requirements using several research methodologies and propose design artifacts to solve the identified problems.

The dissertation is organized into three parts: adaptivity in cybersecurity maturity assessments, cybersecurity standardisation, and the integration of cybersecurity maturity assessments and standardisation.

The first part is titled "Adaptivity in cybersecurity maturity assessments". Chapter 2 investigates the adaptivity of an existing maturity assessment model to organisational contexts. The artifact proposed in this research provides organisations with a method to adapt an existing information security maturity model to their organisational characteristics. Chapter 3 presents an assessment instrument that is adaptable by design through the posed situational questions. The questionnaire model proposed as an artifact helps organisations tailor the assessment instrument interactively by the given answers to the situational questions. Finally, in the first part, Chapter 4 investigates how organisational context affects the design of information security maturity assessment models using design principles and the proposed design requirements can be used for designing maturity assessment models. Enterprises can also use the design requirements to understand what to look for when selecting an assessment model for use within their organisation.

The second part is titled, "Cybersecurity standardisation". Chapter 5 focuses on cybersecurity standardisation and identifies gaps resulting from an international workshop organised with relevant stakeholders. We propose a reseach agenda to fill the identified gaps. Following this research, in Chapter 6, we present the cybersecurity essesntials through five standards and frameworks and a step-by-step process for SMEs to help them establish and improve their cybersecurity based on standards and frameworks.

The third part is titled “Integrating cybersecurity maturity assessments and standardisation”. Chapter 7 investigates how to integrate security assessment and standardiation to meet stakeholder requirements and proposes the adaptable security maturity assessment and standardisation (ASMAS) framework. We demonstrate the ASMAS framework through a user-friendly, web-based software prototype. We conduct seven evaluation interviews with six SMEs from five countries. We used the evaluation constructs based on the Technology Acceptance Model to explain and predict the utility of the ASMAS framework. The evaluation consructs using a Likert scale (1-5), on average, score 4.29 for perceived usefulness, 4.14 for perceived ease of use, and 3.62 for intention to use evaluation constructs. These outcomes reinforce this thesis’ holistic approach to facilitate and consolidate SMEs' independent security assessment and security standardisation efforts in daily practice.

Samenvatting

De eisen van organisaties op het gebied van cyberbeveiliging hebben verschillende beweegredenen, waaronder de noodzaak om hun activiteiten te beschermen tegen cyberaanvallen, te voldoen aan wet- en regelgeving, en vertrouwen op te bouwen. Cyberdreigingen en nieuwe regelgeving ontstaan, alsook de behoefte om passende maatregelen te implementeren en naleving te waarborgen. Met behulp van volwassenheidsbeoordelingen en standaardisering van cyberbeveiliging kunnen maatregelen worden geïmplementeerd en kan zekerheid worden geboden aan regelgevers. Dit proefschrift onderzoekt daarom volwassenheidsbeoordelingen en standaardisering als mogelijke instrumenten om de cyberbeveiliging van organisaties te verbeteren. Wij formuleren onze onderzoeksdoelstelling als het ondersteunen van de verbetering van de cyberbeveiliging van organisaties door middel van volwassenheidsbeoordelingen en standaardisering. Om richting te geven aan dit onderzoeksproject, stellen we onze overkoepelende onderzoeksvraag als volgt: *"Hoe kunnen we het beoordelen van de mate van volwassenheid inzake cyberbeveiliging en de standaardisering van cyberbeveiliging integreren om organisaties op maat te ondersteunen bij hun inspanningen om hun cyberbeveiliging te verbeteren?"*. Om deze hoofdvraag te beantwoorden, gebruiken we de *Design Science Research*-aanpak en onderzoeken we onze probleemruimte door de behoeften, doelen en vereisten van de belanghebbenden te identificeren met behulp van verschillende onderzoeksmethodologieën en stellen we ontwerpartefacten voor om de geïdentificeerde problemen op te lossen.

Dit proefschrift bestaat uit drie delen: adaptiviteit in volwassenheidsbeoordelingen inzake cyberbeveiliging, standaardisering van cyberbeveiliging, en de integratie van volwassenheidsbeoordelingen en standaardisering op het gebied van cyberbeveiliging.

Het eerste deel is getiteld *"Adaptiviteit in volwassenheidsbeoordelingen inzake cyberbeveiliging"*. Hoofdstuk 2 onderzoekt de adaptiviteit van een reeds bestaand model voor volwassenheidsbeoordelingen in organisatorische contexten. Het in dit onderzoek voorgestelde artefact biedt organisaties een methode om een bestaand volwassenheidsmodel voor informatiebeveiliging aan te passen aan hun specifieke profiel van organisatorische kenmerken. Hoofdstuk 3 presenteert een beoordelingsinstrument dat inherent adaptief van aard is via de gestelde situationele vragen. Het vragenlijstmodel dat als artefact wordt voorgesteld, helpt organisaties het beoordelingsinstrument interactief aan te passen middels de gegeven antwoorden op de situationele vragen. Tenslotte wordt in hoofdstuk 4 onderzocht hoe de organisatorische context van invloed is op het ontwerp van beoordelingsmodellen voor de volwassenheid van informatiebeveiliging met behulp van ontwerpprincipes. De voorgestelde ontwerpeisen kunnen tevens worden gebruikt voor het ontwerpen van modellen voor volwassenheidsbeoordelingen in andere toepassingsdomeinen. Organisaties kunnen de ontwerpeisen ook gebruiken om te begrijpen waar zij op moeten letten bij het selecteren van een toepasselijk beoordelingsmodel voor gebruik binnen hun organisatie.

Het tweede deel is getiteld *"Standaardisering van cyberbeveiliging"*. Hoofdstuk 5 onderzoekt de standaardisering op het gebied van cyberbeveiliging en rapporteert over de nog ontbrekende kennis zoals geïdentificeerd tijdens een internationale workshop die wij

organiseerden met alle belanghebbenden. Wij stellen aansluitend een onderzoeksagenda voor om de nog ontbrekende kennis te adresseren. Naar aanleiding van dit onderzoek presenteren we in hoofdstuk 6 de essentiële basiskennis inzake cyberbeveiliging aan de hand van vijf breed gedragen standaarden en kaders, alsook een stapsgewijs proces voor het MKB om hen te helpen hun cyberbeveiliging tot stand te brengen en te verbeteren op basis van reeds beproefde standaarden en kaders.

Het derde deel is getiteld *"Integratie van volwassenheidsbeoordelingen en standaardisering op het gebied van cyberbeveiliging"*. In hoofdstuk 7 wordt onderzocht hoe beveiligingsbeoordelingen en standaardisering kunnen worden geïntegreerd om aan de eisen van alle belanghebbenden te voldoen. Wij stellen het adaptieve ASMAS-raamwerk (*Adaptable Security Maturity Assessment and Standardisation*) voor. We demonstreren het ASMAS-raamwerk aan de hand van een gebruiksvriendelijk, webgebaseerd softwareprototype. Wij hebben zeven evaluatie-interviews gehouden met zes kleine en middelgrote ondernemingen uit vijf landen. We gebruikten de evaluatieconstructen gebaseerd op het *Technology Acceptance Model* om het bruikbaarheid van het ASMAS raamwerk te helpen verklaren en te voorspellen. De evaluatieconstructen, gebruikmakend van een *Likert* schaal (1-5), scoren gemiddeld 4,29 voor waargenomen bruikbaarheid, 4,14 voor waargenomen gebruiksgemak, en 3,62 voor intentie tot gebruik. Deze uitkomsten versterken de holistische benadering van dit proefschrift om onafhankelijke beoordelingen inzake cyberbeveiliging en beveiligingsstandaardisering binnen het MKB in de dagelijkse praktijk te vereenvoudigen en te consolideren.

Curriculum Vitae

Bilge Yigit Ozkan was born on July 30, 1974 in Merzifon, Turkey. She completed her bachelor's degree in Computer Science and Engineering at the Ege University in 1996. She started working in the industry, and completed her master's degree in Engineering Management at the Middle East Technical University in 2010. Before joining the Information and Computing Sciences department at Utrecht University in 2017, she worked in the industry for 20 years in several positions ranging from software engineer, IT systems administrator to information security risk and process manager and IT internal auditor in large enterprises. She worked in the aerospace industry in the information security domain for most of her carrier as a practitioner and auditor. After, she has been pursuing a Ph.D. in cybersecurity maturity assessment and standardisation with the financial support of an EU Horizon 2020 project (SMESEC).

As a researcher, she has presented her work at international conferences and assisted in the information security Bachelor course for three years. She also coordinated the student research Colloquium Business Informatics during the same period.

Since October 2021, Bilge has continued her career in the Dutch finance industry as an IT Security Risk and Compliance Officer at an international finance company.

SIKS Dissertation Series

2016 01 Syed Saiden Abbas (RUN), Recognition of Shapes by Humans and Machines
02 Michiel Christiaan Meulendijk (UU), Optimizing medication reviews through decision support: prescribing a better pill to swallow
03 Maya Sappelli (RUN), Knowledge Work in Context: User Centered Knowledge Worker Support
04 Laurens Rietveld (VU), Publishing and Consuming Linked Data
05 Evgeny Sherkhonov (UVA), Expanded Acyclic Queries: Containment and an Application in Explaining Missing Answers
06 Michel Wilson (TUD), Robust scheduling in an uncertain environment
07 Jeroen de Man (VU), Measuring and modeling negative emotions for virtual training
08 Matje van de Camp (TiU), A Link to the Past: Constructing Historical Social Networks from Unstructured Data
09 Archana Nottamkandath (VU), Trusting Crowdsourced Information on Cultural Artefacts
10 George Karafotias (VUA), Parameter Control for Evolutionary Algorithms
11 Anne Schuth (UVA), Search Engines that Learn from Their Users
12 Max Knobbout (UU), Logics for Modelling and Verifying Normative Multi-Agent Systems
13 Nana Baah Gyan (VU), The Web, Speech Technologies and Rural Development in West Africa - An ICT4D Approach
14 Ravi Khadka (UU), Revisiting Legacy Software System Modernization
15 Steffen Michels (RUN), Hybrid Probabilistic Logics - Theoretical Aspects, Algorithms and Experiments
16 Guangliang Li (UVA), Socially Intelligent Autonomous Agents that Learn from Human Reward
17 Berend Weel (VU), Towards Embodied Evolution of Robot Organisms
18 Albert Meroño Peñuela (VU), Refining Statistical Data on the Web
19 Julia Efremova (Tu/e), Mining Social Structures from Genealogical Data
20 Daan Odijk (UVA), Context & Semantics in News & Web Search
21 Alejandro Moreno Célleri (UT), From Traditional to Interactive Playspaces: Automatic Analysis of Player Behavior in the Interactive Tag Playground
22 Grace Lewis (VU), Software Architecture Strategies for Cyber-Foraging Systems
23 Fei Cai (UVA), Query Auto Completion in Information Retrieval
24 Brend Wanders (UT), Repurposing and Probabilistic Integration of Data; An Iterative and data model independent approach
25 Julia Kiseleva (TU/e), Using Contextual Information to Understand Searching and Browsing Behavior
26 Dilhan Thilakarathne (VU), In or Out of Control: Exploring Computational Models to Study the Role of Human Awareness and Control in Behavioural Choices, with Applications in Aviation and Energy Management Domains
27 Wen Li (TUD), Understanding Geo-spatial Information on Social Media
28 Mingxin Zhang (TUD), Large-scale Agent-based Social Simulation - A study on epidemic prediction and control
29 Nicolas Höning (TUD), Peak reduction in decentralised electricity systems - Markets and prices for flexible planning
30 Ruud Mattheij (UvT), The Eyes Have It
31 Mohammad Khelghati (UT), Deep web content monitoring
32 Eelco Vriezekolk (UT), Assessing Telecommunication Service Availability Risks for Crisis Organisations
33 Peter Bloem (UVA), Single Sample Statistics, exercises in learning from just one example
34 Dennis Schunselaar (TUE), Configurable Process Trees: Elicitation, Analysis, and Enactment
35 Zhaochun Ren (UVA), Monitoring Social Media: Summarization, Classification and Recommendation
36 Daphne Karreman (UT), Beyond R2D2: The design of nonverbal interaction behavior optimized for robot-specific morphologies
37 Giovanni Sileno (UvA), Aligning Law and Action - a conceptual and computational inquiry
38 Andrea Minuto (UT), Materials that Matter - Smart Materials meet Art & Interaction Design
39 Merijn Bruijnes (UT), Believable Suspect Agents; Response and Interpersonal Style Selection for an Artificial Suspect
40 Christian Detweiler (TUD), Accounting for Values in Design
41 Thomas King (TUD), Governing Governance: A Formal Framework for Analysing Institutional Design and Enactment Governance
42 Spyros Martzoukos (UVA), Combinatorial and Compositional Aspects of Bilingual Aligned Corpora
43 Saskia Koldijk (RUN), Context-Aware Support for Stress Self-Management: From Theory to Practice

44 Thibault Sellam (UVA), Automatic Assistants for Database Exploration
45 Bram van de Laar (UT), Experiencing Brain-Computer Interface Control
46 Jorge Gallego Perez (UT), Robots to Make you Happy
47 Christina Weber (UL), Real-time foresight - Preparedness for dynamic innovation networks
48 Tanja Buttler (TUD), Collecting Lessons Learned
49 Gleb Polevoy (TUD), Participation and Interaction in Projects. A Game-Theoretic Analysis
50 Yan Wang (UVT), The Bridge of Dreams: Towards a Method for Operational Performance Alignment in IT-enabled Service Supply Chains

---

2017 01 Jan-Jaap Oerlemans (UL), Investigating Cybercrime
02 Sjoerd Timmer (UU), Designing and Understanding Forensic Bayesian Networks using Argumentation
03 Daniël Harold Telgen (UU), Grid Manufacturing; A Cyber-Physical Approach with Autonomous Products and Reconfigurable Manufacturing Machines
04 Mrunal Gawade (CWI), Multi-core Parallelism in a Column-store
05 Mahdieh Shadi (UVA), Collaboration Behavior
06 Damir Vandic (EUR), Intelligent Information Systems for Web Product Search
07 Roel Bertens (UU), Insight in Information: from Abstract to Anomaly
08 Rob Konijn (VU) , Detecting Interesting Differences:Data Mining in Health Insurance Data using Outlier Detection and Subgroup Discovery
09 Dong Nguyen (UT), Text as Social and Cultural Data: A Computational Perspective on Variation in Text
10 Robby van Delden (UT), (Steering) Interactive Play Behavior
11 Florian Kunneman (RUN), Modelling patterns of time and emotion in Twitter #anticipointment
12 Sander Leemans (TUE), Robust Process Mining with Guarantees
13 Gijs Huisman (UT), Social Touch Technology - Extending the reach of social touch through haptic technology
14 Shoshannah Tekofsky (UvT), You Are Who You Play You Are: Modelling Player Traits from Video Game Behavior
15 Peter Berck (RUN), Memory-Based Text Correction
16 Aleksandr Chuklin (UVA), Understanding and Modeling Users of Modern Search Engines
17 Daniel Dimov (UL), Crowdsourced Online Dispute Resolution
18 Ridho Reinanda (UVA), Entity Associations for Search
19 Jeroen Vuurens (UT), Proximity of Terms, Texts and Semantic Vectors in Information Retrieval
20 Mohammadbashir Sedighi (TUD), Fostering Engagement in Knowledge Sharing: The Role of Perceived Benefits, Costs and Visibility
21 Jeroen Linssen (UT), Meta Matters in Interactive Storytelling and Serious Gaming (A Play on Worlds)
22 Sara Magliacane (VU), Logics for causal inference under uncertainty
23 David Graus (UVA), Entities of Interest — Discovery in Digital Traces
24 Chang Wang (TUD), Use of Affordances for Efficient Robot Learning
25 Veruska Zamborlini (VU), Knowledge Representation for Clinical Guidelines, with applications to Multimorbidity Analysis and Literature Search
26 Merel Jung (UT), Socially intelligent robots that understand and respond to human touch
27 Michiel Joosse (UT), Investigating Positioning and Gaze Behaviors of Social Robots: People's Preferences, Perceptions and Behaviors
28 John Klein (VU), Architecture Practices for Complex Contexts
29 Adel Alhuraibi (UvT), From IT-BusinessStrategic Alignment to Performance: A Moderated Mediation Model of Social Innovation, and Enterprise Governance of IT"
30 Wilma Latuny (UvT), The Power of Facial Expressions
31 Ben Ruijl (UL), Advances in computational methods for QFT calculations
32 Thaer Samar (RUN), Access to and Retrievability of Content in Web Archives
33 Brigit van Loggem (OU), Towards a Design Rationale for Software Documentation: A Model of Computer-Mediated Activity
34 Maren Scheffel (OU), The Evaluation Framework for Learning Analytics
35 Martine de Vos (VU), Interpreting natural science spreadsheets
36 Yuanhao Guo (UL), Shape Analysis for Phenotype Characterisation from High-throughput Imaging
37 Alejandro Montes Garcia (TUE), WiBAF: A Within Browser Adaptation Framework that Enables Control over Privacy
38 Alex Kayal (TUD), Normative Social Applications
39 Sara Ahmadi (RUN), Exploiting properties of the human auditory system and compressive sensing methods to increase noise robustness in ASR
40 Altaf Hussain Abro (VUA), Steer your Mind: Computational Exploration of Human Control in Relation to Emotions, Desires and Social Support For applications in human-aware support systems
41 Adnan Manzoor (VUA), Minding a Healthy Lifestyle: An Exploration of Mental Processes and a Smart Environment to Provide Support for a Healthy Lifestyle
42 Elena Sokolova (RUN), Causal discovery from mixed and missing data with applications on ADHD datasets
43 Maaike de Boer (RUN), Semantic Mapping in Video Retrieval
44 Garm Lucassen (UU), Understanding User Stories - Computational Linguistics in Agile Requirements Engineering
45 Bas Testerink (UU), Decentralized Runtime Norm Enforcement
46 Jan Schneider (OU), Sensor-based Learning Support
47 Jie Yang (TUD), Crowd Knowledge Creation Acceleration
48 Angel Suarez (OU), Collaborative inquiry-based learning

2018 01 Han van der Aa (VUA), Comparing and Aligning Process Representations
02 Felix Mannhardt (TUE), Multi-perspective Process Mining

03 Steven Bosems (UT), Causal Models For Well-Being: Knowledge Modeling, Model-Driven Development of Context-Aware Applications, and Behavior Prediction
04 Jordan Janeiro (TUD), Flexible Coordination Support for Diagnosis Teams in Data-Centric Engineering Tasks
05 Hugo Huurdeman (UVA), Supporting the Complex Dynamics of the Information Seeking Process
06 Dan Ionita (UT), Model-Driven Information Security Risk Assessment of Socio-Technical Systems 07 Jieting Luo (UU), A formal account of opportunism in multi-agent systems
08 Rick Smetsers (RUN), Advances in Model Learning for Software Systems 09 Xu Xie (TUD), Data Assimilation in Discrete Event Simulations
10 Julienka Mollee (VUA), Moving forward: supporting physical activity behavior change through intelligent technology
11 Mahdi Sargolzaei (UVA), Enabling Framework for Service-oriented Collaborative Networks
12 Xixi Lu (TUE), Using behavioral context in process mining
13 Seyed Amin Tabatabaei (VUA), Computing a Sustainable Future
14 Bart Joosten (UVT), Detecting Social Signals with Spatiotemporal Gabor Filters
15 Naser Davarzani (UM), Biomarker discovery in heart failure
16 Jaebok Kim (UT), Automatic recognition of engagement and emotion in a group of children
17 Jianpeng Zhang (TUE), On Graph Sample Clustering
18 Henriette Nakad (UL), De Notaris en Private Rechtspraak
19 Minh Duc Pham (VUA), Emergent relational schemas for RDF
20 Manxia Liu (RUN), Time and Bayesian Networks
21 Aad Slootmaker (OUN), EMERGO: a generic platform for authoring and playing scenario-based serious games
22 Eric Fernandes de Mello Araujo (VUA), Contagious: Modeling the Spread of Behaviours, Perceptions and Emotions in Social Networks
23 Kim Schouten (EUR), Semantics-driven Aspect-Based Sentiment Analysis
24 Jered Vroon (UT), Responsive Social Positioning Behaviour for Semi-Autonomous Telepresence Robots
25 Riste Gligorov (VUA), Serious Games in Audio-Visual Collections
26 Roelof Anne Jelle de Vries (UT),Theory-Based and Tailor-Made: Motivational Messages for Behavior Change Technology
27 Maikel Leemans (TUE), Hierarchical Process Mining for Scalable Software Analysis
28 Christian Willemse (UT), Social Touch Technologies: How they feel and how they make you feel
29 Yu Gu (UVT), Emotion Recognition from Mandarin Speech
30 Wouter Beek, The "K" in "semantic web" stands for "knowledge": scaling semantics to the web

---

2019 01 Rob van Eijk (UL),Web privacy measurement in real-time bidding systems. A graph-based approach to RTB system classification
02 Emmanuelle Beauxis Aussalet (CWI, UU), Statistics and Visualizations for Assessing Class Size Uncertainty
03 Eduardo Gonzalez Lopez de Murillas (TUE), Process Mining on Databases: Extracting Event Data from Real Life Data Sources
04 Ridho Rahmadi (RUN), Finding stable causal structures from clinical data
05 Sebastiaan van Zelst (TUE), Process Mining with Streaming Data
06 Chris Dijkshoorn (VU), Nichesourcing for Improving Access to Linked Cultural Heritage Datasets
07 Soude Fazeli (TUD), Recommender Systems in Social Learning Platforms
08 Frits de Nijs (TUD), Resource-constrained Multi-agent Markov Decision Processes
09 Fahimeh Alizadeh Moghaddam (UVA), Self-adaptation for energy efficiency in software systems
10 Qing Chuan Ye (EUR), Multi-objective Optimization Methods for Allocation and Prediction
11 Yue Zhao (TUD), Learning Analytics Technology to Understand Learner Behavioral Engagement in MOOCs
12 Jacqueline Heinerman (VU), Better Together
13 Guanliang Chen (TUD), MOOC Analytics: Learner Modeling and Content Generation
14 Daniel Davis (TUD), Large-Scale Learning Analytics: Modeling Learner Behavior & Improving Learning Outcomes in Massive Open Online Courses
15 Erwin Walraven (TUD), Planning under Uncertainty in Constrained and Partially Observable Environments
16 Guangming Li (TUE), Process Mining based on Object-Centric Behavioral Constraint (OCBC) Models
17 Ali Hurriyetoglu (RUN),Extracting actionable information from microtexts
18 Gerard Wagenaar (UU), Artefacts in Agile Team Communication
19 Vincent Koeman (TUD), Tools for Developing Cognitive Agents
20 Chide Groenouwe (UU), Fostering technically augmented human collective intelligence
21 Cong Liu (TUE), Software Data Analytics: Architectural Model Discovery and Design Pattern Detection
22 Martin van den Berg (VU),Improving IT Decisions with Enterprise Architecture
23 Qin Liu (TUD), Intelligent Control Systems: Learning, Interpreting, Verification
24 Anca Dumitrache (VU), Truth in Disagreement - Crowdsourcing Labeled Data for Natural Language Processing
25 Emiel van Miltenburg (VU), Pragmatic factors in (automatic) image description
26 Prince Singh (UT), An Integration Platform for Synchromodal Transport
27 Alessandra Antonaci (OUN), The Gamification Design Process applied to (Massive) Open Online Courses
28 Esther Kuindersma (UL), Cleared for take-off: Game-based learning to prepare airline pilots for critical situations
29 Daniel Formolo (VU), Using virtual agents for simulation and training of social skills in safety-critical circumstances
30 Vahid Yazdanpanah (UT), Multiagent Industrial Symbiosis Systems
31 Milan Jelisavcic (VU), Alive and Kicking: Baby Steps in Robotics
32 Chiara Sironi (UM), Monte-Carlo Tree Search for Artificial General Intelligence in Games
33 Anil Yaman (TUE), Evolution of Biologically Inspired Learning in Artificial Neural Networks

34 Negar Ahmadi (TUE), EEG Microstate and Functional Brain Network Features for Classification of Epilepsy and PNES
35 Lisa Facey-Shaw (OUN), Gamification with digital badges in learning programming
36 Kevin Ackermans (OUN), Designing Video-Enhanced Rubrics to Master Complex Skills
37 Jian Fang (TUD), Database Acceleration on FPGAs
38 Akos Kadar (OUN), Learning visually grounded and multilingual representations

---

2020 01 Armon Toubman (UL), Calculated Moves: Generating Air Combat Behaviour
02 Marcos de Paula Bueno (UL), Unraveling Temporal Processes using Probabilistic Graphical Models 03 Mostafa Deghani (UvA), Learning with Imperfect Supervision for Language Understanding
04 Maarten van Gompel (RUN), Context as Linguistic Bridges 05 Yulong Pei (TUE), On local and global structure mining
06 Preethu Rose Anish (UT), Stimulation Architectural Thinking during Requirements Elicitation - An Approach and Tool Support
07 Wim van der Vegt (OUN), Towards a software architecture for reusable game components
08 Ali Mirsoleimani (UL),Structured Parallel Programming for Monte Carlo Tree Search
09 Myriam Traub (UU), Measuring Tool Bias and Improving Data Quality for Digital Humanities Research
10 Alifah Syamsiyah (TUE), In-database Preprocessing for Process Mining
11 Sepideh Mesbah (TUD), Semantic-Enhanced Training Data AugmentationMethods for Long-Tail Entity Recognition Models
12 Ward van Breda (VU), Predictive Modeling in E-Mental Health: Exploring Applicability in Personalised Depression Treatment
13 Marco Virgolin (CWI), Design and Application of Gene-pool Optimal Mixing Evolutionary Algorithms for Genetic Programming
14 Mark Raasveldt (CWI/UL), Integrating Analytics with Relational Databases
15 Konstantinos Georgiadis (OUN), Smart CAT: Machine Learning for Configurable Assessments in Serious Games
16 Ilona Wilmont (RUN), Cognitive Aspects of Conceptual Modelling
17 Daniele Di Mitri (OUN), The Multimodal Tutor: Adaptive Feedback from Multimodal Experiences
18 Georgios Methenitis (TUD), Agent Interactions & Mechanisms in Markets with Uncertainties: Electricity Markets in Renewable Energy Systems
19 Guido van Capelleveen (UT), Industrial Symbiosis Recommender Systems
20 Albert Hankel (VU), Embedding Green ICT Maturity in Organisations
21 Karine da Silva Miras de Araujo (VU), Where is the robot?: Life as it could be
22 Maryam Masoud Khamis (RUN), Understanding complex systems implementation through a modeling approach: the case of e-government in Zanzibar
23 Rianne Conijn (UT), The Keys to Writing: A writing analytics approach to studying writing processes using keystroke logging
24 Lenin da Nobrega Medeiros (VUA/RUN), How are you feeling, human? Towards emotionally supportive chatbots
25 Xin Du (TUE), The Uncertainty in Exceptional Model Mining
26 Krzysztof Leszek Sadowski (UU), GAMBIT: Genetic Algorithm for Model-Based mixed-Integer opTimization
27 Ekaterina Muravyeva (TUD), Personal data and informed consent in an educational context
28 Bibeg Limbu (TUD), Multimodal interaction for deliberate practice: Training complex skills with augmented reality
29 Ioan Gabriel Bucur (RUN), Being Bayesian about Causal Inference
30 Bob Zadok Blok (UL), Creatief, Creatieve, Creatiefst
31 Gongjin Lan (VU), Learning better – From Baby to Better
32 Jason Rhuggenaath (TUE), Revenue management in online markets: pricing and online advertising
33 Rick Gilsing (TUE), Supporting service-dominant business model evaluation in the context of business model innovation
34 Anna Bon (MU), Intervention or Collaboration? Redesigning Information and Communication Technologiesfor Development
35 Siamak Farshidi (UU), Multi-Criteria Decision-Making in Software Production

---

2021 01 Francisco Xavier Dos Santos Fonseca (TUD),Location-based Games for Social Interaction in Public Space
02 Rijk Mercuur (TUD), Simulating Human Routines:Integrating Social Practice Theory in Agent-Based Models 03 Seyyed Hadi Hashemi (UVA), Modeling Users Interacting with Smart Devices
04 Ioana Jivet (OU), The Dashboard That Loved Me: Designing adaptive learning analytics for self-regulated learning
05 Davide Dell'Anna (UU), Data-Driven Supervision of Autonomous Systems
06 Daniel Davison (UT), "Hey robot, what do you think?" How children learn with a social robot
07 Armel Lefebvre (UU), Research data management for open science
08 Nardie Fanchamps (OU), The Influence of Sense-Reason-Act Programming on Computational Thinking
09 Cristina Zaga (UT), The Design of Robothings. Non-Anthropomorphic and Non-Verbal Robots to Promote Children's Collaboration Through Play
10 Quinten Meertens (UvA), Misclassification Bias in Statistical Learning
11 Anne van Rossum (UL), Nonparametric Bayesian Methods in Robotic Vision
12 Lei Pi (UL), External Knowledge Absorption in Chinese SMEs
13 Bob R. Schadenberg (UT), Robots for Autistic Children: Understanding and Facilitating Predictability for Engagement in Learning
14 Negin Samaeemofrad (UL), Business Incubators: The Impact of Their Support
15 Onat Ege Adali (TU/e), Transformation of Value Propositions into Resource Re-Configurations through the

Business Services Paradigm
16 Esam A. H. Ghaleb (UM), BIMODAL EMOTION RECOGNITION FROM AUDIO-VISUAL CUES
17 Dario Dotti (UM), Human Behavior Understanding from motion and bodily cues using deep neural networks
18 Remi Wieten (UU), Bridging the Gap Between Informal Sense-Making Tools and Formal Systems - Facilitating the Construction of Bayesian Networks and Argumentation Frameworks
19 Roberto Verdecchia (VU), Architectural Technical Debt: Identification and Management
20 Masoud Mansoury (TU/e), Understanding and Mitigating Multi-Sided Exposure Bias in Recommender Systems
21 Pedro Thiago Timbó Holanda (CWI), Progressive Indexes
22 Sihang Qiu (TUD), Conversational Crowdsourcing
23 Hugo Manuel Proença (LIACS), Robust rules for prediction and description
24 Kaijie Zhu (TUE), On Efficient Temporal Subgraph Query Processing
25 Eoin Martino Grua (VUA), The Future of E-Health is Mobile: Combining AI and Self-Adaptation to Create Adaptive E-Health Mobile Applications
26 Benno Kruit (CWI & VUA), Reading the Grid: Extending Knowledge Bases from Human-readable Tables
27 Jelte van Waterschoot (UT), Personalized and Personal Conversations: Designing Agents Who Want to Connect With You
28 Christoph Selig (UL), Understanding the Heterogeneity of Corporate Entrepreneurship Programs

2022 1 Judith van Stegeren (UT), Flavor text generation for role-playing video games
2 Paulo da Costa (TU/e), Data-driven Prognostics and Logistics Optimisation: A Deep Learning Journey
3 Ali el Hassouni (VUA), A Model A Day Keeps The Doctor Away: Reinforcement Learning For Personalized Healthcare
4 Ünal Aksu (UU), A Cross-Organizational Process Mining Framework
5 Shiwei Liu (TU/e), Sparse Neural Network Training with In-Time Over-Parameterization
6 Reza Refaei Afshar (TU/e), Machine Learning for Ad Publishers in Real Time Bidding
7 Sambit Praharaj (OU), Measuring the Unmeasurable? Towards Automatic Co-located Collaboration Analytics
8 Maikel L. van Eck (TU/e), Process Mining for Smart Product Design
9 Oana Andreea Inel (VUA), Understanding Events: A Diversity-driven Human-Machine Approach
10 Felipe Moraes Gomes (TUD), Examining the Effectiveness of Collaborative Search Engines
11 Mirjam de Haas (UT), Staying engaged in child-robot interaction, a quantitative approach to studying preschoolers' engagement with robots and tasks during second-language tutoring
12 Guanyi Chen (UU), Computational Generation of Chinese Noun Phrases
13 Xander Wilcke (VUA), Machine Learning on Multimodal Knowledge Graphs: Opportunities, Challenges, and Methods for Learning on Real-World Heterogeneous and Spatially-Oriented Knowledge
14 Michiel Overeem (UU), Evolution of Low-Code Platforms
15 Jelmer Jan Koorn (UU), Work in Process: Unearthing Meaning using Process Mining
16 Pieter Gijsbers (TU/e), Systems for AutoML Research
17 Laura van der Lubbe (VUA), Empowering vulnerable people with serious games and gamification
18 Paris Mavromoustakos Blom (TiU), Player Affect Modelling and Video Game Personalisation

Organisations' cybersecurity requirements have several origins, including the need to protect their business from cyberattacks, comply with laws and regulations, and build trust. Cyber threats and new regulations emerge, thus the need to implement measures and assure compliance. Cybersecurity maturity assessments and cybersecurity standardisation can be used to implement measures for cyber threats and provide assurance for regulators. This dissertation investigates cybersecurity maturity assessment and standardisation to improve organisations' cybersecurity in three parts: adaptivity in cybersecurity maturity assessments, cybersecurity standardisation, and the integration of cybersecurity maturity assessments and standardisation. Adaptivity in cybersecurity maturity assessments enables tailored approaches to address the specific needs of different organisational profiles. Cybersecurity standardisation is about implementing and adopting standards. The integration of cybersecurity maturity assessments and standardisation is accomplished by driving assessment questions based on standards. This dissertation incorporates the adaptivity concept in integrating cybersecurity maturity assessments and standardisation, thus enabling tailored cybersecurity for organisations.

Utrecht University

ISBN: 978-94-6423-887-7