Antwerp Management School

A CYBERSECURITY STANDARD FOR SME

VINCENT VAN DIJK (STUDENT)

Promotors: Barry Derksen & Yuri Bobbert

Academic year: 2020-2022

Degree: Master of Science

Orientation: Executive Master in IT Risk & Cyber Security Management

Table of Contents

Preface	
Introduction	5
Management summary	7
Problem	8
SME Challenges	8
Cybersecurity risk	9
Risk Management	
Cybersecurity standards	
Standards from other sectors	
Accounting	
Food industry	
Potential implication to cybersecurity standard	
Proposed solutions	12
Problem statement	
Research question	14
Definitions	
The definition of an SME	
Cybersecurity risk	
Cybersecurity standard	
Artifact	
Holistic	
Research design	
Research paradigm	
Research methodology	
Question/hypothesis-based research	
Design science research	
Action research	22
System thinking	
Soft Design Methodology	
Selection	
Adaptions to SDM	
Research methods	28
Literature	29
Group Support Sytem (GSS)	
Design	
Analysis	
The experience of the participant	
Hurdles that hinder the adoption of standards	

NIST Cybersecurity Framework (NIST CSF)	37
Risk management process	
Effective components	
Artifact design	41
The 7 steps of SDM	42
Step 1 — The general problem	
Step 2 – The general problem expressed in the requirements	
Step 3 — Answering the research question	44
Step 4 — The specific requirements	46
Step 5 — Comparison between the general requirements and specific requirements	49
Step 6 — Declarative search for a specific solution	50
Step 7 — Construct the solution	51
1. The basic canvas	51
2. Examples	
3. Catalog of components	54
Findings	56
Cybersecurity standard	56
Soft Design Methodology (SDM)	57
NIST CSF	58
Conclusion	60
What hinders the adoption of a cybersecurity standard among SMEs?	
What are the components of an effective cybersecurity standard for SMEs?	
What are the components of a cybersecurity framework tailored toward an SME with	
adoption barrier that is effective in managing cybersecurity risks?	
The artifact	
Checklist	64
Limitations	65
Further research	65
Reflection	66
References	67
Appendix	
A. Version Control	
B. Questions for GSS	
Questions about the participant	
Risk Management process	
Obstacles for the adoption of standards	
Selection of categories	
Artifact	

Preface

Small & Medium size Businesses (SMBs) are the backbone of our society. It often starts with talented and passionate men and women known for their specific handcraft ship, skills, knowledge, and access to specific resources. Growth, globalization, and digitalization bring these organizations new, less specific, opportunities, challenges, and risks. Dealing with them, in the most effective and efficient way, becomes part of doing business and co-defines success or failure.

Zooming in on the Digital transformation, we can all see that it's changing the world. During the COVID-19 crisis it has even enabled many SMB's to sustain some income to survive. But with every technical revolution also come negative side-effects and risks for business and society. Not addressing them is not sustainable. Specific to Digital, cybersecurity & privacy incidents could lead to intellectual property theft, business continuity issues, reputation damage and unforeseen costs. Driven by regulations, or by the need to address risks and digital sustainability goals, organizations turn to experts and industry best practices. SMB's are specifically challenged to execute this in a cost effective way. Finding Cybersecurity experts is difficult and expensive. Using industry best practices for Cybersecurity that are generally designed for large enterprises might not be proportional for SMB's colliding with their strong pressure on costs.

The research of Vincent van Dijk looks for options to bring a cost-effective way of managing cybersecurity risks with industry best practices to SMB's. He investigates what can be learned from other best practices which have been simplified for SMB's while still serving the original goals.

I wish you an interesting read when joining the "journey" of Vincent to find a (short term) solution for SMB's to address this important challenge to keep our digital economy sustainable.

Drs Ad Krikke

Leadership Partner Security & Risk Management Gartner, author of the book "A sustainable Digital Economy"

Introduction

Small and medium-sized enterprises (SMEs) play an essential role in most economies worldwide (Ayyagari et al., 2007; Burgstaller & Wagner, 2015). They are regarded as the most active enterprises in the global economy and play a crucial role in improving human welfare in any nation. (Gama and Geraldes, 2012).

However, cyber risks are threating SMEs; sixty percent of small companies are out of business six months after a cyber-attack (The Denver Post, 2016). Due to SMEs' usually low equity ratio, they are relatively vulnerable to external events compared to larger enterprises (Altman et al., 2010). SMEs rely on cybersecurity professionals to protect their businesses from cyber threats. Cybersecurity professionals use information security standards (ex. ISO27001, NIST) to structure the complex world of cybersecurity. These standards are excellent at precisely doing that—offering structure to the complex cybersecurity world by exploring their defined structure. Cyber professionals must use these structures to design cybersecurity programs for their companies.

A 2021 study by McKinsey showed that 70% of the companies are still in an immature state (figure 1). I suspect that this number is even higher because McKinsey is known to serve highend clients. Immature or smaller organizations cannot manage cyber risks with those standards—especially SMBs. According to a report by PWC, only 27% of SMBs have a dedicated security team (PWC, 2021). Without having people devoted to cybersecurity, the current cybersecurity management standards cannot function. However, simply hiring security professionals is also not a solution. The world lacks 4 million cybersecurity professionals, a gap that is only growing (ISC2, 2019). There is a need for a more straightforward, easier-to-understand solution for cybersecurity management.

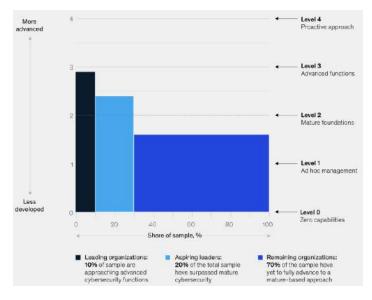


Figure 1, Cybersecurity maturity level, score (0 = low, 4 = high) (n = 114) (McKinsey & Company, 2021)

Literature has proposed three solutions for cybersecurity management for SMEs. (C. Ponsard, et al, 2020; M. Benz & D. Chatterjee 2020; S. Teufel, et al, 2020) However, no requirements had been researched beforehand. Each of the artifacts was created through the researchers' interpretation of cybersecurity standards. Further, the context and risks of the specific SMEs are not considered. One of the proposed solutions of the European Digital SME Alliance is to improve the cybersecurity state of SMEs by developing a new lightweight cybersecurity standard tailored toward SMEs. (2020)

This research researches and designs an artifact, a new cybersecurity standard tailored toward SMEs.

Management summary

Small and medium-sized enterprises (SMEs) play an essential role in most economies worldwide (Ayyagari et al., 2007; Burgstaller & Wagner, 2015). They are regarded as the most active enterprises in the global economy and play a crucial role in improving human welfare in any nation. (Gama and Geraldes, 2012). SMEs are more prone to be affected by specific cyberthreats and attacks than larger enterprises. (M. Antunes, 2021) Moreover, SMEs' usually low equity ratio makes them relatively vulnerable to external events compared to larger enterprises (Altman et al., 2010).

To reduce the effect of cyber risks, organizations need to align their cybersecurity maturity to their risk appetite. In literature, cybersecurity maturity is managed and measured through cybersecurity standards, such as the ISO27001 and the NIST Cybersecurity Framework (D. Proença & J. Borbinha, 2018). However, SMEs are unable effectivity adopt current standards because of the high implementation cost of standards, lack of resources, lack of technical solutions, lack of awareness, and more. (European Digital SME Alliance) The lack of resources for SMEs was the primary reason for the existence of the SME version of the ISRS. (D. Kaya, M. Koch, 2015) Nevertheless, it is unsure if that is also the case for cybersecurity standards.

"SMEs cannot adopt current cybersecurity standards effectively because of the lack of standards tailored toward SMEs. "

This research proses a cybersecurity standard tailored towards SMEs based on research conducted on the following primary question:

"What components of a cybersecurity standard are tailored toward an SME with a low adoption barrier that effectively manages cybersecurity risks?"

The research concludes that the lack of resources for SMEs and the implementation cost of standards are hurdles to SMEs adopting a cybersecurity standard. Furthermore, the research concludes on six essential components of a cybersecurity standard:

- Management approval of the risk management processes
- An organization-wide approach to risk management
- The organization has at least a limited understanding of the broader ecosystem
- Risk assessment
- Protective technology
- Identity management and access control

The primary conclusion of the thesis is that a cybersecurity management standard for SMEs must be flexible. The complexity and unpredictability of today's business climate necessitate increased adaptability for businesses to survive. Adaptability to environmental conditions is essential for SME survival; its development must be deliberate and supported by internal procedures. (Anning-Dorson, T, 2021). The result of the thesis suggests that a cybersecurity management standard for SMEs needs deliberate flexibility.

Problem

Small and medium-sized enterprises (SMEs) play an essential role in most economies worldwide (Ayyagari et al., 2007; Burgstaller & Wagner, 2015). They are regarded as the most active enterprises in the global economy and play a crucial role in improving human welfare in any nation. Recent evidence indicates that SMEs account for 90 percent of businesses and employ approximately 60 percent of the world's labor force (Munro, 2013). Around 99% of the economic activities in the European Union can be traced back to SMEs, which account for two-thirds of all jobs in the private sector (Gama & Geraldes, 2012).

The essential value of SMEs to the economy is their potential to utilize local resources such as local raw materials, the development of local savings, the provision of opportunities for self-employment, and the training of semi-skilled laborers through apprenticeships (Asare et al., 2015). Additionally, SMEs are significant for the job market; SMEs create the most jobs in any economy (S. Gamage, 2020)

SME Challenges

Compared to larger firms, SMEs have more straightforward internal organization and thus are more flexible and faster at responding and adapting to change (Lavia Lopez & Hiebl, 2014). At the same time, SMEs frequently face significant challenges. Compared to larger enterprises, SMEs profit less often from economies of scale, and fewer have access to a vast resource base (Burgstaller & Wagner, 2015; Lavia Lopez & Hiebl, 2014). Due to SMEs' usually low equity ratio, they are relatively vulnerable to external events compared to larger enterprises (Altman et al., 2010). Thus, not only larger enterprises face various risks but also SMEs, whose survival is threatened easily due to their smaller set of (both financial and non-financial) resources.

Based on research conducted in Malaysia, compiled a list of the most significant obstacles to innovation and technology adaptation, including an inadequate budget, a lack of resources, difficulties in expanding the existing capacity and improving the quality of products, a lack of research and development, low productivity because of inefficient technologies, and a lack of new knowledge utilization in the development of new products. (H. K. Mustafa & S. Yaakub, 2018) Due to the numerous obstacles associated with implementing innovations, SMEs should be cautious in planning and operations. (Sener et al. 2014).

Cybersecurity risk

The development of information and communication technology (ICT) is identified as one of the intensifying drivers for the internationalization and globalization of SMEs. As knowledge is an essential resource, and in the setting where resources and resource transfer are more important for the usability of resources, it is more important to transfer resources (Narteh, 2008).

Adoption of information technology (IT) is one of the areas recommended to small and medium-sized enterprises (SMEs) to confront competitive challenges (M. A. Nugroho et al., 2017). IT creates several advantages for the expansion of SME businesses. Adoption of webbased technology reduces operational costs, enhances customer service, accelerates producer-to-customer and producer-to-input-supplier interactions, improves market knowledge, and strengthens relationships with trading partners. (M. Quayle, & J. K, Christiansen, 2004; T. Tse & K. Soufani, 2003)

However, the rise of information technology also poses challenges. Verizon's Data Breach Investigation report stated 1,037 incidents that year, which is more than 819 incidents at large organizations. (Verizon, 2021). SMEs are prone to be more intensively affected by specific cyberthreats and attacks than larger enterprises. (M. Antunes, 2021) Cyberattacks, such as data breaches, data destruction, and data access denial, typically pose a threat to the assets of SMEs, which likely harm several business operations. Despite this, many indicators suggest that SMEs underestimate cyber threats by not implementing effective security measures. (K. Renaud & G. R. S Weir, 2016) Most experts have conceded that cybercrimes pose the greatest threat to businesses, although SMEs believe they are immune due to their size. (Y. Barlette, 2017)

Employees' current behavior in SMEs accounts for several cybersecurity issues: ignoring information policies, organizational norms, and firm rules. (Y. Barlette, 2017). Training and education are essential for enhancing knowledge, but in some instances, information alone cannot guarantee appropriate behavior (T. Gundu, 2019). The previous study revealed that after employee awareness campaigns and training courses, 85 percent of employees stated that their level of behavior was adequate, while the actual level of behavior was much lower at 54 percent (T. Gundu, 2019).

Risk Management

SMEs, like major corporations, face a variety of risks; nevertheless, their existence is more insecure at any one time due to their limited financial and nonfinancial resources. (A. Fielder et al., 2016). Ordinarily, business strategies demonstrate less attention to risk management implications, while several strategic moves, such as avoidance, control, and cooperation, could reduce uncertainties (K. D. Miller, 1992, as cited in A. Alahmari & B. Duncan, 2020). Underestimating the risks leads to unfortunate consequences, which usually affect tangible and intangible assets and, even worse, drive the business to bankruptcy (K. W. Hollman & S. Mohammad-Zadeh, 1984, as cited in A. Alahmari & B. Duncan, 2020).

Risk management may help SME managers to identify significant risks that could jeopardize the success or existence of the company in time to cope with them efficiently (Miller, 1992; Brustbauer, 2014). Misjudging or failing to recognize risks can, in the worst case, have disastrous consequences, ranging from customer loss to damaging liability, environmental damage, and possibly even bankruptcy (Hollman & Mohammad-Zadeh, 1984). However, many SMEs do not – or do not adequately – apply risk management practices, mainly because they cannot afford to rededicate resources due to their constraints (Marcelino-Sádaba et al., 2014).

Cybersecurity standards

To reduce the effect of cyber risks, organizations need to align their cybersecurity maturity to their risk appetite. In literature, cybersecurity maturity is managed and measured through cybersecurity standards, such as the ISO27001 and the NIST Cybersecurity Framework (D. Proença & J. Borbinha, 2018). In some countries, such as the Netherlands, an adapted version of the ISO27001 is used as a standard to enforce cybersecurity among government and healthcare organizations.

However, the available standards are scarce and usually focused on large companies that have a well-structured business process. (Javaid et al., 2017, as cited in M. Antunes, 2021) The Digital SME Alliance confirmed the views of Javaid et al. and stated that standards are not tailored to SMEs; as a result, SMEs have difficulty adopting standards. (Europian Digital SME Alliance, 2020) Furthermore, research shows that "organizational IT security research has largely neglected the SME context.". The research results imply that common assumptions such as the availability of a qualified workforce, documented processes, or IT budget planning must be modified in the security discussion for SMEs. (M. Heidt et al., 2019, as cited in S. Teufel et al, 2020)

Standards from other sectors

Companies need to comply with regulations and standards. The standards they need to comply with depend on the specifics of the organization: country, nature of their business, sector, and more. Different organizations recognized that alternative standards need to be developed for SMEs.

Accounting

In July 2009, the International Accounting Standards Board (IASB) issued the International Financial Reporting Standard for Small and Medium-sized Entities. IFRS for SMEs is an adaptation of the ISRS designed for SMEs because Market participants argued that full IFRS is too complicated and burdensome for non-publicly accountable entities and, thus, the benefits for these firms are offset by high transitional and implementation costs. (D. Kaya, M. Koch, 2015)

Food industry

Hazard analysis-based procedures have been required to reduce the number of food poisoning incidents in the United Kingdom (Great Britain, 1995; EU, 1993, as cited in L. M. Fielding, 2005). Hazard Analysis Critical Control Point (HACCP) presents obstacles to even the most prominent food firms with extensive financial, technical, and management capabilities; SMEs frequently feel that the difficulties of HACCP are possibly insurmountable (E. Taylor & K. Kane, 2005). However, research reveals that SMEs lack a fundamental understanding of the HACCP methodology. Taylor and Kane (2005).

Potential implication to cybersecurity standard

In the case of the IFRS, an adaptation tailored toward SMEs was required because of the high implementation cost. (D. Kaya, M. Koch, 2015) However, the standard did need to be tailored toward SMEs for the HACCP because only the main concern was the SME's basic understanding of the HACCP approach. (E. Taylor & K. Kane, 2005) From those two examples, one could put forward the notion that only in the case of a high cost of implementing a standard needs to be tailored because SMEs struggle with financial and non-financial resources. (H. K. Mustafa & S. Yaakub, 2018). The implementation cost of standards and lack of resources was two of the hurdles mentioned in the position paper of the European Digital SME Alliance (2020), which resulted in their call for a cybersecurity standard tailored toward SMEs.

Proposed solutions

Three solutions are proposed in the literature. The first solution is a certification scheme that has been developed by the University of Antwerp, which is in the pilot phase. Their solution is an extensive checklist on which government-selected auditors audit an SME. (C. Ponsard et al., 2020) Second, a maturity evaluation tool has been developed based on NIST CSF. The framework uses maturity to compare to the SME industry and suggest improvements. However, it lacks the link to the specific context and risks of the SME (M. Benz & D. Chatterjee 2020). Third, a canvas is proposed, which should be treated like a checklist of components on which an SME needs to comply. (S. Teufel et al., 2020)

Each of the solutions has been evaluated through surveys or case studies. However, no requirements had been researched beforehand. Each artifact was created through the interpretation of the researchers' on cybersecurity standards. Further, the context and risks of the specific SMEs are not considered. Lastly, each artifact assumed that a questionnaire or checklist was the correct form of the artifact.

Solution	Strengths	Criteria	Reference
Certification scheme based on a checklist	• Potential enforcement of governments to ensure SMEs compliance	 The solution composed of multiple complex standards, NIST, ISO27001 and the CIS Controls which is unnecessary complex The solution is compliance based and SMEs will likely threat it as a "check in the box" Risk management is part of the checkbox 	C. Ponsard, et al, 2020
Evaluation tool	 Includes industry averages Direct link toward the NIST CSF 	 The assessment tool neglects the link to the SME's risks 	M. Benz & D. Chatterjee 2020
Canvas	• Simplified overview of the components	 One-size-fit all approach Complex Lacks connection to risks 	S. Teufel, et al, 2020

Problem statement

Adoption of information technology (IT) is one of the areas recommended to small and medium-sized enterprises (SMEs) to confront competitive challenges (M. A. Nugroho et al., 2017). However, the rise of information technology also poses challenges.

SMEs are prone to be more intensively affected by some specific cyberthreats and attacks than larger enterprises. (M. Antunes, 2021) To reduce the effect of cyber risks, organizations must align their cybersecurity maturity with their risk appetite. Cybersecurity maturity is managed and measured through cybersecurity standards, such as the ISO27001 and the NIST Cybersecurity Framework (D. Proença & J. Borbinha, 2018) However, SMEs are unable effectivity adopt current standards because of the high implementation cost of standards, lack of resources, lack of technical solutions, lack of awareness and more. (European Digital SME Alliance) The lack of resources of SME was the primary reason of the existence of the SME version of the ISRS. (D. Kaya, M. Koch, 2015) Yet it is unsure of that is also the case for cybersecurity standards.

Exciting solutions originating from academic research lack the involvement of an SME's context and risks. Moreover, no study has been conducted into the required components of a standard.

For this research, the thesis uses the following problem statement:

"SMEs cannot adopt current cybersecurity standards effectively because of the lack of standards tailored toward SMEs. "

Research question

This thesis aims to construct an artifact that can be used as a cybersecurity standard tailored toward SMEs. The standard's artifact needs to manage cybersecurity risk effectively while keeping a low adoption barrier. A low adoption barrier is required for SMEs because of financial and non-financial resource challenges. (H. K. Mustafa & S. Yaakub, 2018) One of the reasons the IFRS accounting standard introduced a version tailored toward SMEs. (D. Kaya, M. Koch, 2015) Thus, the research question includes the research that hinders the adoption of a cybersecurity standard. Furthermore, the thesis researches the components of a standard effective at managing cybersecurity risks.

The primary question is:

"What components of a cybersecurity standard are tailored toward an SME with a low adoption barrier that effectively manages cybersecurity risks?"

The thesis divides the primary questions into two sub-questions: one question regarding the hinders of adoption and one regarding the components of an effective cybersecurity standard.

- 1. What hinders the adoption of a cybersecurity standard among SMEs?
- 2. What are the components of an effective cybersecurity standard for SMEs?

Definitions

The definition of an SME

Small and medium-sized enterprises (SMEs) represent 99% of all businesses in the EU. The thesis bases the definition of the headcount and financials of an enterprise (turnover or balance sheet total. An SME is an organization that employs less than 250 people and has a turnover of fewer than 50 million euros. (European Commission, 2003) (Figure 2).

Further, the European Digital SME Alliance (2020) defines four types of SMEs relevant to cybersecurity standards.

- 1. There are SMEs that produce and sell digital hardware, software, and services. These are the "enablers of digital" **Digital enablers** are a part of the supply side of cybersecurity.
- 2. **Digitally based** SMEs are not fundamentally digital or cyber, but their business structures and primary functions substantially rely on digital technologies. They must understand compliance and cybersecurity needs to request them from their providers. These firms in the cybersecurity market rely on cybersecurity solutions to ensure the continuity of their business operations (demand side) and are "digitally dependent."
- 3. This type of SME is "digitally dependent" and needs standard ICT to operate. The number of **"digitally dependent"** companies in the digital economy is expanding rapidly. This group may have the greatest need for understandable and practical solutions.
- 4. **Start-ups** are a subset of the first and second categories. Being preoccupied with the functional development of their business models, they frequently overlook (or are unaware of) criteria such as 'security by design.' Security is a low priority under the pressure of competitiveness and aspirations to expand swiftly. To embrace security standards, this type of business requires measures and incentives.

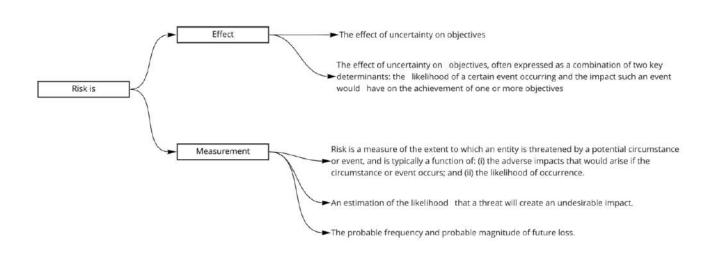
Company category	Staff headcount	Turnover	or Balance sheet total
Medium-sized	< 250	≤€ 50 m	≤€ 43 m
Small	< 50	≤€10 m	≤€ 10 m
Micro	< 10	≤€2 m	≤€2 m

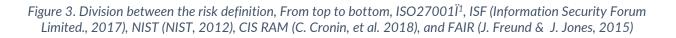
Figure 2, Definition of an SME. (European Commission, 2003).

Cybersecurity risk

For different people, the term "risk" has different meanings. The different meanings impact the way people perceive risk and, at the same time, influence how we measure and evaluate risk. This perception of risk influences the communication of risk. (Grima et al., 2021) Correct communication is required to measure and communicate risk correctly; hence, a clearconsistent risk definition must be employed. (Grima et al., 2021) (Jack Freund, J. J. 2015). However, the risk profession has not embraced a standard definition of the term risk (Jack Freund, J. J. 2015) – making it difficult to arrive at a clear-cut definition.

The thesis researches several authoritative publications and standards within the cybersecurity risk sector to arrive at a solid definition of risk.





The breakdown of the risk definitions identifies two significant differences between them. Risk is viewed as an "effect" by one group (ISO and ISF). The other group regards risk as a "measurement," a measure, an estimate, or a probability (NIST, CIS, FAIR). Figure 3 depicts the division.

The thesis uses the definition of the ISO27001: "**the effect of uncertainty on objectives**." Because of its holistic nature of the definition. In this definition, risk is a measurement. Thus, the definition of risk is open for interpretation by the organization.

¹ The ISO27001 uses the definition from the ISO31000 (ISO, 2018)

A cybersecurity standard for SME – Vincent van Dijk

Cybersecurity standard

NIST says that cyber security standards aim to improve the security of information technology (IT) systems, networks, and critical infrastructures. A cyber security standard defines functional and assurance requirements within a product, system, process, or technology environment. Security standards facilitate sharing knowledge and best practices by helping to ensure a common understanding of concepts, terms, and definitions, which prevents errors. (K. Scarfone et al., 2009)

A study conducted by ENISA into Information and Cybersecurity standards referred only to standards that an official issuer of standards issued. (ENISA, 2015) The ISO27001 is an example of such a standard issued by an official issuer: the International Organization of Standardization (ISO). The NIST Cybersecurity Framework issued by the National Institute of Standards and Technology is also an example.

However, not all standards used in practice are issued by organizations that are officially recognized for developing standards. The CIS Controls is an example of a widely used standard but not issued by an official issuer. Also, the Secure Control Framework is a standard created by volunteers.

In its essence, a standard is a level of quality. (Oxford Learners Dictionaries, n.d.) Thus, a standard can refer to a technical guideline, a policy, a framework, etc. For example, a standard policy has a certain level of quality that a group of people has set.

Within the scope of this research, the thesis scopes the word cybersecurity standard as a framework meant to communicate cybersecurity risks and related activities.

A cybersecurity standard is a framework to communicate cybersecurity risks and related activities,

Artifact

In Design Science Research, an *artifact* is defined as an object created by humans to solve a practical problem. To maintain a relationship both to common-sense and technical sciences and to give depth to the design aspect, an artifact must have a relation to "a human-made object. (Weigand, H. et al., 2021)

Based on system thinking, the thesis adjusts the current definition to a more holistic one because there is a need for a more holistic definition of artifact (Weigand, H. et al., 2021). System thinking regards itself as a more holistic approach to looking at the world. System thinking moved away from working with the idea of an `obvious' problem that required a solution to a situation that, for various reasons, may be regarded as problematical, which changed the aim of system thinking to improve a problematical situation instead of solving a problem. (P. Checkland, 2000)

An *artifact* is defined as an object created by humans with the intention of improving a problematical situation.

A cybersecurity standard for SME – Vincent van Dijk

Holistic

The thesis uses the word "holistic" multiple times. Because of the significance of the word to the direction of the research, the thesis defines the "holistic." The Oxford dictionary defines holistic as "considering a whole thing or being to be more than a collection of parts" or the medical definition as "treating the whole person rather than just the symptoms (= effects) of a disease." (Dictionaries, Oxford Learners, n.d.)

The core of the holistic definition is to not look at something like a collection of parts but to consider it whole. In system thinking, the analogy of the car is used to describe this concept. Only when a car is seen as it can perform its function to transport from A to B. The individual part cannot perform this function on its own. Therefore, the study of the car is holistic, and the study of the individual parts is not.

In systems biology, the study of interconnected structure and dynamics of cells and organisms are considered holistic. On the opposite, methodological reductionism describes the idea that complex systems or phenomena can be understood by analyzing simpler components. (F. Fang & A. Casadevall, 2011) Reductionism research is the opposite of holistic research; reductionism studies the individual parts instead of the whole.

The thesis studies a general problem; a general problem is holistic. Thus, **holistic research is studying the whole problem instead of the specific problems.**

Research design

There is a good deal of debate about the terminology of research. As the debate terminology gets more in the way of good research than encourages it, the thesis structures the research based on the research hierarchy (Figure 4). The hierarchy emphasis the "doing" rather than the "debating." (Pickard, A. J. 2013)

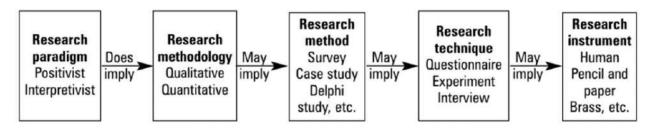


Figure 4, research hierarchy (Pickard, Dixon, 2002)

Research paradigm

A paradigm is a basic framework of assumptions, principles, and methods scientists conduct research. It is a set of norms that tell a scientist how to think and behave. (Kuhn, 1962). A paradigm comes before the theoretical perspective of the research. (Pickard and Dixon, 2002). For example, there is a discussion about the definition and usage of paradigms in the literature. Alan R. Hevner describes two research paradigms: design science and behavioral science.

Moreover, A.J. Pickard describes three paradigms: positivist, postpositivist, and interpretivism. The thesis uses the paradigms provided by A.J. Pickard. (Figure 4) to stay consistent with the thesis's research approach.

In the case of this investigation, the thesis interacts with an "object,"; the object being the artifact. The research on the interaction of an object falls under the interpretivism paradigm. Interpretivism is used as a general term for numerous types of research. Interpretivism is broken down into "empirical interpretivism" and "critical theory." The first is about looking at social phenomena in natural settings, while the second is about how people think and how society works now. The research is based on the second one, critical theory.

Research methodology

In Peter's talk in 2012, he emphasizes the usage of the word "methodology,"; where he says methodologies is distinctly different from the word "method." A methodology is a set of principles that need to be crafted into a method, a method being a set of rules and guidelines to tackle a particular problem. (Lancaster University Management School, 2012)

The thesis investigates multiple research methodologies and describes each approach in a paragraph. An enlightened choice is made by comparing the situations in which each approach excels in combination with the classification of the methodology as quantitative, qualitative, or mixed methods.

- 1. Question or hypothesis-based research
- 2. Design science research
- 3. Action research
- 4. System thinking
- 5. Soft design methodology

Question/hypothesis-based research

Question or hypothesis-based research is a traditional research approach. In this type of research, the researcher takes an observational view of the problem and asks questions such as "Does management style influence worker productivity?" (McNiff, Jean. Action Research, p. 10). These questions are from an outsider's perspective, looking at a situation and asking questions. Because of this, the traditional research approach applies well to the natural sciences. In the natural sciences, the researcher can only be the observer. Research is about obtaining an answer for a well-defined question by exploring literature and data or validating a hypothesis.

Design science research

Unlike the question or hypothesis-based research, design science aims to create an artifact. An artifact could be anything from a software application to a process, model or technique. Although one could assume that the study of design science is about the investigation into the design of an artifact, design science is actually about the investigation into an artifact in the context of a problem (Wieringa, 2014). The goal is to improve or solve the problem by inspecting and validating the interaction between the artifact and the context of the problem (Figure 5).

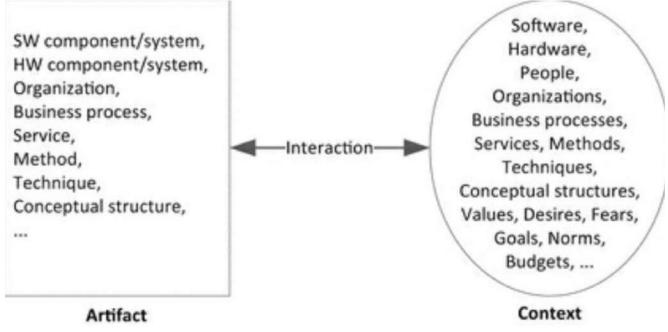


Figure 5, The subject of design science: an artifact interacting with its context

Action research

Action research is the researcher's inquiry into a problem while they are involved in the situation in which the problem occurs. For comparison, traditional researchers would ask, "Does management style influence worker productivity?" A researcher using action research, on the other hand, would ask, "How do I improve my management style to encourage productivity?" Action research aims to improve the situation (figure 6; McNiff, Jean, 2007).

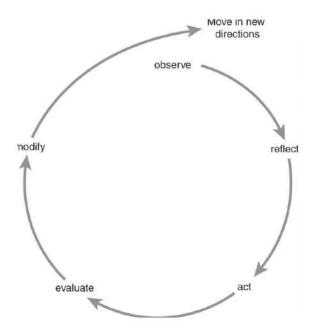


Figure 6, A typical action-reflection cycle (McNiff, Jean, 2007, p. 12)

System thinking

System thinking is divided into two streams: hard and soft. In hard system methodology (HSM), one assumes that the world can be seen as systems that interact with each other; some systems work well and some do not. One assumes that they can design a system into a better state. In soft system methodology (SSM), one does not assume that the world is a set of interacting systems—the systematic learning about and exploration of the complex world is the system. The learning about and exploring the complex world itself can be viewed as a "learning system." These differences can be seen in figure 7 (P. Checkland, 2000). For that reason, SSM shares similarities with actions research.

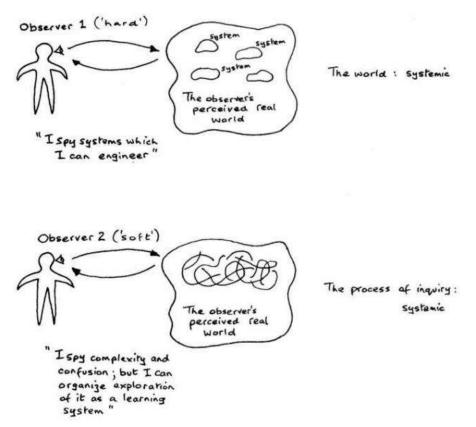


Figure 7, hard and soft system stances (Peter Checkland. Systems Thinking, Systems Practice: Includes a 30-Year Retrospective (Kindle Location 185). Kindle Edition.

Soft Design Methodology

Soft design methodology (SDM) is a methodology that emerged from combining soft system methodology (SSM) and design science. SSM accommodates the characteristics of design science, which makes combining the two methodologies straightforward. Although they differ in the abstraction process, abstractions arise from theorizing about design in design science, while the abstractions in SSM arise from drawing conceptual models. (Baskerville et al., 2009) SDM is a methodology that provides a process that excels at designing artifacts for problematic situations.

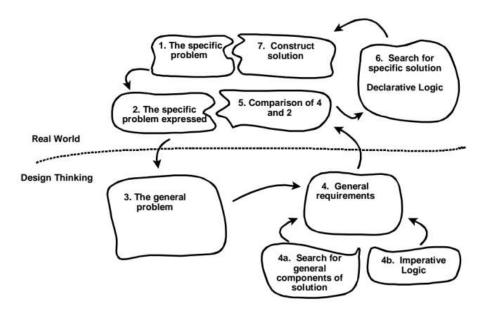


Figure 8, the Soft Design methodology process (Baskerville et al., 2009, page 5)

Selection

The thesis compares research approaches in table 1. Each of the approaches excels in different situations. Notable, the difference between quantitively, qualitative, or mixed methods does provide a distinctive difference for the choice of methodology. For this research, the thesis does not start from a case, which means the research approach should include a methodology that

- 1. Provides a holistic approach, a methodology that supports ill-defined problems
- 2. Results in an artifact

The first criteria arose because there is a need for a more holistic perspective. (Weigand, H. et al., 2021) System thinking is a holistic reaction against reductionism. The latest stream of system thinking (SSM) starts holistic problem solving from an ill-defined problem. (Checkland, 2000) Secondly, the thesis aims to result in an artifact that improves the ill-defined problem.

Thus, HSM, SSM, and SDM are appropriate options; all the other approaches require welldefined issues. However, only SDM results in an artifact out of those three options. Thus, SDM is selected for the research.

Approach	Excels in situation	Quantitively or qualitive
Question/hypothesis- based research	Researching from an observer view of a situation	Quantitively, qualitative or mixed methods
Design science	Creation of an artifact for well- defined problems	Quantitively, qualitative or mixed methods
Action research	Researching while doing the activity being researched	Qualitative
Hard System Methodology (HSM)	Solving/dissolving problems in scenario's where the systems can be clearly observed and defined	Qualitative
Soft System Methodology (SSM)	Deciding on actions where the problem is ill-defined	Qualitative
Soft Design Methodology (SDM)	Designing an artifact for ill- defined problems	Quantitively, qualitative or mixed methods

Soft Design Methodology (SDM) is selected as the approach for this research.

Table 1, comparison of the research approaches

Adaptions to SDM

SDM consists of 7 steps. These seven steps are seven activities that the researcher needs to follow to solve a specific problem. (Baskerville et al., 2009).

- 1. The researcher identifies and expresses the specific problem.
- 2. This problem is then be expressed as a specific set of requirements
- 3. In the systems world, the requirements for the specific problem are systemically abstracted and translated into a general problem with both technical and social dimensions. Here the design thinking is about a class of problems rather than the specific problem owned by the client
- 4. A general solution design (a class of solutions) for the general problem is derived through systems thinking and expressed in terms of general requirements. This activity involves a combination of design science techniques, such as the search for general components of the solution together with expression using imperative logic.
- 5. The general design requirements are compared with the specific problem for fit. In this activity the specific problem is re-articulated in terms of the general requirements and the imperative logic.
- 6. A declarative search is then made for the specific components that will provide a workable instance of a solution to the general requirements. The declarative search is made necessary by difficulties in operating imperative logic.
- 7. An instance of the specific solution is constructed and deployed into the social system. In this way, the specific problem is changed (hopefully improved), learning, is derived, and the cycle begins again.

Step 1 starts with a specific problem, a problem that has been observed in the real world. In the context of the design science research framework (Figure 9), SDM's first step starts at the relevancy cycle, then moves to design science and rigor.

Although the thesis begins with rigor rather than relevance because far too frequently, design study is confined to building/evaluating a single technical output within a defined project. This may have sufficed in the past, but now we need a more holistic perspective. (Weigand, H. et al., 2021)

SDM is designed to go from left to right, from relevance to rigor. In the case of this research, the thesis does not start from the relevance cycle but from the rigor cycle. Thus, the steps in the SDM process need to be changed to fit the thesis's scenario. As a result, the thesis switches steps 1 and 2 for 3 and 4.

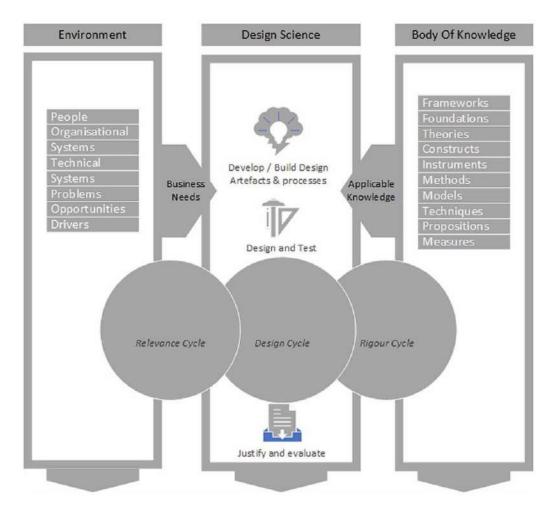


Figure 9, Hevner's Design Science Research Framework (2004)

During the research proces, it was noticed that the specific problem, step 3, is not a good fit in the process. Because the step assumes that the people know the specific problem, which was not the case because of the broad scope of the general problem; the general problem's complexity could not be translated to a specific problem. Instead, the thesis uses research questions to guide the exploration to requirements (step 4).

In conclusion, the thesis adapts the steps from SDM to the following seven steps.

In conclusion, I adapt the steps from SDM to the following seven steps.

- 1. The general problem
- 2. The general problem expressed as requirements
- 3. Answering the research question
- 4. The research question expressed as requirements
- 5. Comparison between the general requirements and specific requirements
- 6. Declarative search for a specific solution
- 7. Construct solution

Research methods

The research method is in the frame of SDM, the methodology. SDM provides a process, set of principles, and research process. However, it does not provide the underlying methods. Peter Checkland suggests using multiple methods. (Peter Checkland, 2000)

Before going into the seven steps, the thesis collects a literature dataset. The literature dataset provides the initial search for the general problem (step 1). Furthermore, the thesis uses Group Support System (GSS) in step 3 to collect data for the research questions. GSS can be used to brainstorm, rate, select and prioritize with a group of people — the participants. The use of GSS over the Delphi method or interviews because GSS supports collecting qualitative data such as comments and brainstorming items in a group setting. The comments and brainstorming items are great for the general problems, a problem where not all the underlying specific problems are known. Furthermore, the discussions into open-ended questions provide a creative opportunity for participants to discuss an artifact.

Literature

The thesis uses the literature dataset throughout the seven steps of the SDM methodology. However, the primary purpose of the literature dataset is to provide the general problem in step 1.

The snowballing technique is used to create a dataset of 50 relevant publications. Snowballing is a technique to systematically build a literature dataset by iterating over publications referring to each other.

Fifty publications are estimated to have a comprehensive set of resources but still provide indepth analysis within the timeframe to conduct this research. The thesis starts with backward snowballing and moves towards forward snowballing when not enough publications can be gathered that meet the criteria.

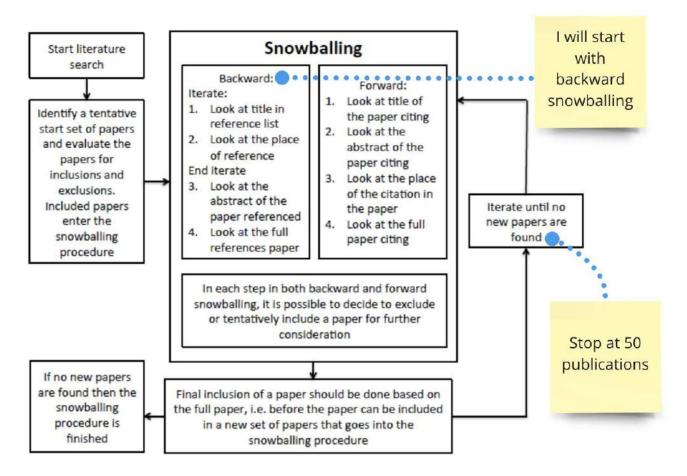


Figure 10 snowballing procedure (C. Wohlin, 2014)

Fourteen articles were collected from the "SME cybersecurity" search term to start the snowballing process. The search term is generic. The thesis uses a generic term because a generic term is an excellent interface for searching for a general problem (step 1) as it starts the search from the highest level of abstraction.

For each of these publications, the references were gathered. The number of publications explodes to a total of 426. A graph database called Neo4j is used to visualize the dataset of references. Figure 11 shows the relations between the references. Although the nodes in the graph are not readable, the visualizations show multiple connections between references:

- Some articles are a referred to by multiple publications
- The starting publications refer to each other

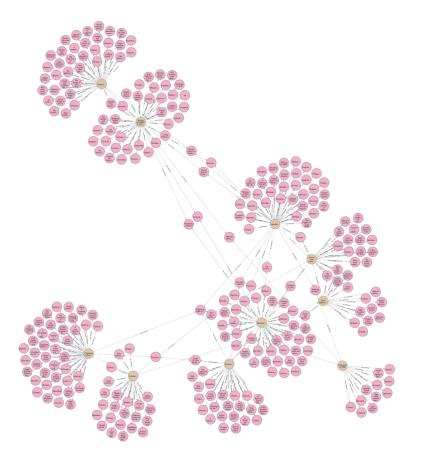


Figure 11 visualizes the explosion of references based on the 14 start publications. The brown nodes are the starting publications; the pink ones are the references.

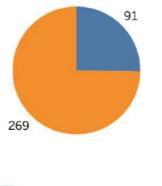
Thirty references were present in more than one publication; 2 references were present three times, and two references were present in 4 publications. These references are interesting because the assumption can be made that they might form the base for multiple starting publications. Later in the process, the thesis assesses if they are valuable.

- 1. Exploring SME cybersecurity practices in developing countries -4 times
- 2. Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs -4 times
- 3. Cyber security guide for SME 3 times

All the publications referred to more than once were added to the dataset of publications because those publications might be necessary to the foundation of the 14 start publications, in total that concludes with 44 references. The publications, which were only mentioned once, were labeled in a Label Studio tool to continue growing the dataset of potential valuable publications. *Label Studio* is an open-source software meant to label and annotate texts, images, and audio. Label Studio is used to label relevant publications according to the following criteria.

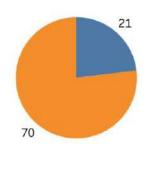
- 1. The publication is aimed at SMEs or aimed at organizational characteristics AND
- 2. The publication is about cybersecurity, information or data security or risk AND
- 3. The publication is focused on
 - A. Identifying challenges OR
 - B. Identifying a state OR
 - C. Identifying potential improvements OR
 - D. Identifying factors OR
 - E. Provides a framework, method, or another artifact

These criteria have been set up to identify relevant publications. Out of the 360 articles that were only referred to 1 time, 91 were about SMEs (1). Of the 91 SME publications, 70 were about cybersecurity (2); 60 publications had an in-scope focus (3). Adding those 60 publications to the dataset concludes in a dataset of 104 publications.



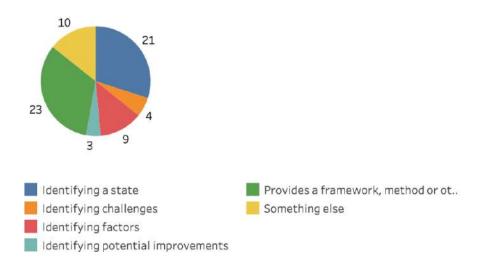
The publication is about SME
 The publication is NOT about SME

Figure 12, criteria 1, the publication is aimed at SMEs or organizational characteristics.



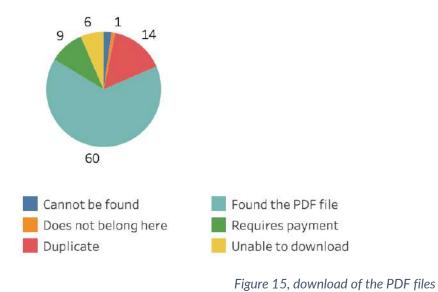
The publication is about another topic
The publication is about cybersecurity, information or data security







To continue the research by trying to download the PDF files. Out of the 90 publications, 60 can be downloaded; 1 publication was corrupted and labeled as "does not belong here." Surprisingly, 14 duplicates were found; these were cases of references having different titles but linked to the same document. 60 PDF files were added to the 14 starting PDF files and concluded a dataset of 74 PDF files.



A cybersecurity standard for SME – Vincent van Dijk

Group Support Sytem (GSS)

GSS is defined as an interactive computer-based system that enables a group of decisionmakers to solve unstructured problems. GSS is a collection of techniques, software, and technology to enhance group communication, discussion, and decision-making. Numerous studies have proven that GSS effectively increases the efficiency, dependability, and quality of group decision-making in meetings. (Q. Shen et al. 2004)

Design

The uses GSS to research the research questions among a group of experts likely to use the artifact after its creation, a representative target audience panel. The thesis groups the questions used in the session into five groups. Furthermore, each group is linked to the research question. The questions are based on the position paper of the European Digital SME Alliance and a cybersecurity standard that was chosen. (Table 2).

The authors ask for a cybersecurity standard tailored toward SMEs in the European Digital SME Alliance position paper. One of their requirements for such a framework is that the standard is freely available to the whole community. (European Digital SME Alliance, 2021) Thus, the research must be based on a standard that enables the free sharing of derivative work.

The thesis selects the NIST Cybersecurity Framework for this purpose as the only widely used framework that is freely available. (Table 3)

Dr. Yuri Bobbert facilitated the session to prevent bias from the researcher.

Category	Research question	Questions	Source
The experience of the participant	N/A	Appendix A. 1	N/A
Desired risk management level	What are the components of an effective cybersecurity framework for SMEs?	Appendix A. 2	National Institute of Standards and Technology, 2016
Hurdles that hinder the adoption of standards	What hinders the adoption of a cybersecurity framework among SMEs?	Appendix A. 3	European Digital SME Alliance, 2021
Effective components	What are the components of an effective cybersecurity framework for SMEs?	Appendix A. 4	National Institute of Standards and Technology, 2016
Artifact design	What are the components of an effective cybersecurity framework for SMEs?	Appendix A. 5	N/A

Table 2, question categories

Framework	Free commercial usage	Transform material
NIST Cybersecurity Framework (NIST CSF)	Yes	Yes
ISO27001	No	No
CIS Controls version 8	No	No
Secure Control Framework (SCF)	Yes	No

Table 3, license of four cybersecurity frameworks

Analysis

The experience of the participant

Eight participants specified their years of experience with cybersecurity. In total the participants have more than 130 years of experience, an average of 16 years per participant. Furthermore, 7 out of 9 participants have experience with cybersecurity management and technical cybersecurity. One participant only had experience with cybersecurity management, and one participant only had experience with technical cybersecurity.

Hurdles that hinder the adoption of standards

The Digital SME Alliance lists 13 hurdles that hinder the adoption of a cybersecurity standard for SMEs. In the GSS session, the participants allocated 100 points among hurdles. Most points were given to those hurdles that most hindered the adoption. Then, the average number of points is calculated per hurdle.

Two hurdles were most dominant.

- 1. Lack of resources. Average points: 27.5
- 2. Implementation cost of standards. Average points 21.9

The third hurdle was behind the other two hurdles with an average of 14.4 points: 34% lower than "Implementation cost of standards."

In conclusion, according to the session participants, the lack of resources and the implementation cost of standards are the most dominant hurdles that hinder the adoption of a cybersecurity framework among SMEs.

NIST Cybersecurity Framework (NIST CSF)

To understand the analysis of the "risk management process" and the "effective components," you need to understand their origin, NIST CSF. NIST CSF consists of 3 components: core, tiers, and profile. (National Institute of Standards and Technology, 2016)

- Core provides a set of desired cybersecurity activities and outcomes using a common language that is easy to understand.
- Tiers assist organizations by providing context on how an organization views cybersecurity risk management.
- Profiles are an organization's unique alignment of its organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core.

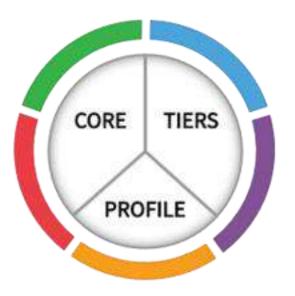


Figure 16, NIST CSF Framework Components (NIST, n.d.)

In the scope of the research, only core and tiers are relevant because the profile is the organizational context that can only be known after implementing the standard.

The tiers refer to the degree of risk management that an organization wants. According to the participants, the thesis uses statements from those tiers to assess how an SME should view its risk management process.

Core provides a common language to cybersecurity, divided into five functions and 23 categories. The thesis shortens the 23 categories to 16 categories, the respond and recover function were combined into two categories instead 9. The thesis uses these 16 categories to research effective components for a cybersecurity program.

Risk management process

The participants rated statements extracted from the NIST CSF on the risk management process, desired integration of risk management, and the desired level of participation in the larger ecosystem.

- 7/10 of participants agreed that management should at least approve the risk management processes, even though there might not be an organizational-wide policy.
 4 out of the 7 participants expressed that the policy should also be formally approved.
- The participants agreed that risk management needs an organization-wide approach (9/10 votes).
- 10/10 of participants agreed that an SME should have a limited understanding of its role in the broader ecosystem. Although, the participants could not agree to which degree an SME should contribute to the larger ecosystem. 3/10 voted for no contribution, 4/10 for maybe contribute, and 3/10 voted for sharing risk information

Effective components

The Participants ranked each category on effectiveness and ease of implementation. The two rankings determine which categories are, according to the participants, most effective in reducing cybersecurity risks and which categories have an effective implementation process.

Figure 17 shows how the participants rate the categories on effectiveness against the ease of implementation. Notable, most categories which high effectiveness are also easy to implement. Notable, categories with low perceived ease of implementation also have low perceived effectiveness.

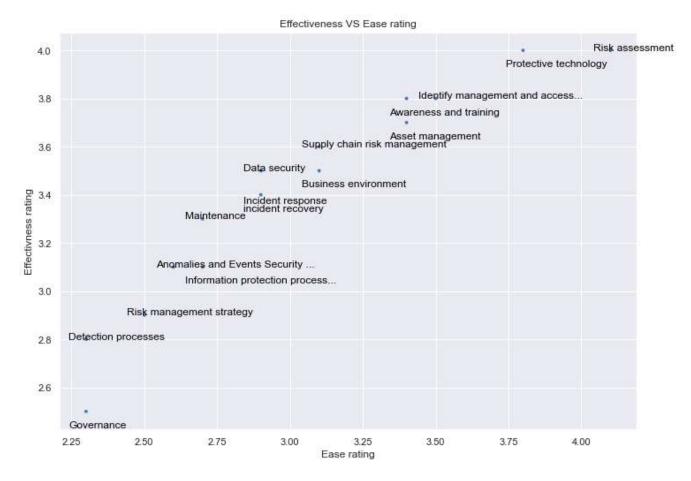


Figure 17, effectiveness vs ease of implementation

Figure 18 shows the variability of the participant's ratings on effectiveness and ease of implementation. The variability indicates to which degree participants did or did not agree with each other. Maintenance was a severe outlier; the effectiveness and ease of implementation variability are more than 0.7. Multiple participants commented on the effectiveness that maintenance is a precondition for effective cybersecurity, while one participant argued that maintenance is not suitable for SMEs.

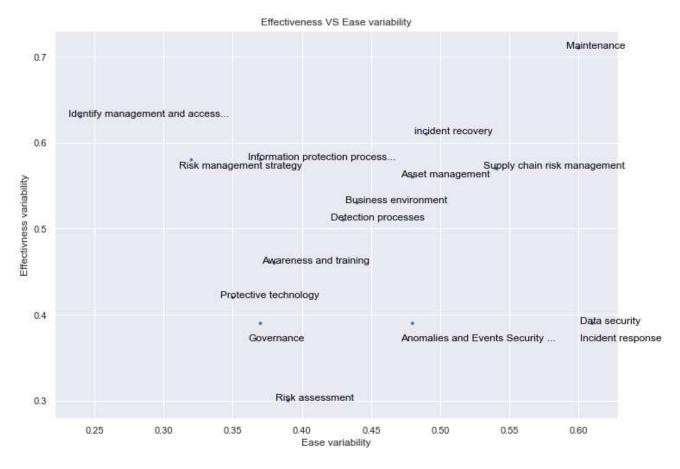


Figure 18, effectiveness vs ease of implementation variability,

Furthermore, the data suggest that participants have a different opinions on the effectiveness. 9 out of 16 categories have a variability above 0.5.

- 1. Maintenance
- 2. Identify management and access control
- 3. Incident recovery
- 4. Information protection processes
- 5. Risk management strategy
- 6. Supply chain risk management
- 7. Asset management
- 8. Business environment
- 9. Detection processes

However, the data suggests that the participants mostly agree on the ease of implementation. Only 4 out of 16 categories have a variability above 0.5.

- 1. Maintenance
- 2. Data security
- 3. Incident response
- 4. Supply chain risk management

Additional to the rating of the categories, participants commented multiple times that, even though the list of categories is already condensed from 23 to 16 categories, the categories need to be further condensed; duplicates and lookalikes need to be removed.

Artifact design

Participants see the need that the standard needs to be designed for the person responsible for cybersecurity within an organization. The person responsible for cybersecurity could be the CISO, a CIO in the absence of a CISO, or an external. Also, participants agree that there needs to be involvement from C-level, but they are not the one that implements and use the standard. Furthermore, the standard needs to be understandable by everyone in the organization.

In the standard format, participants seem to have widely different ideas, but they most dominantly refer to the standard in the form of a checklist. A checklist is mentioned 4 out of 13 times. Although, a wide area of different answers, the thesis concludes that the participants are unsure about the format of the standard.

Finally, 9 out of 10 participants said they would advise the standard to SMEs. One participant said "no" and argued that the standard is too explicit, and an SME requires flexibility to create a fit for the organization.

The 7 steps of SDM

SDM consists of 7 steps. These seven steps are seven activities that the researcher needs to follow to solve a specific problem. (Baskerville et al., 2009). The steps start at a general problem and continue searching for a specific solution. The seven steps facilitated the search for a specific solution.

Step 1 – The general problem

This step repeats the problem statement because the problem statement is the general problem.

Adoption of information technology (IT) is one of the areas recommended to small and medium-sized enterprises (SMEs) to confront competitive challenges (M. A. Nugroho et al., 2017). However, the rise of information technology also poses challenges.

SMEs are prone to be more intensively affected by some specific cyberthreats and attacks than larger enterprises. (M. Antunes, 2021) To reduce the effect of cyber risks, organizations must align their cybersecurity maturity with their risk appetite. Cybersecurity maturity is managed and measured through cybersecurity standards, such as the ISO27001 and the NIST Cybersecurity Framework (D. Proença & J. Borbinha, 2018) However, SMEs are unable effectivity adopt current standards because of the high implementation cost of standards, lack of resources, lack of technical solutions, lack of awareness and more. (European Digital SME Alliance) The lack of resources of SME was the primary reason of the existence of the SME version of the ISRS. (D. Kaya, M. Koch, 2015) Yet it is unsure of that is also the case for cybersecurity standards.

Exciting solutions originating from academic research lack the involvement of an SME's context and risks. Moreover, no study has been conducted into the required components of a standard.

For this research, the thesis uses the following problem statement:

"SMEs cannot adopt current cybersecurity standards effectively because of the lack of standards tailored toward SMEs. "

Step 2 – The general problem expressed in the requirements

The problem statement translates into two requirements. Currently, SMEs are unable to adopt the current cybersecurity standard effectiveness. The adoption part of the problem statement can be expressed as a requirement that the artifact should be easily adoptable by SME. Also, the cybersecurity standard should not lack effectiveness because then the adoption of the standard would not be desired. Finally, the problem statement expresses the need for the standard tailored toward SMEs. This expression is the third requirement.

In total, the general problem can be expressed into the following requirements:

- 1. SMEs can easily adopt the cybersecurity standard
- 2. The cybersecurity standard is effective at managing cybersecurity risk
- 3. The artifact needs to be tailored toward SME

Step 3 – Answering the research question

In the chapter "Research question," the thesis states the research question and the underlying sub-question. The thesis uses the analysis of the GSS located in the chapter "Group Support System (GSS)" to answer the question,

Sub-question 1: What hinders the adoption of a cybersecurity framework among SMEs?

According to the session participants, the lack of resources and the implementation cost of standards are the most dominant hurdles that hinder the adoption of a cybersecurity framework among SMEs.

Sub-question 2: What components of an effective cybersecurity standard for SMEs?

In the analysis of the risk management process, the thesis concludes three components regarding the risk management process that are components of an effective cybersecurity standard for SMEs.

- 1. Management approval on the risk management processes
- 2. An organization-wide approach to risk management
- 3. Promote at least a limited understanding of the broader ecosystem.

Furthermore, the research on the categories shows that there are nine categories perceived to be effective at managing cybersecurity risks (rate above 3.5).

- 1. Risk assessment (effectiveness: 4.0)
- 2. Protective technology (effectiveness: 4.0)
- 3. Identify management and access... (effectiveness: 3.8)
- 4. Awareness and training (effectiveness: 3.8)
- 5. Asset management (effectiveness: 3.7)
- 6. Supply chain risk management (effectiveness: 3.6)
- 7. Business environment (effectiveness: 3.5)
- 8. Data security (effectiveness: 3.5)
- 9. Incident response (effectiveness: 3.5)

Combing these two lists result in a list of effective components of a cybersecurity standard for SMEs.

- 1. Management approval on the risk management processes
- 2. An organization-wide approach to risk management
- 3. Promote at least a limited understanding of the broader ecosystem.
- 4. Risk assessment
- 5. Protective technology
- 6. Identify management and access control
- 7. Awareness and training
- 8. Asset management
- 9. Supply chain risk management
- 10. Business environment
- 11. Data security
- 12. Incident response

The central question: What components of a cybersecurity standard are tailored toward an SME with a low adoption barrier that effectively manages cybersecurity risks?"

The answer to the first sub-question showed that there are two hurdles:

- 1. Lack of resources
- 2. The implementation cost of the standard

In the analysis of the categories, there is a clear difference in effectiveness between categories. The thesis chose to select only the categories to be perceived effective (rate above 3.5) and with a perceived rate of implementation above 3.5 to accommodate the hurdles mentioned in answer to the first sub-question. The criteria resulted in three categories relevant as components.

- 1. Risk assessment (effectiveness: 4.0, ease of implementation: 4.1)
- 2. Protective technology (effectiveness: 4.0, ease of implementation: 3.8)
- Identify management and access control (effectiveness: 3.8, ease of implementation: 3.5)

Combined with the risk management process components, the resulting list counts six components.

- 1. Management approval on the risk management processes
- 2. An organization-wide approach to risk management
- 3. The organization has at least a limited understanding of the broader ecosystem
- 4. Risk assessment
- 5. Protective technology
- 6. Identity management and access control

Step 4 – The specific requirements

The components from step 3 need to be expressed as requirements to create an artifact. The requirements will be used in step 6 to search for a specific solution. The thesis expresses the components as requirements in Table 4.

Component	Expressed as a requirement
Management approval on the risk management processes	It is a requirement that management approval needs to be promoted
An organization-wide approach to risk management	It is a requirement should allow for easy communication towards the whole organization
The organization has at least a limited understanding of the broader ecosystem	It is a requirement that the artifact includes an understanding of the broader ecosystem
Risk assessment	It is a requirement that the artifact includes a risk assessment
Protective technology	It is a requirement that the protective technology is included in the artifact

Table 4, Components expressed as requirements

Furthermore, the thesis uses imperative logic on the comments from the participants to further define specific requirements.

Comment from participants	Expressed as a requirement	Rationale
 Depends on the company and their way of working The industry of SME companies has similar context and often can use similar processes Dynamic checklist Local rules and regulations that may impact on how the SME does/is allowed to do risk 	It is a requirement that the artifact is flexible and can deal with the specific requirements of the environment of the company	The participants expressed that the artifact needs to be tailored to the SME that uses it: depending on their way of working and the industry, local law, etc. Secondly, the dynamic checklist was a proposed solution by multiple participants to deal with the company specifics. Finally, a participant argued he would not advice the standard to SMEs because the standard is too explicit and flexibility is required.
 Categories are for Security managers (CISO, ISO etc.) and for C-level. rationales need to come in multiple forms related to different personas 	 It is a requirement that the artifact can be used by subject matter experts It is a requirement that the artifact can be understood by C-level and all other employees 	Participants expressed that the artifact needs to be understandable for different personas, categories into 1. Subject matter experts (CISO, CIO, external consultant) 2. C-level / management 3. All other employees

Table 5, participants comments expressed as requirements

Combing the two tables together results in a final list of eight specific requirements.

- 1. It is a requirement that management approval needs to be promoted
- 2. It is a requirement should allow for easy communication towards the whole organization
- 3. It is a requirement that the artifact includes an understanding of the broader ecosystem
- 4. It is a requirement that the artifact includes a risk assessment
- 5. It is a requirement that the protective technology is included in the artifact
- 6. It is a requirement that the artifact is flexible and can deal with the specific requirements of the environment of the company
- 7. It is a requirement that the artifact can be used by subject matter experts
- 8. It is a requirement that the artifact can be understood by C-level and all other employees

Step 5 – Comparison between the general requirements and specific requirements

The comparison between the general and specific requirements reveals if there are any gaps between the two types of requirements.

Based on the analysis of table 6, the thesis concludes that there is no gap perceived between the general and specific requirements. The specific requirements are selected by answering the research question with the first and second general requirements in mind.

General requirements	Specific requirements
SMEs can easily adopt the cybersecurity standard	It is a requirement that management approval needs to be promoted
The cybersecurity standard is effective at managing cybersecurity risk	It is a requirement should allow for easy communication towards the whole organization
The artifact needs to be tailored toward SME	It is a requirement that the artifact includes an understanding of the broader ecosystem
	It is a requirement that the artifact includes a risk assessment
	It is a requirement that the protective technology is included in the artifact
	It is a requirement that the artifact is flexible and can deal with the specific requirements of the environment of the company
	It is a requirement that the artifact can be used by subject matter experts
	It is a requirement that the artifact can be understood by C-level and all other employees

Table 6, comparison between the general and specific requirements

Step 6 – Declarative search for a specific solution

The search for a specific solution is a creative process where the output heavily relies on the researcher's capabilities, experience, and creativity. In the search for the solution, the thesis draws inspiration from literature, the analysis of the GSS session, and experience in the industry. The declarative search outputs imperative statements on the specific solution. (Baskerville et al., 2009)

Imperative statement	Rationale
The artifact is expressed as a model which includes all the specific requirements	Models such as the Business Model Canvas, SWOT analysis, 7P marketing mix are widely used by management.
The artifact is a presented in a widely used format, such as a presentation or document	The artifact needs to be customizable by the organization. (Referring to specific requirement 6)
Example usage of the artifact	Examples show people how the artifact can be used; making it easier to understand
Easily adjustable by offering components for customization	Because of the complex nature of organization and custom requirements should the model be easily customizable

Step 7 – Construct the solution

The solution is the small cybersecurity canvas. The individuals can use the canvas to get involved from a strategic perspective about the risks, cybersecurity, and measures. The canvas is made in PowerPoint format and can be easily adjusted and customized.

- 1. The basic canvas
- 2. Examples
 - $\circ \quad \text{Small online retailer} \\$
 - Small IT service provider (custom)
- 3. Catalog of components

1. The basic canvas

The basic canvas provides (figure 19) the user with the company details on the left and the measures on the right. The left side is centered around company specifications and risk assessment.

- 1. Business context: explaining why the business wants to conduct a cybersecurity program
- 2. Company risks: the integration with company-wide risk management. The list of company risks will list all the critical non-cyber-related risks.
- 3. Cyber-risks: short for cybersecurity risks. Here the cybersecurity-specific risks are being listed.

On the right side are the measures that reduce or mitigate the risks. Only the two categories with the second and third highest perceived effectiveness (protective technology and identity and access) are mentioned in the basic version. The category with the highest perceived effectivity, risk assessment, is represented on the left side. Within the boxes, the user can specify measures they implemented or want to implement from that category.

Furthermore, the individuals are presented with three steps that can be used as guidance to fill in the canvas.

Small Cybersecurity Canvas — 🛛 🕦 BASIC	Decide on the company on the left first, business context, cyber-risks and company-risks. The move on to the right side. Here you determine the measures you want to have in place. The green notes and the controls that are in place. Red notes still need to be implemented or indicate issues.
Company	Measures
Business context Why did the company start the initiative to improve cybersecurity? Note	Protective technology Which protective technology does your company have? (ex. antivirus, firewalls, etc.) Note
Company-risks Which risks, which are not cyber-related, might hurt your company? (ex. failure to acquire funding, completion risks, etc.)	Identity and access How are roles and permissions implemented in your company?(ex. role based access, quarterly check-up)
Cyber-risks Which most important cyber-risks might hurt your company?	Note

Figure 19, basic version of the Small Cybersecurity Canvas

2. Examples

The artifact contains examples that help the user with how the canvas can potentially be used. The first example, the small online retailer, implements the basic canvas. Moreover, the second example shows a small IT service provider's implementation of a customized canvas.



	technlogy		
	technology does your x. antivirus, firewalls,		
Creditcard processing nrough secure third party	Firewalls Backups	Ant-virus	Web Application Firewall
Identity ar	Id access Id permissions implei ble based access, qua		
		and the second s	

Figure 20, example 1

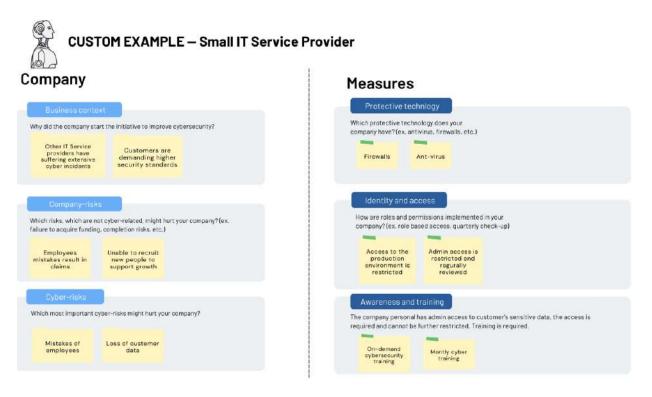


Figure 21, example 2

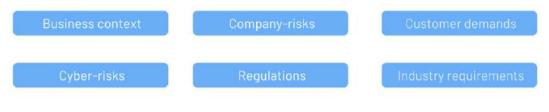
3. Catalog of components

The catalog of components lists components that a user can copy and paste into their custom canvas. These components are grouped into "company", "measures" and empty components.

The company components are components that can be used to define the left side. These components are about business context and risk.

Company

Components you can use to organize the business side of the canvas. These components are examples, and it is promoted to create your owncomponents if it helps you better express the business's context.





The measures components are—a consolidated list of categories of the NIST Cybersecurity. (Table 8). The list got consolidated because of the multiple comments from the GSS session asking for consolidation. Additionally, the categories "business environment" and "risk management" are not in the measures catalog because they were represented in the "company" catalog.

Measures

The measure categories are sorted based on the perceived effectiveness and ease of implementation. You can use these categories or create your own. All the categories are based on the NIST Cybersecurity Framework.



Figure 23 measures components

Lastly, the empty components are a set of empty components that users can use to create their own components.

<company></company>		
escription?		
	_	
<measure></measure>		
ote> <note></note>	<note></note>	
(note)	<note></note>	



Findings

The research led to several findings in different categories. The main objective of researching a cybersecurity standard for SMEs led to most findings. Nevertheless, apart from the main objective, several findings could be concluded on the NIST CSF and the research methodology, SDM.

Cybersecurity standard

The thesis concludes with several findings relevant to developing a cybersecurity standard for SMEs. Furthermore, the findings show that further research is required into the effectiveness of NIST CSF categories; participants had a high variance in scoring the categories on effectiveness. The thesis extracts seven findings from the GSS session are listed below.

- 1. The participants of the GSS session mostly agree on the ease of implementation of NIST CSF categories. However, there is a high variance among participants on the effectiveness of the categories.
- 2. The perceived effectiveness and ease of implementation of maintenance practices are highly varied.
- 3. Participants agree that the lack of resources and the cost of implementing standards are the most dominant perceived hurdles for SMEs to improve cybersecurity.
- 4. Participants agreed that their cybersecurity needs an organization-wide approach.
- 5. Participants agreed that an SME needs at least to have a limited understanding of the eco-system
- 6. Participants agreed that senior management approval is required for cybersecurity risk management.
- 7. Participants mentioned that most components of a framework depend on the specific context of the SME in question.

Soft Design Methodology (SDM)

The SDM process does not work on problems that originate in the rigid cycle of design science; instead, the process starts from relevancy. Adjustments were needed to perform the process from the rigid cycle. The adjustments to the steps resulted in new steps within a new sequence. Future research that takes a similar, holistic approach to the rigid cycle of design science can use these seven steps.

Furthermore, the seven steps could be further developed to enhance the depth of SDM.

- 1. The general problem
- 2. The general problem expressed as requirements
- 3. Answering the research question
- 4. The research question expressed as requirements
- 5. Comparison between the general requirements and specific requirements
- 6. Declarative search for a specific solution
- 7. Construct solution

NIST CSF

Participants experienced confusion on the categories of the NIST CSF. There seems to be an overlap between categories. The GSS session resulted in a consolidated list of categories (table 7 & 8). Practitioners that use the NIST CSF could consider the new set of categories instead of the original NIST CSF categories.

Although the new list is consolidated of categories according to the research results, further research is required to verify if the consolidated list works in practice.

Categories	Resulting category	Rationale
 Risk management strategy Risk assessment Supply chain risk management 	Risk management	Participants expressed that these three categories need to be consolidated into one.
All the categories of function response have been consolidated	Incident response	There are duplicated categories in response that are also present in recovery. Furthermore, the size of the categories seems too small to be taken as separate categories.
All the categories of function recover have been consolidated	Incident recovery	There are duplicated categories in response that are also present in response. Furthermore, the size of the categories seems too small to be taken as separate categories.
 Information Protection Processes and Procedures Data security 	Data security	Participants expressed that these two categories need to be consolidated into one.
 Anomalies and Events Security Continuous Monitoring 	Monitoring of events and anomalies	These two categories could be viewed as sub-categories, but they are too small to view them as separate.

 Table 7, the rationale behind the consolidation of components

Function	Category
Identify	Asset Management
	Risk Management
	Business Environment
	Governance
Protect	Protective Technology
	Awareness and Training
	Data Security
	Maintenance
Detect	Monitoring of Events and Anomalies
	Detection Processes
Response	Incident Response
Recover	Incident Recovery

Table 8, the list of 12 consolidated NIST CSF categories

Conclusion

The thesis concludes with answers to the research questions. Moreover, the conclusion goes into the artifact and compares the artifact to the literature. Finally, based on the conclusions, the thesis draws a checklist that SMEs can follow to comply with the best practices concluded from the research; the participants of the GSS session requested a checklist.

What hinders the adoption of a cybersecurity standard among SMEs?

According to the session participants, the lack of resources and the implementation cost of standards are the most dominant hurdles that hinder the adoption of a cybersecurity framework among SMEs. Those two findings confirm the International Accounting Standards Board (IASB) conclusion to tailor an accounting standard toward SMEs. (D. Kaya, M. Koch, 2015) And the request for a cybersecurity standard tailored toward SMEs was made by the European Digital SME Alliance (2020).

What are the components of an effective cybersecurity standard for SMEs?

A combined list of applicable categories and risk management parts concludes a list of twelve components that are, according to the participants, required for a cybersecurity standard.

- 1. Management approval on the risk management processes
- 2. An organization-wide approach to risk management
- 3. Promote at least a limited understanding of the broader ecosystem.
- 4. Risk assessment
- 5. Protective technology
- 6. Identify management and access control
- 7. Awareness and training
- 8. Asset management
- 9. Supply chain risk management
- 10. Business environment
- 11. Data security
- 12. Incident response

What are the components of a cybersecurity framework tailored toward an SME with a low adoption barrier that is effective in managing cybersecurity risks?

The answer to the first sub-question showed revealed there are two hurdles. These two hurdles confirm the conclusion hurdles mentioned in the literature. (D. Kaya, M. Koch, 2015; European Digital SME Alliance, 2020)

- 1. Lack of resources
- 2. The implementation cost of the standard

In the analysis of the categories, there is a clear difference in effectiveness between categories. The thesis selects only the categories to be perceived effective (rate above 3.5) and with a perceived rate of implementation above 3.5 to accommodate the hurdles mentioned in answer to the first sub-question. The criteria resulted in three categories relevant as components.

- 1. Risk assessment (effectiveness: 4.0, ease of implementation: 4.1)
- 2. Protective technology (effectiveness: 4.0, ease of implementation: 3.8)
- Identify management and access control (effectiveness: 3.8, ease of implementation: 3.5)

Combined with the risk management process components, the resulting list counts six components.

- 1. Management approval of the risk management processes
- 2. An organization-wide approach to risk management
- 3. The organization has at least a limited understanding of the broader ecosystem
- 4. Risk assessment
- 5. Protective technology
- 6. Identity management and access control

The artifact

A cybersecurity standard for SMEs is already proposed in the form of a canvas (S. Teufel et al., 2020). Nevertheless, their canvas had the characteristics of a "one-size-fits-all." The authors already hinted that this might be a limitation of their canvas. Moreover, according to the participants of the GSS, a one-size-fits-all approach is indeed not desired. Thus, the resulting framework needs to be flexible to fit the specific requirements of the SME.

Furthermore, this conclusion confirms the research results on Organizational Characteristics Influencing SMEs (F. Mijnhardt et al., 2016). Their research concludes 14 organizational characteristics that influence information security in SMEs, more than the one characteristic in this research, organization size. The European Digital SME Alliance (2020) also confirm the same conclusion with their four types of SMEs. They state that the standards and certifications need to be tailored toward their four different SME types.

Thus, a cybersecurity standard needs to either

- 1. Include more organizational characteristics or
- 2. provide the flexibility for organizations to add their own relevant components

The artifact developed within this research proposes the second option. Components can easily be added or removed. Also, a practitioner of the standard can create their components or select components from the provided library. The participants of the GSS articulated the need for flexibility; thus, flexibility was considered in the design of the artifact instead of the more organizational characteristics.

Flexibility in organization

Literature confirms the need for flexibility for SMEs: from a strategic perspective, there is a positive relationship between strategic flexibility and SME performance. (Guo, H., & Cao, Z., 2004) The complexity and unpredictability of today's business climate necessitate increased adaptability for businesses to survive. Organizational adaptability is a sought-after competitive advantage in today's fast-paced and ever-changing environment. Although adaptability to environmental conditions is essential for SME survival, its development must be deliberate and supported by internal procedures. (Anning-Dorson, T, 2021). The artifact needs to be deliberate in its flexibility to ensure the same flexibility in managing cybersecurity risks.

Flexibility in risk

Flexibility also eases the risk assessment process component of the artifact. The person(s) performing the risk analysis is free to choose the level of abstraction. This flexibility simplifies finding risks and does not "lock" analysts to a single level of abstraction (such as identifying risks solely at the technical or business level). (Omerovic, A et al., 2019) Within the artifact, the flexibility in the risk assessment is expressed through the open nature of the standard to add risks, in any abstraction, that are relevant to the SME.

How does the artifact compare to the other solutions?

Three solutions are proposed in the literature. The first solution is a certification scheme that the University of Antwerp has developed, which is in the pilot phase. Their solution is an extensive checklist on which government-selected auditors audit an SME. (C. Ponsard et al., 2020) Second, a maturity evaluation tool has been developed based on NIST CSF. The framework uses maturity to compare to the SME industry and suggest improvements. (M. Benz & D. Chatterjee 2020). Third, a canvas is proposed, which should be treated like a checklist of components on which an SME needs to comply. (S. Teufel et al., 2020)

The primary difference between the artifact proposed in this thesis is the simplicity, flexibility, and the emphasis placed on risks. (Table 9) Moreover, the artifact also differentiates in its comparison to risks unrelated to cybersecurity and the collection of the context of the SME.

Solution	Strengths of the solution compared to the artifact	Strengths of the artifact compared to the solution	Reference
Certification scheme based on a checklist	 Potential government enforcement by design More rigid 	 Simpler Flexible More emphasis placed on risk 	C. Ponsard, et al, 2020
Evaluation tool	 Includes industry averages Least involvement required of experts 	SimplerFlexibleEmphasis placed on risk	M. Benz & D. Chatterjee 2020
Canvas	More rigid	SimplerFlexibleEmphasis placed on risk	S. Teufel, et al, 2020

Table 9, comparison between the artifact and solutions from literature

Checklist

The participants expressed that they want a checklist for SMEs. With the results of research and my expertise in my advice, a checklist.

- 1. Document the answer: "Why is cybersecurity relevant for the company?"
- 2. Document the most important risks to the organization. (Do not focus only on cybersecurity risks)
- 3. Document the most important cybersecurity risks.
- 4. Rent expertise to determine appropriate measures for those risks. Determine measures that fit those risks. Prefer measures that use protective technology or identity and access of users.
- 5. Plan bi-weekly, monthly, or quarterly meetings with the expert to adjust to changes and ensure progress. The timeframe depends on the level of risk and risk appetite of the SME.

Step 1 is the essential question that ensures support from the stakeholders. Also, if other risks are more critical to the objectives of the SME, then those should be considered above cybersecurity. "Risk is the effect of uncertainty on objectives" (ISO, 2018). Cybersecurity risks alike need to be measures compared to other risks. And only then will it make sense for stakeholders to initiate cybersecurity initiatives.

Step 2 ensures that the participant reflects on the company's risks other than the cybersecurity risks. The effect of uncertainty on an SME's mission and objectives may be considered an "enterprise risk" that must be similarly managed. (Stine, K, 2020).

Step 3 focuses on the cybersecurity risks. These risks need to be defined as the purpose of the cybersecurity initiatives is to reduce cybersecurity risks.

Step 4. Cybersecurity expertise needs to be brought into the SME to select the proper measures. Most SMEs do not have the expertise themselves. (PWC, 2021) Moreover, hiring a full-time professional is not needed. M. Benz and D. Chatterjee recommend 40 hours a year for low effort, 40-200 hours for medium, and over 200 hours for high effort (2020).

Step 5 ensures that cybersecurity efforts are being tracked and expertise is regularly brought into the company. Regular contact with an expert helps the SME stay informed regarding cybersecurity risks and solutions.

Limitations

The research has limitations; although the choice of limitations has been carefully considered during the research design process and the research, limitations persist.

The research is based on a limited set of experts: male experts from the Netherlands. This might pose a limitation because the outcome could be different when the study is conducted with a different group of people of different sexes, cultures, and countries. Also, the GSS session retrieved the participants' opinions from that point in time. Different results could be expected when the research is conducted one or more years later. Furthermore, the artifact itself is not verified after construction. Although, most participants expressed that they would use the artifact after its creation.

Secondly, the artifact's design is based on the categories of the NIST CSF. Although the standard was carefully considered and chosen, the framework might still be limiting. Third, because of the scope of the research, only the depth of the categories could be considered; further depth to the depth might be desirable. Finally, the GSS did not consider design questions because of the SDM approach. Other streams of design science recommend using design questions to discover the artifact's design.

Further research

The limitations posed multiple points for further research. The artifact should be verified on effectivity, preferably among a group of people different from the current participants of the research. Secondly, the perceived effectivity of the NIST CSF categories was varied and might need considerable extra data input to be conclusive. Third, other cybersecurity standards could be researched to find out if they fit within the frame of the artifact. Finally, one characteristic, the size of the organization (SME, employs max 250 people), could not be considered enough; other organization characteristics should be researched. Other organizational characteristics should be included as potential requirements of the artifact. Moreover, the more depth could be gained from researching the different SME types suggested by the European Digital SME Alliance (2020)

However, most importantly, research needs to be conducted to determine if implementing a cybersecurity standard would be desirable compared to the other challenges that SMEs already face. If a cybersecurity standard is desirable, further research could be conducted into the auditing and certification criteria of the cybersecurity standard.

Reflection

Writing a thesis was educational. Writing a thesis led me on a journey through different research methods and different scientific topics, which led to the discovery of new interests, such as system thinking and design science. Also, my ability to reason and write has improved drastically. With my improved ability to reason and write, I was armed in meaningful discussions where my opinion conflicted with the general opinion. As Aristotle's said, "A 'thesis' is a supposition of some eminent philosopher that conflicts with the general opinion." (Aristotle, W.D. Ross, J.A. Smith., 1928)

The process of writing was challenging because I am always prone to quick decisions and conclusions. This has led me far within my career, but also blocked me. The process of writing taught me to back up my conclusions and decisions and strengthen them.

Apart from the less I learned in the process, I must admit the flaws and the possibility for improvements.

- 1. I should have been more rigid in documenting the process of research and my conclusions and decisions made throughout the research.
- 2. Although the snowballing approach was great, I think the extent of my use of the method is flawed because it distracted me from the formulation of the central opinion. Instead, it led to a numb accusation of publications and reduced my motivation to continue the research.
- 3. More focus should have been placed on setting up a people for continual review and discussions. The lack of discussions and reviews has led to a waste of time and unnecessary obstacles within the thinking process.
- 4. My conclusions about the need for a cybersecurity standard were too quick. After reevaluating the artifact and the SMEs' problems, I realized that a new cybersecurity standard might not be the right solution.

On improvement number 4, SMEs' adoption of the cybersecurity standard and the enforcement of such a standard is still open for discussion. SMEs face multiple challenges, and cybersecurity risk is one of those challenges. However, cybersecurity risks might not be the most crucial challenge. SMEs face multiple challenges such as innovation and technology adaptation, inadequate budget, a lack of resources, difficulties in expanding the existing capacity, and lack of new knowledge utilization in developing new products. (H. K. Mustafa & S. Yaakub, 2018) The use of a cybersecurity standard might not be the right choice. Misjudging risks can have disastrous consequences, ranging from customer loss to damaging liability and possibly even bankruptcy (Hollman & Mohammad-Zadeh, 1984). Spending SME resources, who already lack resources, on cybersecurity might be one of those misjudgments.

Special Thanks to Barry Derksen, Yuri Bobbert and Hans Mulder. My promoter Barry Derksen for the direction and advice you gave me. Yuri Bobbert, for all the valuable insights and practical guidance. Moreover, Hans Mulder, for the valuable input you gave me on my design science approach.

References

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5.

Altman, E. I., Sabato, G., & Wilson, N. (2008). The Value of Non-Financial Information in SME Risk Management. In *https://papers.ssrn.com > SSRN_ID1466813_code451378https://papers.ssrn.com > SSRN_ID1466813_code451378*. https://doi.org/10.2139/ssrn.1320612

An introduction to the components of the Framework. (n.d.). NIST. Retrieved May 10, 2022, from https://www.nist.gov/cyberframework/online-learning/components-framework

Anning-Dorson, T. (2021). Organizational culture and leadership as antecedents to organizational flexibility: implications for SME competitiveness. Journal of Entrepreneurship in Emerging Economies, 13(5), 1309–1325.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1* (2), 219–238.

Aristotle, W.D. Ross, J.A. Smith. (1928). The works of Aristotle - Volume 1. Oxford : Clarendon Press.

Asare, R., Akuffobea, M., Quaye, W., & Atta-Antwi, K. (2015). Characteristics of micro, small and medium enterprises in Ghana: gender and implications for economic growth. *African Journal of Science Technology Innovation and Development*, *7* (1), 26–35.

awal street journal. (2015, November 1). *Systems Thinking Speech by Dr. Russell Ackoff*. Youtube. https://youtu.be/EbLh7rZ3rhU?t=3610

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systemes D'information Management*, *22* (3), 7–45.

Baskerville, R., Pries-Heje, J., & Venable, J. (2009). *Soft design science methodology*. https://doi.org/10.1145/1555619.1555631

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons, 63(4), 531–540.

Burgstaller, J., & Wagner, E. (2015). How do family ownership and founder management affect capital structure decisions and adjustment of SMEs? *Journal of Risk Finance*, *16* (1), 73–101.

C. Cronin, HALOCK Security Labs, J. Mirochnik, T. Kurzynski, and Da. Andrew, E. Leach, S. Lawn, P. Otto, Hogan Lovells US LLP. (2018). *CIS RAM Version 1.0*.

Carsa:carsa, N. A., Econ, N. A. D., corporate-body. EASME:Executive Agency for Small, Medium-sized Enterprises, LE Europe:LE Europe, N. A., & PwC:PwC, N. A. (2021). *Annual report on European SMEs 2020/2021 : digitalisation of SMEs^{*}. Publications Office of the European Union.

Checkland, P. (2000). *Systems Thinking, Systems Practice*

Dictionaries, O. L. (n.d.-a). *Holistic*. Retrieved May 4, 2022, from https://www.oxfordlearnersdictionaries.com/definition/english/holistic?q=holistic Dictionaries, O. L. (n.d.-b). *Standard*. Retrieved May 3, 2022, from https://www.oxfordlearnersdictionaries.com/definition/english/standard_1?q=standard

European Commission. (n.d.). *SME definition*. Internal Market, Industry, Entrepreneurship and SMEs. Retrieved December 29, 2021, from https://ec.europa.eu/growth/smes/sme-definition_en

Europian Digital SME Alliance. (2020). *The EU Cybersecurity Act and the role of standards for SMEs*. https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf

Fang, F. C., & Casadevall, A. (2011). Reductionistic and holistic science. *Infection and Immunity*, *79*(4), 1401–1404. Scarfone, K. A., Benigni, D. R., & Grance, T. (n.d.). *Cyber Security Standards*. Retrieved May 3, 2022, from https://www.nist.gov/publications/cyber-security-standards

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23.

Fielding, L. M., Ellis, L., Beveridge, C., & Peters, A. C. (2005). An evaluation of HACCP implementation status in UK small and medium enterprises in food manufacturing. International Journal of Environmental Health Research, 15 (2), 117–126.

Grima, S., Hamarat, B., Özen, E., Girlando, A., & Dalli-Gonzi, R. (2021). The Relationship between Risk Perception and Risk Definition and Risk-Addressing Behaviour during the Early COVID-19 Stages. *Journal of Risk and Financial Management*, *14* (6), 272.

Gundu, T. (2019, May 13). Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity Compliance. *International Conference on Cyber Warfare and Security*. http://dx.doi.org/

Guo, H., & Cao, Z. (2014). Strategic flexibility and SME performance in an emerging economy A contingency perspective. Journal of Organizational Change Management, 27(2), 273–298.

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.

Hevner, S., & March, J. (2004). Design Science Research in Information Systems. Management Information Systems Quarterly, 28(1), 75–105.

Hollman K.W., & Mohammad-Zadeh S.(1984) Risk management in small business. J. Small Bus. Manag., vol. 1, pp. 47–55, 1984.

Information security and privacy standards for SMEs. (2015, December 14). ENISA. https://www.enisa.europa.eu/publications/standardisation-for-smes

Information Security Forum Limited. (2017). The Next Generation of Assessing Information Risk.

ISC2. (2019). *Cybersecurity workforce study*

ISO. (2018). ISO 31000:2018(en) Risk management. Iso. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Iso/iec 27001*. (2020). ISO. https://www.iso.org/isoiec-27001-information-security.html

Jack Freund, J. J. (2015). *Book PDF Measuring and managing Information Risk - A FAIR approach*. Elsevier.

Jack Freund, J. J. (2015). Measuring and managing Information Risk - A FAIR approach. Elsevier.

Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *2017 International Conference on Communication Technologies (ComTech)*, 78–90.

K. W. Hollman and S. Mohammad-Zadeh, "Risk management in small business," J. Small Bus. Manag., vol. 1, pp. 47–55, 1984.

Kaya, D., & Koch, M. (2015). Countries' adoption of the International Financial Reporting Standard for Small and Medium-sized Entities (IFRS for SMEs) – early empirical evidence. Accounting and Business Research, 45 (1), 93–120.

Kuhn, T. S. (2018). The Structure of Scientific Revolutions. In *Oxford Scholarship Online*. https://doi.org/10.1093/oso/9780190851408.003.0003

Lancaster University Management School. (2012, April 30). *Peter Checkland on the origins of SSM*. Youtube. https://www.youtube.com/watch?v=XA2i1n-o9L0

Lavia Lopez, O. and Hiebl, M.R.W. (2014), "Management Accounting in Small and Mediumsized Enterprises: Current Knowledge and Avenues for Further Research", Journal of

Management Accounting Research, in press, doi: 10.2308/jmar-50915.

McNiff, J. (2013). *Action research: Principles and practice*. https://www.taylorfrancis.com/books/mono/10.4324/9780203112755/action-researchjean-mcniff

Miller, G. (2016, October 23). 60% of small companies that suffer a cyber attack are out of business within six months. *The Denver Post*. https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

Miller, K. D. (1992). A Framework for Integrated Risk Management in International Business.

Journal of International Business Studies^{*}, *23*(2), 311–331.

Munro, D. 2013. A Guide to Financing SMEs. New York: Palgrave Macmillan.

Mustafa, H. K., & Yaakub, S. (2018). Innovation and technology adoption challenges: impact on SMEs' company performance. *International Journal of Accounting, Auditing and Peformance Evaluation*, *3* (15), 57–65.

Naradda Gamage, S. K., Ekanayake, E. M. S., Abeyrathne, G., Prasanna, R., Jayasundara, J., & Rajapakshe, P. S. K. (2020). A Review of Global Challenges and Survival Strategies of Small and Medium Enterprises (SMEs). *Economies et Societes*, *8*(4), 79.

Narteh, B. (2008). Knowledge transfer in developed-developing country interfirm collaborations: a conceptual framework. *Journal of Knowledge Management*, *12* (1), 78–91.

National Institute of Standards and Technology. (2016). Introduction to the Framework for Improving Critical Infrastructure Cybersecurity. In *Securing an IT Organization through Governance, Risk Management, and Audit* (pp. 60–83). https://doi.org/10.1201/b19194-8

National Institute of Standards and Technology. (2016). Introduction to the Framework for Improving Critical Infrastructure Cybersecurity. In *Securing an IT Organization through Governance, Risk Management, and Audit* (pp. 60–83). https://doi.org/10.1201/b19194-8

NIST. (2012). Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Nugroho, M. A., Susilo, A. Z., Fajar, M. A., & Rahmawati, D. (2017). Exploratory Study of SMEs Technology Adoption Readiness Factors. *Procedia Computer Science*, *124* , 329–336.

Omerovic, A., Vefsnmo, H., Erdogan, G., Gjerde, O., Gramme, E., & Simonsen, S. (2019). A Feasibility Study of a Method for Identification and Modelling of Cybersecurity Risks in the Context of Smart Power Grid. SciTePress.

Organizational cyber maturity: A survey of industries. (2021, August 2). McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries

Pickard, A. J. (2013). *Research Methods in Information*. Facet Publishing.

Ponsard, C., Massonet, P., Grandclaudon, J., & Point, N. (2020). From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 75–78.

Proença, D., & Borbinha, J. (2018). Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. In *Business Information Systems* (pp. 102–114). unknown.

Quayle, M., & Christiansen, J. K. (2004). *Quayle and Christiansen: E-Commerce Adoption in UK and Denmark SMEs*. unknown.

Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the Unbearability of Uncertainty. 2016 Cybersecurity and Cyberforensics Conference (CCC)*, 137–143.

Scarfone, K. A., Benigni, D. R., & Grance, T. (2009). *Cyber Security Standards*. https://www.nist.gov/publications/cyber-security-standards

A cybersecurity standard for SME – Vincent van Dijk

Scarfone, K. A., Benigni, D. R., & Grance, T. (n.d.). *Cyber Security Standards*. Retrieved May 3, 2022, from https://www.nist.gov/publications/cyber-security-standards

Şener, S., Savrul, M., & Aydın, O. (2014). Structure of Small and Medium-Sized Enterprises in Turkey and Global Competitiveness Strategies. *Procedia - Social and Behavioral Sciences*, *150*, 212–221.

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). Integrating cybersecurity and enterprise risk management (ERM). National Institute of Standards and Technology. <u>https://doi.org/10.6028/nist.ir.8286</u>

Taylor, E., & Kane, K. (2005). Reducing the burden of HACCP on SMEs. Food Control , 16 (10), 833–839.

Teufel, S., Teufel, B., Aldabbas, M., & Nguyen, M. (2020). Cyber Security Canvas for SMEs. Information and Cyber Security, 20–33.

Tse, T., & Soufani, K. (2003). Business strategies for small firms in the new economy. Journal of Small Business and Enterprise Development^{*}, *10^{*} (3), 306–320.

van Amerongen, J. (2021, August 28). *Ransomware raakt kleine ondernemers keihard: "Ik zie bedrijven kapot gaan."* RTL Nieuws.

https://www.rtlnieuws.nl/tech/artikel/5250115/ransomware-mkb-nederland-ondernemers-cybercrime

Verizon: 2021 data breach investigations report (Vol. 2021, p. 4). (2021). Verizon. https://doi.org/10.1016/s1361-3723(21)00061-0

Weigand, H., Johannesson, P., & Andersson, B. (2021). An artifact ontology for design science research. *Data & Knowledge Engineering*, *133*, 101878.

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering* (2014th ed.). Springer.

Appendix

A. Version Control

Date	Status / Change	Actioned by
22 Nov 2021	Draft	Barry Derksen
31 Jan 2022	Draft	Barry Derksen en Hans Mulder
20 April 2022	Draft	Barry Derksen
29 April 2022	First version for go-no	Yuri Bobbert
5 May 2022	Major changes toward on the document, such as, problem statement, findings, conclusions, reflection.	Yuri Bobbert
12 May	Improvement on the SME definition and conclusion	Yuri Bobbert
13 May	Improvement on problem, conclusion, and introduction	Ad Krikke

B. Questions for GSS

Questions about the participant

The questions listed below are meant to determine the experience of the participant. The experience can later be correlated to the answers to the later questions.

Question: How long do you have in-field experience with cybersecurity?

- 1. Less than three years
- 2. More than three years
- 3. More than five years
- 4. More than ten years

Question: For how many years did you work for an organization that is less than 250 employees?

- 1. Less than 3 years
- 2. More than 3 years
- 3. More than 5 years
- 4. More than 10 years

Risk Management process

The questions are based on the four tiers defined in the NIST Cybersecurity Framework (CSF). The goal of these questions is to determine the desired level of risk management of a SME

Questions:

- 1. What is the desired risk management process for a SME?
 - a. The risk management process is not formalized, and risk are managed in a reactive matter
 - b. Management has approved the risk management processes, but there might not be an organizational wide policy.
 - c. The organization's risk management practices are formally approved, expressed as policy and regularly updated
 - d. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.
- 2. What is the desired integration of risk management for an SME?
 - a. Risk management is not integrated into the organization
 - b. Within the organization cybersecurity is shared on an informal basis; cybersecurity is considered is typically not repeatable or reoccurring.
 - c. There is an organization-wide approach to manage cybersecurity risk where senior executives ensure consideration of cybersecurity through all lines of operation in the organization
 - d. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events
- 3. What is the desired level of participation of an SME should have in the larger ecosystem?
 - a. The organization does not understand it's role in the larger ecosystem of risk management.
 - b. The organization has a limited understanding of its role in the larger ecosystem. The organization is aware of the risks in the supply chain but does not act formally upon those risks
 - c. The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks
 - d. The organization shares risk information from the community

Obstacles for the adoption of standards

The goal of these questions is to figure out what hurdles SMEs to adopt a cybersecurity standard. The question is based on "The EU Cybersecurity Act and the Role of Standards for SME" (European Digital SME Alliance, 2020, p9).

Question: What is the biggest hurdle for the adoption of cybersecurity standards? (Divide 100 points to the most important obstacles for adoption)

- Free access to standards
- Implementation costs of standards
- Tailoring/adapting standards: Some standards are not very practical nor useful, nor easy to apply for SMEs.
- Language translation and adaptation is rare for specific technical standards.
- There is a lack of simple or easy cybersecurity solutions or guides.
- Lack of technical solutions
- Awareness about the existence of standards
- The awareness of how standards add business value is limited.
- There are misconceptions about the complexity of standards and unfair market regulations
- Standards are often hard to understand for SMEs which do not have the inhouse expertise for translating standards into specific tasks and activities.
- SMEs that have outsourced the ICT function may suffer from limited internal knowledge about cyber threats.
- Lack of resources
- The design of standards is mainly driven by large companies, which have different requirements

Selection of categories

The following categories are based on the NIST CSF. The goal of these questions is to determine the categories that are relevant for a cybersecurity framework for SME.

Question: What effectiveness of the category? (Rate 1 to 5)

- 1) Asset management
- 2) Business environment (determine the business environment of the SME)
- 3) Governance
- 4) Risk assessment
- 5) Risk management strategy
- 6) Supply chain risk management
- 7) Identify management and access control
- 8) Awareness and training
- 9) Data security
- 10)Information protection processes and procedures
- 11)Maintenance (Maintenance and repairs of information system components are performed consistent with policies and procedures.)
- 12)Protective technology
- 13) Anomalies and Events Security Continuous Monitoring
- 14) Detection processes
- 15)Incident response

Question: How complex is the implementation and maintenance of the category? (Rate 1 to 5)

- Asset management
- Business environment (determine the business environment of the SME)
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management
- Identify management and access control
- Awareness and training
- Data security
- Information protection processes and procedures
- Maintenance (Maintenance and repairs of information system components are performed consistent with policies and procedures.)
- Protective technology
- Anomalies and Events Security Continuous Monitoring
- Detection processes
- Incident response

Artifact

The artifact questions aim to extract specific requirements for the artifact.

Question: Who should the framework be made for? (eg. CIO, CEO or consultants etc.)

Question: How should the framework be presented? (As a self- assessment application, a document, an infographic, etc.)

Question: If this SME oriented Framework would come available, would you advise it to an SME?

Question: What would you like to add.... (This questions captures free format data regarding the artifact)