



**DESIGNING A CYBER RISK
ASSESSMENT TOOL FOR
SMALL TO MEDIUM
ENTERPRISES**

RUBEN KOEZE
DELFT UNIVERSITY OF TECHNOLOGY

Ruben Koeze
Delft University of Technology
Faculty of Technology, Policy and Management
Research conducted at KPMG Advisory N.V.
November 2017
Electronic version available at <http://repository.tudelft.nl>



Designing a cyber risk assessment tool for small to medium enterprises

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in Systems Engineering, Policy Analysis and Management

Faculty of Technology, Policy and Management

by

Ruben Koeze

Student number: 4107810

To be defended in public on November 22nd 2017

Graduation committee

Chairperson : Prof. Dr. Ir. P. van Gelder, section Safety and Security Science
First Supervisor : Dr. Ir. W. Pieters, section Safety and Security Science
Second Supervisor : Dr. M.V. Dignum, section Policy and Management
External Supervisor : I. de Wit, MSc, KPMG

PREFACE

Ok, well, this is it.

It was supposed to take five years, but I took me a little over two years more. I am of course talking about my study Systems Engineering, Policy Analysis and Management (I still cannot fully explain what that means). Because you are reading this, you probably know what it is that you are reading, but just to make sure: this is the last part of the puzzle: my master's thesis. I can honestly say that I have never put this much work in anything school related, and while that sounds like I have done a lot of work over the last 8 months, this is not actually the case. As some people might know, I am hard to motivate for anything that is school related, which resulted in me doing way too little work in the first months. This gave some people quite some headaches (but more on that later) and it resulted in me doing quite the "eindsprint" as it is called in Dutch. Now that my thesis is finished, I can say that the work that I have produced is something that I can be quite proud of, maybe I have even learned some things in the process.

First my gratitude goes out to Wolter Pieters, who guided me through the whole process of this research. While I can imagine that I was not the ideal person to work with in these months, Wolter always was of great help; helping me in forming the subject and research questions, always prepared to answer questions and using just enough of pressure to keep me working.

Secondly I want to thank KPMG, especially Ivan de Wit, in helping me with this research. Ivan always did his utmost best in supporting me, giving suggestions for the path to take and of course supporting me in the feedback sessions in Delft.

Of course I want to thank Simone for her support in finishing this thesis, or my study for that matter, I know that you have had more stress and headaches because of my laziness. Even in these less immaculate moments you have always supported me.

Last but not least, I want to thank my parents for supporting me throughout my "study career". While I know it was not easy for them, my strategy of keeping them in the dark most of the times payed off in the end. Not showing the struggles in the process, but only the end result saved them a lot of stress as well.

Ruben Koeze

Rotterdam, November 2017

SUMMARY

Internet usage is on the rise, not only with personal use, but also in the business sector. This means that more people everyday use a computer (with internet) for their daily work activities. This daily use of computers and internet gives us a lot of advantages, but also lots of risks. With cybercrime on the rise, these risks become more evident on a daily basis. However, research shows us that small to medium enterprise (SMEs) do too little or even nothing in order to protect themselves from the cyber threats that exist. The conclusions from surveys and existing literature are that SMEs do not think that such a threat will be relevant for them, while this is proofed not to be the case. On the other hand, companies indicate that they think about the threats, and they admit that something should change, but they do not have the time, knowledge and resources to improve on their cybersecurity. There is no clear method or tool to help SMEs in doing their risk assessments. The frameworks and assessments that exist are not suited for SMEs due to the abovementioned constraints. For this reason, the main research question is:

What would a tool look like that helps SMEs do cyber-risk assessments and point out the weaknesses in their cybersecurity?

The following sub-questions, in support of the main research question, are defined:

1. What are the most commonly used cybersecurity frameworks and risk assessments?
2. What does the existing literature say about cybersecurity for SMEs?
3. How can existing frameworks and assessment methods be tailored for SMEs?
4. What are the design requirements for a tool to do cybersecurity risk assessments specific for SMEs?
5. How can the tool be built?
6. Does the tool meet the requirements of SMEs?

The first three sub questions will be answered on the base of a literature research. The last three sub questions will be answered by combining the Design Science method with an agile development method. Requirements will be determined based on literature and interviews. The validation will also be done based on interviews and an expert session.

First the most commonly used cybersecurity frameworks are reviewed. This is done on the basis of a research which indicates three most used frameworks: The NIST framework for Improving Critical Infrastructure Cybersecurity, the ISO27001 standard and the CIS Critical Security Controls for Effective Cyber Defense. All these frameworks have the same property: they need to be used by people that have knowledge of cybersecurity. Something that is not the case in most SMEs, thus rendering these frameworks more or less useless for SMEs to use.

Secondly the most suited cybersecurity risk assessments for SMEs are reviewed. Also selected on the basis of a research, in which the most common risk assessment methods are selected. Based on this selection, the three risk assessment methods that are covered are CORAS, NIST SP800-30 and TRESPASS. Looking at these three methods, they all give similar problems when SMEs will apply them. The methods require SMEs to estimate their own risks. This is not realistic, as most SMEs do not have the required knowledge about cybersecurity to do these estimations. Therefore, the covered methods are not suited for SMEs to use.

Looking at what the existing literature says about cybersecurity for SMEs, there is a clear common theme in the published articles: there is no clear cybersecurity approach for SMEs. The articles mention that some controls that can be found in the literature can be used by SMEs, but this also requires knowledge of the implementation of these controls. With regards to doing an assessment of the current status of cybersecurity of a company, the literature does not give clear solutions, most of the articles only state that there is no clear solution for SMEs.

Concluding from the existing literature, it is clear that there is no suited method for SMEs. To overcome this problem, a model is created in order to suit the constraints that SMEs have. For this reason, the TRESPASS model is adapted and slimmed down in order to fit the needs of SMEs. The model consists of different components: actors, devices, assets and policies. These components are elements that are part of the company. For example an actor can use a laptop (device) in order to get to the credit card data (asset) that is stored within the company. There are certain probabilities that the device or the actor will be breached, and thus the credit card data can be accessed. To lower this probability, the company can apply policies with regards to the device or the actor. This can be for example the policy that the laptop will patch security updates every month; drastically reducing the probability that it will be breached. The breach probabilities for every component will be determined by experts and stored in a knowledge base, thus overcoming the issue that SMEs do not have specific cybersecurity knowledge. The calculations of the probabilities will be done using the Gordon-Loeb model, in order to take the effect of diminishing marginal return on cybersecurity investments into account. This essentially means that every extra policy on a component will have less effect on improving that probability than the previous one.

Implementing this model in a tool that is suited for SMEs required determining the requirements for this tool. These requirements were initially set by using literature, but were later validated and further extended by interviewing a SME. An important requirement that came out of these sessions was that a visual representation of the structure of a company could help in doing this risk assessment. This is perfectly in line with the model that is created, as the components of the model can be visualized in the tool.

To validate this model and requirements that were set, an interview with a security office at a SME and an expert session with information security consultants was held. These sessions confirm that the model as such will work, but might be oversimplified. Both sessions indicate that the model could be extended with extra components or extra factors working on the model. Concerning the requirements of the tool, not all of the requirements could be validated, as they were not confirmed by either the interview or the expert session. However, most of the requirements that were determined, were indeed discussed and approved on by the sessions.

The determined requirements in combination with the model suited for SMEs make for a tool that is both easy in use, clear in the results and accurate enough to show the vulnerabilities for a SME. While the tool is not the same as an extensive audit by an external consultant, it is something that can help SMEs in a first checkup on their cybersecurity status without specific knowledge and a lot of investments needed.

TABLE OF CONTENTS

Preface	4
Summary	5
List of figures.....	9
List of tables.....	10
Introduction	11
Small and Medium-sized enterprises	11
Cyberattacks on SMEs.....	11
Research questions.....	13
Scientific relevance	13
Societal relevance	13
Methodology	15
Literature review	15
Design science.....	15
Agile software development.....	16
Requirements engineering	17
Requirements prioritization.....	19
Requirements modelling.....	19
Cybersecurity frameworks.....	20
NIST Framework for Improving Critical Infrastructure Cybersecurity	20
ISO27001 standard	22
The CIS Critical Security Controls for Effective Cyber Defense	23
Conclusion.....	24
Cybersecurity risk assessments	25
CORAS	26
NIST SP800-30.....	27
TRESPASS.....	28
Conclusion.....	29
Cybersecurity for SMEs.....	30
Background	30
Frameworks fitted for SMEs	32
Frameworks	34
Conclusion.....	34
Modeling and calculating the risk.....	36
Elements in the model.....	36
Structure of the model	38

Calculating the risk.....	39
Determining the rules.....	46
Development of the tool.....	47
First development sprint.....	47
Second development sprint.....	51
Design implementation.....	54
Validation.....	57
Extracting findings.....	57
Validating the requirements.....	58
Validation of the model.....	59
Conclusion.....	59
Synthesis.....	60
Conclusions.....	60
Discussion.....	62
Limitations.....	63
Recommendations and future work.....	64
References.....	65
Appendix A – Literature research.....	68
Appendix B – Requirements Prioritization Sprint 1.....	69
Appendix C – Requirements Prioritization Sprint 2.....	71
Appendix D – Interview guide.....	72
Appendix E – Summary first interview.....	74
Appendix F – Summary second interview.....	75
Appendix G – Summary expert session.....	76
Appendix H – Rules from expert session.....	77
Different devices.....	77
Rules on devices.....	77
Rules on actors.....	77

LIST OF FIGURES

Figure 1 - Design Science framework.....	16
Figure 2 - Workflow	17
Figure 3 - CORAS steps.....	26
Figure 4 - Example CORAS threat diagram	27
Figure 5 - Connections between different components.....	38
Figure 6 - Influence of policies on devices and actors	39
Figure 7 - Attack tree example [49]	39
Figure 8 - Translate model to diagram for probabilities.....	41
Figure 9 – Diminishing marginal returns effect of number of policies	44
Figure 10 - Impact on breach probability.....	45
Figure 11 – First goal sketch	47
Figure 12 – Further defined goal sketched based on literature	48
Figure 13 - Login page mockup	50
Figure 14 - Overview page mockup	50
Figure 15 - Visual Assessment blocks.....	50
Figure 16 - Goal modelling sprint 2.....	52
Figure 17 - Assessment wizard mockup.....	53
Figure 18 - Risks in visual assessment mockup.....	53
Figure 19 - Numbered risks in visual assessment mockup	53
Figure 20 - Complete modelling overview	55
Figure 21 - Partial modelling overview	55
Figure 22 - Complete risk assessment overview.....	56
Figure 23 - Partial risk assessment overview	56
Figure 24 - Ranked visualization of risks.....	56

LIST OF TABLES

Table 1 - Findings from literature	12
Table 2 - NIST Framework Structure	21
Table 3 - Different component TRESPASS [38].....	29
Table 4 - Worksheet information types.....	33
Table 5 - Different component TRESPASS [38].....	36
Table 6 - TRESPASS modeling components fitted to the real world [38].....	36
Table 7 - User input conversion	42
Table 8 - Risk names and corresponding colors.....	42
Table 9 - Policy rules in table form	46
Table 10 - Goal modelling sprint 2.....	49
Table 11 - Weights for prioritization.....	49
Table 12 - Weighted scores.....	49
Table 13 – Final prioritization	49
Table 14 - Findings from interview	51
Table 15 - Goal modelling sprint 2 - Overview.....	52
Table 16 - Weighted scores sprint 2	53
Table 17 – Final prioritization sprint 2.....	53
Table 18 - Policies database schema	54
Table 19 - Population of the policies schema	55
Table 20 - Validation of requirements.....	59
Table 21 - Final requirements	62

INTRODUCTION

The penetration of internet in the Netherlands is at an all-time high, with only 8 percent of the population never using the internet [1]. While the Netherlands is one of the front-runners in the penetration of the internet, the rest of the European Union is not far behind. Within the whole of the European Union, the internet usage is at 82% for people between 16 and 74 years old [2].

With the rise of the internet come threats via the internet. These attacks can vary from installing malware that shows ads, stealing critical company information or bringing down ICT infrastructure. While these attacks can be aimed at the individual, they can also be aimed at companies. Everything concerning the prevention and response of and to these attacks is called cybersecurity. While this topic is also on the rise, as can be seen in Google Trends [3], it still remains a neglected subject for a lot of people, but especially for companies.

With a lack of cybersecurity, a lot of issues can arise. The causes of these issues come with different likelihoods and impacts. By using risk management, the costs of risks “firing” can be minimized. Risk management as defined by Cambridge University: “*the activity of calculating and reducing risk, so that an organization does not fail or lose money*” [4]. The first part of this definition is the calculation of the risk. This calculation is done by doing a risk assessment. A risk assessment is the basis for risk management and although it can be applied in many sectors, it is also essential for cybersecurity [5, 6].

Small and Medium-sized enterprises

The focus of this research will lie on Small and Medium-sized Enterprises, or SMEs. For this research the definition used for a SME is that the company may have a maximum of 250 employees or a maximum turnover of 50 million euros. The focus on SMEs is chosen because of the big part of the economy they represent and because the state of their cybersecurity. In the Netherlands, SMEs are a big part of the national economy. According to the *Centraal Bureau voor Statistiek* SMEs make up more than 60% of the Gross Domestic Product and provide 70% of the employment opportunities in the Netherlands [7]. According to Eurostat, SMEs provide for 99% of the jobs within the European Union [8].

As the internet usage rises, this is also the case for the internet usage within companies. In 2014, 55% to 60% of all SME employees used internet for their daily work activities. [9]. The definition used for a SME is that the company may have a maximum of 250 employees or a maximum turnover of 50 million euros. The number for internet usage may not seem that high of a number, but when looking at the different sectors, the usage percentage goes up for some sectors and down for others. For example, in the financial sector the internet usage is 100% percent, but in the construction sector this percentage drops to 45%. This means that everyone in SMEs working in the financial sector use internet for their job, but in construction less than half of the employees need internet for their daily activities.

Cyberattacks on SMEs

Over 25% of the SMEs in the Netherlands were victim of a cybercrime [10]. In a research conducted in the United Kingdom, it came to light that almost 60% of the small businesses had experienced a breach [11]. What

does this mean for such an SME? In a research conducted by Experian, the average costs vary from 10.000 euros to 250.000 euros [12]. This could have a huge impact on the operations of a SME. For some SMEs this would actually mean the bankruptcy of the business.

While the threat of being breached by a cyber-attack is real, the awareness is low [9, 11], this has as a result that the measures taken to prevent or lower the risk of a cyber-attack being successful are small. These measures to minimize the risk of a breach happening, or even preventing that a breach can happen all together, is what is called cybersecurity. These measures can vary from creating awareness on the risks of cyber threats in the company, training employees to prevent them from falling for tricks, installing software and hardware or hiring an external company to monitor internet traffic to look for suspicious behavior.

In a research conducted by Capgemini and TNS Nipo, only 35% of the SMEs did pay attention to cybersecurity once in a while [9]. This is also confirmed by research by the NCSC [13]. This is no surprise when looking at the percentage of SMEs that think that it is very unlikely that they will be the target of an attack. More than half of the SMEs thought that it is very unlikely that they will become the target of a cyber-attack, mainly due to an underestimation of their asset value [11]. This might explain why SMEs do not take measures, even though, when asked, they are aware of the fact that they are not well protected and prepared against a possible cyber-attack [14]. Only 14% of the SMEs rate their ability to mitigate cyber risks above 6 on a scale from 1 to 10 [15]. One of the reasons that SMEs do not pay much attention to cybersecurity is the thought that they do not have high value assets for attackers [11, 16]. However, different researches found other reasons for this lack of security. Other reasons are: lack of investments in cybersecurity [15, 17], a lack of in-house expertise [18] and limited resources [18]. While companies often have IT staff, they are not specialized or focused on cybersecurity. But what is important to notice is that with limited resources and small measures, big results can be achieved [9].

With the realization that small measures can have a big impact in the cybersecurity of a company, the risk of a successful attack will go down. Showing SMEs where the biggest risks for their company lie and showing them what measures can mitigate those risks can help in the understanding of cybersecurity.

FINDINGS FROM LITERATURE

In the parts of this research that are supported by literature, the different findings are numbered and summarized at the end of each paragraph or chapter. Using this structure, the literature supporting different findings can be easily referenced to in the requirements engineering part.

#	Finding	Literature
F1	Awareness for cybersecurity under SMEs is low	[9, 11, 16]
F2	Lack of investments (time and money)	[15, 17, 18]
F3	To little expertise	[18]

Table 1 - Findings from literature

Research questions

Based on the existing literature, no tool is suited for helping SMEs in doing a cyber-risk assessment without creating a lot of overhead. Therefore a research is proposed to fill this knowledge gap. This research will be done by answering the main question:

What would a tool look like that helps SMEs do cyber-risk assessments and point out the weaknesses in their cybersecurity?

With the help of multiple sub questions this main question will be answered. The following sub questions are defined:

1. What are the most commonly used cybersecurity frameworks and risk assessments?
2. What does the existing literature say about cybersecurity for SMEs?
3. How can existing frameworks and assessment methods be tailored for SMEs?
4. What are the design requirements for a tool to do cybersecurity risk assessments specific for SMEs?
5. How can the tool be built?
6. Does the tool meet the requirements of SMEs?

Scientific relevance

The scientific relevance will lie in the results that come from the design science approach. By using this approach the aspects that are relevant for designing for a SME become clear. These aspects can be of value for further or other research concerning SMEs, in particular in the cybersecurity sector.

As stated in the knowledge gap, there is a fundamental change necessary in the way SMEs approach their cybersecurity [19]. This change can be established by creating the proposed tool. By creating a low threshold, both in time and resources, for SMEs to do a cyber risk assessment in a way that can be understood by the management of such a company, the way SMEs will look at cybersecurity can fundamentally change.

Finally, the need for such an assessment tool was endorsed by the SANS institute, leading in information security training [20]. The process steps needed for implementing ISO27001 standards into SMEs are described, however, an assessment tool specific for SMEs would ease this process and ensure an easier implementation.

Societal relevance

As stated, SMEs make up a large part of the Dutch gross domestic product and employment opportunities [7]. With SMEs being better prepared for cyberattacks, and thus bringing down the number of successful attacks, the amount of money these businesses need to spend on handling and recovering from the breach will go down. This saves them one of the issues they have to cope with, besides competing with the big corporate companies. Alongside with the economic improvement, the improvement will also have effect for the security and privacy of data processed by SMEs. With improved security, personal data from civilians a SME might process is better protected.

STAKEHOLDERS

The proposed tool will have an impact on multiple stakeholders. First of all of course the SMEs which are the main stakeholder. The tool is meant for them and thus should meet their requirements. While the tool will be designed for SMEs to improve their cybersecurity with limited knowledge and resources, the awareness is very low among SMEs. So while the effects of this research and tool are merely positive for SMEs, the awareness of the need for such a tool might be low. This might pose a problem with the eventual adoption rate of the tool among SMEs.

Another stakeholder in this matter is the Dutch government. In a report drafted by the Dutch Cyber Security Council the advice is that the Dutch government should be leading in the cybersecurity efforts in the Netherlands [21]. With 60% of the GDP of the Netherlands, SMEs are a major player in the Dutch economy. This research will thus be of importance for the Dutch government in creating a strategy to get SMEs to improve their cybersecurity.

I will be conducting this research at KPMG, thus they are a stakeholder as well. While the focus of KPMG mainly lies on businesses bigger than SMEs, they have shown interest in facilitating SMEs with cybersecurity services. At this point KPMG lack the right tools and knowledge for giving fitting advice to SMEs that is also within the resources of those SMEs, but this research can be a first step in creating this knowledge, and of course also a tool to use.

METHODOLOGY

In order to answer the abovementioned questions, different methods are required. In this chapter, the research method for each of the sub questions will be explained.

Literature review

Sub question one, two and three will be answered by the means of a literature study. Searches for existing literature will be conducted by the use of Google Scholar, Scopus and Web of Science. A sample of the keywords, or combination, used will be: cybersecurity, framework, SME, risk assessment, cyber risk. In the found literature, the references can be used for further exploration of the subject.

Design science

The main deliverable for the proposed research is a tool. This tool shall be built based on the principles proposed by the design science theory by Hevner [22]. The theory by Hevner consists of three parts. The environment, the knowledge base and the IS research. The environment can be seen as the problem space. Within this space, everything that defines the problem that creates the urge for the to be designed artifact is present.

The knowledge base is the existing literature that defines frameworks, theories, methods and everything that is relevant for the research. Knowledge can be extracted from the knowledge base, but the research will also provide new additions to it.

The last part, as can be seen in the center of Figure 1, is the IS research. This research is done with the input from the environment and the knowledge base. In this part the actual building of the artifact is done by using all knowledge and then evaluating the artifact, also using knowledge from both the environment and the knowledge base. This is a repeating process in which the artifact is built, evaluated and then changed on the basis of what the evaluation concludes.

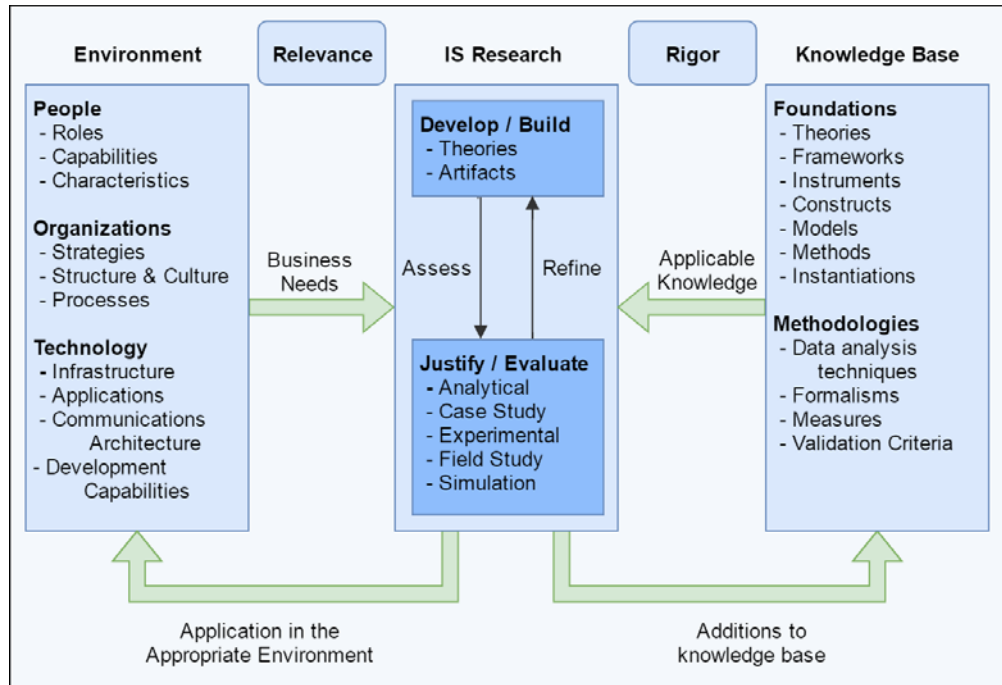


Figure 1 - Design Science framework

Agile software development

An extension to this design science research is the structure of developing; the center part of Figure 1. There are different development approaches to tackle such a project. In general there are two different approaches, traditional and agile. Both of these approaches have pros and cons concerning different kinds of projects. In a comparison made by Stoica, Mircea and Ghilic-Micu [23], the main differences are listed. As described, an agile development approach is more suitable for small to medium scale projects, requirements are emergent with rapid changes and the primary objective is quick value. The deliverable of this thesis can be seen as all those things, as the scale of the project is small and the objective is to get a working proof of concept; not a safely tested and robust solution.

Concerning the requirements, while most projects assume that there is a customer that works closely together with the development team, this is not the case for this project. While this project has a target group of SMEs, there are no SMEs continuously connected to this project. This makes the gathering of requirements harder, as there is no returning contact with the “customer”.

AGILE METHOD

There are multiple agile methods available, the most used approaches to agile developing are SCRUM, Extreme Programming (XP) and Kanban. The problem with these methods is the scale on which they operate. All of these approaches assume that the work is being done in teams. In SCRUM this results in different roles for different people in a team. In Extreme Programming one of the practices is that programming has to be done in couples, ensuring that code is reviewed by at least one person. For this reason, it is not wise to adopt a

complete methodology in this project, as this project will not be developed in a team form. To overcome this problem, the aspects and practices are chosen that will fit this project.

The approach that will be used will make use of a prioritized list of requirements. These requirements are constantly changing based on the new insights that are required by doing interviews. By adding new features and getting feedback from interviews, the product will gradually grow into the final product. The first requirements will be determined with literature, so that the first requirements can be prioritized and built. Following the first build, interviews will be conducted in which new requirements are determined and feedback is collected. Because due to scope and time constraints, this process will include 2 interviews with SMEs for determining requirements and a focus group of experts to validate the final build.

WORKFLOW

All research methods will contribute to a sub question within the complete research. In Figure 2, the workflow for the proposed research is displayed. This workflow represents the steps, and the order in which those steps are taken, for coming to the final deliverable.

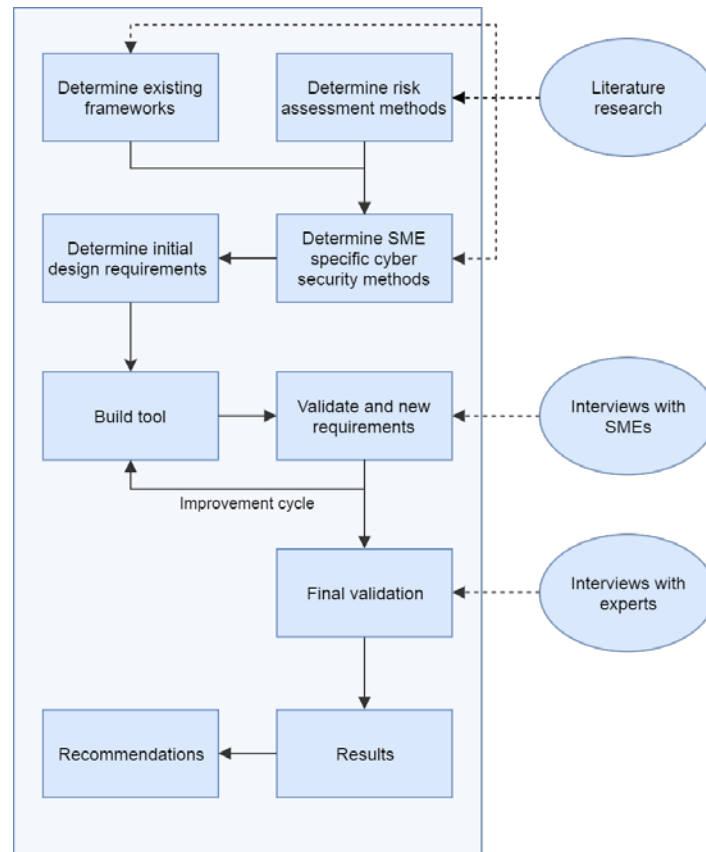


Figure 2 - Workflow

Requirements engineering

As described in the workflow, requirements need to be determined for each cycle, or sprint. After a quick scan on methods on requirements engineering in software development, *Engineering and Managing Software*

Requirements by Wohlin and Aurum [24] was chosen as base for the requirements process. This choice was made on the basis of number of citations and the extensiveness of description within the book. While this is a positive aspect of this book, as it gives a lot of options to use for the process of requirements engineering, not all of these options are suited for this thesis. Some methods and techniques may not be suited due to the size of the project, but some methods might just not fit into the scope of this research. To determine what techniques and methods are most used and most common, a literature review by Inayat et al. is used [25].

In this literature review by Inayat et al., different agile requirements engineering practices and challenges are looked at. These practices are ranked according to the amount of times used in different studies that are analyzed. This ranking concludes that requirements prioritization is investigated in most studies (five). Second was testing before coding, this was encountered four times. On a shared third place are face-to-face communication, customer involvement and retrospectives with all three mentions. Requirements modelling is only seen twice, but because it is also a major subject in the book by Wohlin and Aurum, it is also taken into consideration. First, all of the practices will be shortly explained, after which the argumentation why the practice will be, or not be, taken into account.

Requirements prioritization is the process of determining which requirements are the most relevant for the project at this point. While requirements prioritization is done only once in traditional requirements engineering, namely at the start of the project, it is done before every cycle in agile development.

Testing before coding means that tests are written before starting with the real code. This ensures that all requirements are transferred into tests first, after which these tests can be used as a check to see if the requirements are fulfilled.

Face-to-face communication is the process of having frequent meetings with the client in order to see if the project is still going in the direction they visioned.

Customer interaction is in the same line as face-to-face communication. However, the communication may not be face-to-face, but via email or documents. The reason is the same as with face-to-face communication, checking whether the project is still going in the right direction.

Retrospectives are meeting held after the completion of a cycle. This is done with the customer to see if the requirements fit and if the customer has new requirements for the next cycle.

Requirements modelling is, as the term suggests, the modelling of the requirements. The goal is to schematically make the goals of a project visible, and creating a structure in which new requirements can be easily found.

When looking at these five practices, testing before coding is not relevant for this thesis. As the tool built is a proof of concept and not an application that will be live in a production environment. Also, the retrospective is hard to accomplish, as the interviews that are conducted do not have a follow-up interview. This means that the requirements gathered from different interviews can be implemented, but these implementation cannot be checked in a retrospective after each design cycle. This kind of retrospective does not fit within the time

schedule and scope of this research. The requirements prioritization is a practice that could be well fitted for this thesis, as this makes it clear what needs to be done for creating a working proof of concept. The face-to-face communication and customer involvement are both practices that are harder to achieve in this project, since there is not one clear customer for which the tool is developed. Though, with the interviews that are conducted, the goal is to include potential customers in the development of the tool, and thus both fulfilling these practices. The requirements modelling is a practice that can help with the determining of the requirements. Based on the paper of Inayat et al., the method proposed by Boness and Harrison seems like a fit for this project. The method, goal sketching, is a simple and practical method for determining requirements in an agile project.

Requirements prioritization

As discussed, requirements prioritization is well fitted for this project. In the book by Wohlin and Aurum, multiple methods for conducting a requirements prioritization are discussed. The first thing to determine is on what to prioritize requirements. In the book, *importance*, *penalty*, *cost*, *time risk* and *volatility* are mentioned as concrete examples. They state that this list is not exhaustive and aspects can be fitted on the project. It is also possible to combine aspects to create a prioritization that is based on multiple aspects. For this thesis, some of the aspects mentioned are not relevant. Risk, cost and penalty are not relevant for this project, and thus not considered. Importance and time are two aspects that are relevant. While time is a factor in this project, the end result needs to be good, more than that it needs to be finished on time. For this reason, importance is chosen as the aspect on which the prioritization is done. As described by Wohlin and Aurum, this is a very difficult and multifaceted concept. For this project, importance is defined as the urgency for implementation to get a working tool; the importance to get a working end result.

The technique used for the requirements prioritization is Analytical Hierarchy Process, or AHP. This technique is shortly described in the book by Wohlin and Aurum, but is also found in other literature. In an evaluation of methods for requirements prioritization by Karlsson [26], AHP came out on top for prioritizing (a limited number of) requirements.

Requirements modelling

The article by Inayat et al. describes requirements modelling and sees two methods for agile requirements modelling. The method by Boness and Harrison describes a method for goal sketching [27]. The goal sketching method starts off with determining high level motivations that express the intentions behind the actual development of the project. These motivations are then refined and further defined in motivations, constraints, behavior and assumptions. In the end, a tree like structure will be formed in which the goals, or high level motivations, are in the top of the tree. Underneath these high level motivations are the refinements that will ultimately describe the requirements.

CYBERSECURITY FRAMEWORKS

First step is to establish what cybersecurity frameworks exist and what they consist of. This chapter will discuss the most used cybersecurity frameworks. These frameworks often are the basis of a cybersecurity strategy within a company. Understanding these frameworks helps in understanding how these frameworks can help in structuring the tool in such a way that it resembles techniques that are existent. The goal of the analysis of these frameworks is to see what already exists in the approach of cybersecurity for companies and to see where such a tool fits in, and how parts of the framework can be used in the tool.

According to a survey by Dimensional Research in 2016 [28], the most used frameworks in 2016 are the NIST Framework for Improving Critical Infrastructure Cybersecurity [29], the ISO270001 standard [30] and the CIS Critical Security Controls [31]. This survey also incorporates the Payment Card Industry Data Security Council Standard, but as the name suggests, this is a framework intended specifically for the payment industry. For that reason, this framework will not be discussed further.

NIST Framework for Improving Critical Infrastructure Cybersecurity

While, according to the survey by Dimensional Research, the NIST is not the most widely adopted framework, it is the framework that is the most on the rise. The framework is developed by the United States National Institute of Standards and Technology, or NIST. The development was commissioned by President Obama in 2013 as described in the framework: *“President Obama issued Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013.1 This Executive Order calls for the development of a voluntary Cybersecurity Framework (“Framework”) that provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services.”* [29].

While the framework is designed for critical infrastructures, assets that are critical for the functioning of the economy or society, this is not the only field where it can be applied. In fact, the framework is being adopted by all different kind of sectors and companies, as can be seen in the research by Dimensional.

The framework exists of three parts, the Framework Core, the Framework Implementation Tiers and the Framework Profile. These three parts have different functions, which will be explained in the next paragraphs

FRAMEWORK CORE

The core of the NIST framework consists of four main elements: functions, categories subcategories and informative references. The idea of the framework core is to create a set of activities that eventually lead to the desired cybersecurity outcome.

The structure of the framework core can be seen in Table 2. The functions are the highest level of cybersecurity activities within an organization. These activities are accomplished by categories. These categories are lower level. Within the NIST framework the examples “Asset Management” and “Detection Processes” are given. The subcategories are following the categories in further determining the activities. These subcategories are

specific and are hands-on things that need to be implemented. Just like the categories the NIST framework gives some examples: “External information systems are catalogued” and “Data-at-rest is protected”. Finally the informative references are the standards or guidelines that are used to implement the previous mentioned steps.

Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Detect			
Respond			
Recover			

Table 2 - NIST Framework Structure

FRAMEWORK IMPLEMENTATION TIERS

The second part of the framework are the implementation tiers. These tiers are an indication of where a company is at with their cybersecurity implementation. The four tiers are: partial, risk informed, repeatable and adaptive. Within every tier, the implementation for a company’s cybersecurity on three aspects is described: risk management process, integrated risk management program, external participation.

While tier 2 is a complete implantation of cybersecurity, and 3 is complete than 4, it does not necessarily mean that a company should aim for a higher tier. As is described in the framework: “*Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective.*” [29].

FRAMEWORK PROFILE

The third part of the framework is the framework profile. This profile is created to describe an alignment between the business as it is and the goals set concerning cybersecurity. This creates a roadmap for the company to be followed in order to create a solid cybersecurity strategy that fits the business. Within the NIST framework, no template is given for creating this profile, it is free form.

EXAMPLE USAGE

Within the framework document an example is given on how to establish or improve a cybersecurity program within a company. Seven steps are given to follow, and repeat, when using the NIST framework. These steps are:

1. Prioritize and scope
2. Orient
3. Create a Current Profile

4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze, and Prioritize Gaps
7. Implement Action Plan

All these steps are based on parts of the framework. With the different steps, different parts of the framework can be filled and thus a strategy can be set out.

ISO27001 standard

The ISO27001 standard is a framework by the International Organization for Standardization (ISO) for implementing cybersecurity. The standard consists of a list of different measures that need to be implemented for being compliant to the standard. Directly from the table of contents of the standard [30]:

4. *Information security management system*
 - 4.1 *General requirements*
 - 4.2 *Establishing and managing the ISMS*
 - 4.2.1 *Establish the ISMS*
 - 4.2.2 *Implement and operate the ISMS*
 - 4.2.3 *Monitor and review the ISMS*
 - 4.2.4 *Maintain and improve the ISMS*
 - 4.3 *Documentation requirements*
 - 4.3.1 *General*
 - 4.3.2 *Control of documents*
 - 4.3.3 *Control of records*
5. *Management responsibility*
 - 5.1 *Management commitment*
 - 5.2 *Resource management*
 - 5.2.1 *Provision of resources*
 - 5.2.2 *Training, awareness and competence*
6. *Internal ISMS audits*
7. *Management review of the ISMS*
 - 7.1 *General*
 - 7.2 *Review input*
 - 7.3 *Review output*
8. *ISMS improvement*
 - 8.1 *Continual improvement*
 - 8.2 *Corrective action*
 - 8.3 *Preventive action*

Because ISO27001 is a standard, it gives a list of things that need to be implemented for complying with the standard. The table of contents gives an idea of what kind of steps need to be taken for to comply with the standard.

For example paragraph 4.2; *“Establishing and managing the ISMS”*. Within this paragraph different subparagraphs exist: Establish the ISMS, Implement and operate the ISMS, Monitor and review the ISMS and Maintain and improve the ISMS. Each of these paragraphs give a list of things a company has to do in order to comply. This is literally written as: *“The organization shall do the following”* [30]. The list following this statement consist of things like defining the scope of the ISMS, define a risk assessment approach and evaluate the assessed risk and the treatment options for those risks.

The steps of which the standard exists are extensive, but do not go into implementation level. What is left is a list of checkboxes which have to be checked in order to comply with the standard. Because, as described in the previous paragraph, the points that need to be complied to are on a high level, they leave the implementation to own interpretation. This can be a pro for a company that has (a lot of) knowledge on how to interpret and implement these measures, but it can be a big con for a company that does not have this specific knowledge.

The CIS Critical Security Controls for Effective Cyber Defense

The Center for Internet Security (CIS) is a non-profit organization founded in 2000. Part of the goal of the CIS is: *“Identify, develop, validate, promote, and sustain best practices in cybersecurity”* [32]. This is partly achieved by creating the CIS Critical Security Controls for Effective Cyber Defense. These controls are prioritized security actions that an organization should take in order to ensure the cybersecurity of a company.

The list of controls is based on the most common threats to companies at the moment. The first five controls are considered essential for each company. But while these are considered essential, it is not the case that all of the 20 controls are fit for every company. The CIS is not a one-size-fits-all framework, as described in the document. It is important for each company to assess which controls are of added value to your company.

THE CONTROLS

To get an idea of what the controls are, some examples will be given. The first, and therefore the control with the highest priority, is *Inventory of Authorized and Unauthorized Devices*. Each control starts with a short explanation why this control is relevant and what the risks are if not implemented. After this first explanation different steps are given for implementation of this control. For the first control there are six different things to do for implementing the control. For each of the measures a category and description is given. Per measure is also the “maturity” of the measure stated, this can be foundational or advanced. For this first control, the first five measures are foundational. In other words, it is highly advised to implement the first five measures of this control.

These measures are quite specific. For the first control they consist of deploying an automated asset inventory discovery tool, deploying DHCP logging, update the inventory profile automatically, maintain an asset inventory of all systems connected to the network, and the fifth, deploy network level authentication. While these

measures are specific, they are also quite technical. This means that a cybersecurity expert will have a good idea what to do with the measures mentioned, but that someone with less experience in this field will, for example, have no idea on how to configure a DHCP server correctly.

Conclusion

While there are differences in the frameworks that are discussed, they all have a similarity: they need to be used by people with knowledge of cybersecurity. The first two (NIST and ISO27001) are high level frameworks that only give areas in which a company should investigate; how this is done or how problems are solved is not discussed. The third framework (CIS controls) is different in that perspective, it is quite specific. While it is not as high level as the previous frameworks, it still requires a lot of knowledge, because controls cannot just be implemented without finding out where the weak points in the organization are.

These frameworks are all not suited for SMEs in the sense that they require knowledge, resources or funds that most SMEs do not possess. The discussed frameworks are written not specifically for SMEs, but there is literature that tries to overcome these shortcomings in these frameworks. This literature will be discussed further on in this thesis.

CYBERSECURITY RISK ASSESSMENTS

Within all of the discussed frameworks, there is a part where a risk assessment needs to be done. A risk assessment is simply the identification of the assets that are at risk from a cyber-attack and also identifying the different risks that could impact that asset. The goal is to find the highest risks. This is done by looking at the probability of the risk firing and the impact that such an event will have. This is a very simplistic way of looking at the risk calculation method, but it gives an idea of how the risk is determined. The actual calculation of the risk will differ per risk assessment method.

The risk assessment is a major part of the tool, as it generates the results that are relevant. With information gathered via the interface, a risk assessment should show the vulnerabilities within the organization.

Just like with the discussed frameworks, there are a lot of different methods for doing the risk assessment. Because discussing all of these methods is not within the scope of this research, other literature will be used to determine what methods to examine. In a research done by Dan Ionita [33] a selection of risk assessment methods is done on the base of existing literature. This selection is further trimmed with the help of a list of criteria. These criteria fit the scope of this thesis as well, but still 14 risk assessment methods remain. Because the risk assessment for this thesis needs to be well defined, as the intention is to implement it very specific within the tool, an extra criterion is added. The extra criterion is that the risk assessment goes low level with the implementation and focusses on actual implementations of counter measures. Within the research of Ionita an analysis has been done concerning this criterion has been done, and as such, four methods remain. These methods are:

- CORAS
- Cramm
- Mehari
- NIST SP800-30

While searching for the documents describing the methods it came to light that the Cramm method is no longer active. The website that should provide the documents on the method is offline and the method cannot be found online anymore. For this reason, the Cramm method will not be further analyzed.

In researching the Mehari method, the website was still active, and documents still available, except for the *Mehari Knowledge Base*, this document gave an error. Because the importance of this part of the assessment, the analysis of Mehari became unworkable, thus deciding that the Mehari method would not be further analyzed.

One important addition to this list, which was not included by Dan Ionita, is TRESPASS. The reason that this method is chosen is the research by Gadyatskaya, Labunets and Paci, in which different automated risk assessment methods are compared [34]. The two risk assessment methods that are compared in this research are CORAS and TRESPASS. Because literature sees these two methods are similar (or comparable) it is relevant to include TRESPASS as well.

CORAS

In chapter 3 of the book *Model-Driven Risk Analysis - The CORAS Approach [35]*, the method for doing risk assessments according to CORAS is described. Within this chapter, an example of the whole process is given in which two analysts carry out the risk assessment. The method consists of eight steps. Each of these steps will be concisely explained in the following paragraphs.

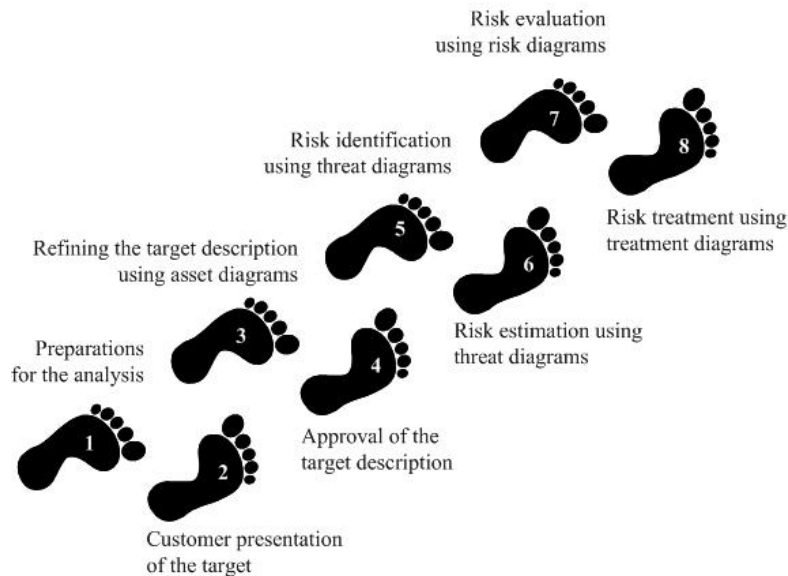


Figure 3 - CORAS steps

STEP 1 – PREPARATIONS FOR THE ANALYSIS

Within this step it is the intention to get a grasp of what the analysis will behold. This means scoping the to-be-analyzed system. Within the example the framework gives, this means having a meeting with the one responsible for cybersecurity within the organization. Within this meeting the scoping has to be done and the planning for the project has to be done.

STEP 2 – CUSTOMER PRESENTATION OF THE TARGET

The goal of step 2 is determining where the targets of the possible risks lie. This target is high level and gives a first idea of the target. In the example a meeting with representatives of the organization is hold to identify these targets

STEP 3 – REFINING THE TARGET DESCRIPTION USING ASSET DIAGRAMS

Within CORAS a certain type of asset diagrams is used. Within this diagram language, target can be defined as well as the paths leading up to the breach of such a target. This is done in the third step. While the target has been defined in step two, the goal of step three is the refinement of this target. This is done by creating an asset diagram in which the path leading up to the breach of the target is defined.

STEP 4 – APPROVAL OF TARGET DESCRIPTIONS

This step is relatively straight forward. The conclusions of step 3 have to be approved by the persons responsible within the company. This can be done via a meeting, but can for example also be done via email.

STEP 5 – RISK IDENTIFICATION USING THREAT DIAGRAMS

With the CORAS modelling language and the targets created in the previous steps, the risks to these threats need to be defined. This can be done with the modelling language. Within this diagram, the person involved, the reason for the risk and the consequences are shown in a simple way. Figure 4 gives an example of such a diagram.

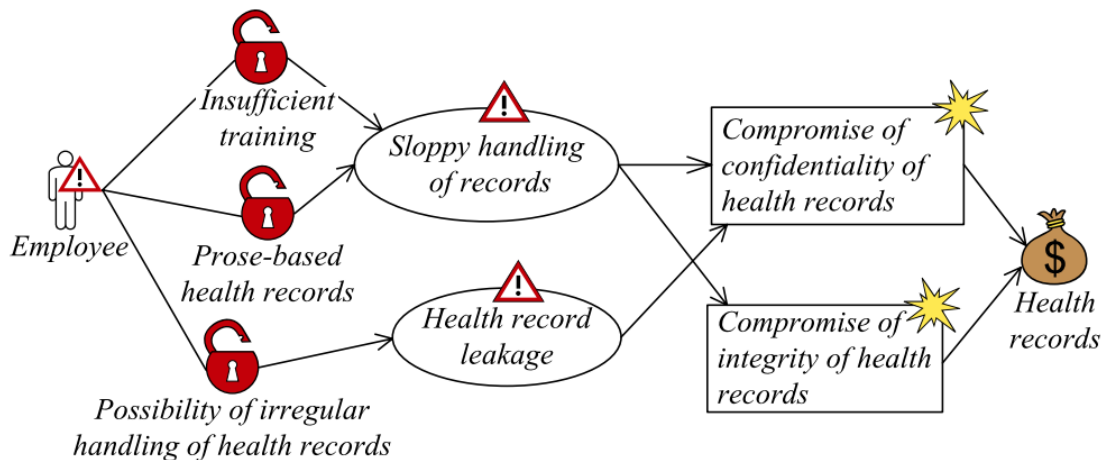


Figure 4 - Example CORAS threat diagram

STEP 6 – RISK ESTIMATION USING THREAT DIAGRAMS

With an idea of what threats there are, an estimation of the severity of the risks has to be done. This is done by estimating the likelihood and impact of a risk. This can be done either by using a tool to calculate these numbers, but this can also be done by estimating these numbers. With knowledge of the field, a good estimation can be made of the likelihood and impact of a risk. The combination of these two numbers will indicate the severity of the risk.

STEP 7 – RISK EVALUATION USING RISK DIAGRAMS

Step 7 gives an overview of what risks exist and what the impact of this risk is. In this step the last checks are done and the risks are categorized to represent their impact. The result of this step is the final to use diagram in the last step.

STEP 8 – RISK TREATMENT USING TREATMENT DIAGRAMS

In the last step, the final diagram is used. Within this diagram, treatment options are added. This is done by adding *Treatment Scenario* steps. These steps are measures or actions that will mitigate the risks.

NIST SP800-30

In Special Publication 800-30, the National Institute of Standards and Technology has published a guide for conducting risk assessments [36]. This guide fills a gap that the NIST Framework, as discussed in the previous chapter, leaves. Where the framework states that a risk assessment has to be conducted, this guide can be used to conduct that risk assessment. The process of conducting the risk assessment consists of four steps:

Prepare for Assessment, Conduct Assessment, Communicate Results and Maintain Assessment. Because the communication and maintenance of the risk assessment is out of the scope of this research, these steps will not be included in this analysis.

STEP 1 – PREPARE FOR THE RISK ASSESSMENT

The goal of the first step is to establish the context for the assessment. In the document, the following steps are stated as part of the preparation [36]:

- Identify the purpose of the assessment;
- Identify the scope of the assessment;
- Identify the assumptions and constraints associated with the assessment;
- Identify the sources of information to be used as inputs to the assessment; and
- Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

For each of these steps a detailed guidance is written in what is required in that analysis.

STEP 2 – CONDUCT THE ASSESSMENT

The real risk assessment also consists of multiple steps. These steps are:

- Identify threat sources
- Identify threat events
- Identify vulnerabilities and predisposing conditions
- Determine likelihood
- Determine impact
- Determine risk

For every step within step 2, a detailed guide is given. For example for the step *identify threat sources*, a structured table is given. Within this table, multiple classifications of threats are given. Examples of these are that it can be an individual, a group, an organization or a state. Within the individual group there are outsiders, insiders, trusted insider and privileged insider. This list helps to get an idea of what threat categories exist and helps in finding threats for a company.

TREsPASS

The TREsPASS project is a cooperation between multiple organizations and universities in Europe. The project provides an “attack navigator”. As stated on the website of the TREsPASS project: *“This navigator makes it possible to say which attack opportunities are possible, which of them are the most urgent, and which countermeasures are most effective.”* [37]. The way TREsPASS accomplishes this is the use of a visual representation of the company; called a Socio-Technical security model, or the TREsPASS-model within TREsPASS. This model consists of multiple elements that can create the structure of an organization. These elements are shown in Table 3.

Component	Description
Actors	Represent human players or processes involved in the system
Assets	Can be either items or data
Locations	Represent where actors or items may be situated either physically or digitally
Edges	Describe possible relocation paths between locations
Policies	Describe access control and specify allowed actions, e.g., get some data item from a location or move between locations
Processes	Formalize certain state transition mechanisms, e.g., computer programs or virtual machines

Table 3 - Different component TRESPASS [38]

An important aspect of this process is the fact that the modelling is done in cooperation with an analyst with specific cybersecurity knowledge. This is done because the inner workings of the TRESPASS attack tree navigator (and the modelling that goes with it) are so complex, that it needs specific knowledge of its workings in order to be used. The advantage of the comprehensive structure of TRESPASS is that it is suited for big companies or projects. The disadvantage of this, is that it is not easy to use by smaller actors and the threshold for using TRESPASS is therefore high.

Conclusion

The methods described are clear in the sense that they provide steps in order to conduct a risk assessment. However, for a SME, these methods are not suited in the sense that risks have to be thought of by the risk assessor. This means that the risk assessment cannot be conducted by someone without knowledge of cybersecurity. However, the methods for doing risk assessment can be incorporated in the tool, as a rule-based set of risks that can be touched upon with the information entered by the user of the tool. How, and if, this will work will be discussed in the requirements chapter.

CYBERSECURITY FOR SMES

In the previous chapters frameworks and risk assessments methods have been discussed. The focus of these chapters was more on the general cybersecurity, to see what fits on SMEs. In this chapter, literature specific for SMEs will be discussed. After this, the applicability of the discussed frameworks and risk assessments methods on SMEs will be reviewed.

Background

As written in the introduction, Dimopoulos et al. [19] write about the need for a risk assessment method specific to SMEs. In this research, it is again confirmed that cyber security within SMEs is lacking due to a lack of resources and funds. This is partly due to the fact that no suitable risk assessment method fitted for SMEs is available. In the research conducted by Dimopoulos it came to light that personnel has no formal training in cybersecurity and not formal IT security certifications. The majority of SMEs also do not conduct any form of risk assessment method, as stated, because of lack of budget, lack of expertise and lack of awareness. The conclusion of the research is that a risk assessment method to show the shortcomings in cybersecurity for a SME is needed in order to overcome these drawbacks for SMEs.

In a research by Parkin, Fielder and Ashby [39] it is stated that there are controls that are suitable for SMEs. The controls they use are the from the CES [31]. However, these controls cannot be fitted correctly by SMEs, due to lack of capacity or in-house skills. The research is focused on finding an optimization for implementing certain controls first to optimize the security it offers. This is done by creating different SME archetypes based on the most common structures of SMEs out there. For each archetype the different controls are modelled to figure out what the effectiveness of a control is. The results of the research conclude that 2-factor authentication is the most effective control in order to raise the security level. However, Parkin, Fielder and Asby state: *"2FA may not be manageable for companies with less available capacity for security, suggesting a need for less effortful protection measures to mitigate theft of credentials."* Which raises the question what criteria determine if two factor authentication may be suitable.

This result is supported by a research by Fielder et al. [40]. In this research, the controls from the Cyber Essential Scheme [41] are analyzed on the basis of effectiveness and cost. The results show that implementing a few of the controls shows significant impact on the security. Depending on the size of the organization, it is not wise to implement all controls. Implementing more controls than the optimum will result in a security improvement that is not in proportion with the higher costs that it brings. The controls that are deemed most cost efficient are adequate patch management and having anti-malware and firewall software installed.

The fact that cybersecurity for SMEs is different than it is for large corporations is clearly mentioned in the articles mentioned above. This is also confirmed by Park et al. [42] who developed a strategy for cybersecurity in SMEs, due to the fact that there is no clear strategy for SMEs. In this article, the strategy for cybersecurity within SMEs is focused on four levels: organizational, workflow, information and infrastructure. The research concludes that the infrastructure layer of an organization, even for SMEs, is quite adequate. This means that the security aspects on the infrastructural level are not the issue, most of the times. The biggest improvements

can be made in the organizational aspects of cyber security. The human-factor, or the user, is an important part of security. The solution to the risks that employees bring within an organization are not necessarily solved by creating restrictions, it is solved by creating understanding within the organization. Understanding raises the awareness of employees, giving them more information on the consequences of their actions. This way, employees have a clearer view of the risks that an action might bring, which makes them think twice before committing to something. This will create a situation in which risky cyber activities are considered twice, and thus incidents will go down.

An article by Stephen Pritchard [43] looks at the struggles that SMEs have in getting their organization secure. What SMEs should do, as there are a lot of options possible, is unclear. This is especially an issue as resources and knowledge are low. For example, there is a lot of software on the market that protects the IT side of a company, however, it is unclear what software is needed for the SME. This means that as a SME with not a lot of knowledge and not a lot of resources, a choice has to be made between different options. However, in most cases it is unclear what aspects of the organization need attention. In the one organization it might be the personnel that needs better training, in the other organization it might be the patch management that is not correct. However, finding out which aspects need improvement are hard to do for SMEs.

In a separate research, Lopes and Oliveira [44] looked at the SMEs and their perspective on the implementation or the non-implementation of information security policies. A policy within a company can be interpreted as the intention to train new employees on the dangers of cyber security, or a policy on patch management. These are all relevant for the overall cybersecurity of a company. The results show that the majority of SMEs interviewed do not have a policy in place. Within these two groups of SMES (with and without policy in place), the question was still asked what the most important success factors were for an information security policy. What the researchers found out, was that users' training is seen as one of the most important factors, in both the groups of SMEs. This is in line with different previous discussed articles; that the employee has an important role in the security of an SME. What is also a result that is in line with previous findings, is the fact that the implementation of such an information security policy is hard due to the willingness of the executive board. This is in line with the lack of attention, resources and funds for implementing an adequate strategy for cyber security within SMEs.

One solution for creating awareness within the group of employees of a SME is proposed by Sanchez, Santos-Olmo, Fernandez-Medina and Piattini [45]. The realization that employees think and know not enough about cyber security is also shared by this article. The solution created is creating a cybersecurity policy in the company. This is not all, this policy needs to be read by every employee that uses a computer for work. This is achieved by showing this policy on first use of the computer. After showing the policy, the employee has to answer 20 questions about this policy. When the employee answers at least 50% of the questions correct, a cybersecurity certificate is earned. This ensures that employees have read, or at least have knowledge of, the cybersecurity policy, thus creating a situation where the awareness for cybersecurity is higher.

Frameworks fitted for SMEs

In previous chapters, framework for cybersecurity in general are discussed. There are however some frameworks that are specifically fitted for SMEs. In the previous paragraph, articles concerning ideas on SME security were discussed. In the next paragraph, clear frameworks for implementation of cybersecurity within SMEs is discussed.

NIST – SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS

The NIST has developed a widely adopted framework that has been discussed in the previous chapter. In the coming paragraphs, the weaknesses for implementing this framework in a SME context will be reviewed. For the purpose of helping SMEs in implementing the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, they wrote a guide on how to do this. The purpose, directly from the document itself, is: “*This NIST Interagency Report (NISTIR) provides guidance on how small businesses can provide basic security for their information, systems, and networks.*” [46].

The document describes the steps of the NIST Framework, but with measures that a SME can take. For this purpose, examples and worksheets to help with this process are given. Examples are, *require individual user accounts for each employee or patch your operating systems and applications*. For each of the examples an extensive explanation and suggestions are given.

Maybe more important are the worksheets that are given. These are forms that can be filled in order to identify risks and measures in a structured way; something that the original NIST frameworks lacks. These worksheets, in combination with the explanation written in the report, provide a base to determine the inventory of the company concerning cyber security, identify threats and vulnerabilities and prioritize resolution actions.

These worksheets provide a good base of what should be determined by a SME to do a good risk assessment. For example the worksheet to identify and prioritize information types. For this worksheet, the different types of information need to be determined by the company. This leaves some freedom for the company to interpret, as the document states that a company should determine what their kind of information types are. Next, for each of the information type, there are some scenarios. These scenarios are situations that can happen to the information type. For each of these scenarios a damage should be determined. This can be in monetary value, but it can also be on a scale like 1-10 or low, medium, high. Apart from the scenarios there are some standards that are relevant for each scenarios, these should also be scaled. In the end, the different information types should be prioritized on the base of the number that are filled in. This gives a good start in determining which information types are the most important.

	Info type 1	Info type 2	Info type 3	...
Cost of revelation (Confidentiality)				
Cost to verify information (Integrity)				
Cost of lost access (Availability)				
Cost of lost work				
Fines, penalties, customer notification				
Other legal costs				
Reputation / public relations costs				
Costs to identify and repair problem				
Priority				

Table 4 - Worksheet information types

Just like this worksheet, there are three more for different goals. These sheets are clear in their setup and can definitely help an SME in determining the critical information needed for a risk assessment.

ENISA – CLOUD SECURITY GUIDE FOR SMES

The title of this report states the meaning, it is not focused on the whole spectrum of cybersecurity of SMEs, but merely on the cloud aspect. Because the focus is so specifically on SMEs and SMEs are using the cloud more and more. In a recent research it came to light that SMEs that make use of cloud computing in Spain, Germany, the United Kingdom, Greece and Portugal are all over 70% [47]. This indicates that cloud computing is becoming a big part of IT in SMEs.

The guide [48] is structured in three main sections: opportunities, risks and questions. In the first section, the opportunities, advantages on security that can be taken with the use of cloud computing are described. In this section things that should be taken into account when using cloud computing are discussed and for each opportunity, a comparison with the traditional IT solution is given. For every opportunities given a link to one or more questions is made, what this means will be explained in the following paragraphs.

The second section are the risks. With the use of cloud computing, certain risks are also encountered. These risks are specific for the use of certain cloud provider. This means that SMEs should check these risks when working with cloud computing. Just as with the opportunities, all these risks have one or more linked questions.

The section with questions in the final part of the guide. They can be used in order to help with the gathering of information on the security of their cloud service. In this process, they help in using the before mentioned opportunities and risks.

While these opportunities, risks and questions help in securing the use of cloud computing, they still require a lot of research and knowledge. Examples of questions are *“How does the cloud service sustain disasters affecting datacenters or connections and which data is backed up where?”* and *“How does the provider ensure that personnel works securely?”* [48]. While these are valid questions, they are hard to answer. First of all,

substantial technological knowledge is required to answer some of the questions, but secondly, and most important, this information is hard to come by. Not all cloud providers will be willing to share this information, making it hard to answer these questions, especially for SMEs with limited resources and limited technological knowledge.

Frameworks

The frameworks as discussed in the previous chapter will be reviewed on the base of applicability on SMEs. This will be done on a per framework basis.

NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

The NIST framework is relatively short compared to the other two discussed frameworks. This is mainly due to the fact that the NIST framework does not go into specifics on what to do or what to implement. The framework gives a strategy on how to tackle cybersecurity and what steps need to be taken to come to measures that need to be implemented. This is a good fit for larger companies with knowledge on IT and/or cybersecurity because with the NIST framework, flexibility for own methods and techniques exists. This however, requires knowledge of IT and cybersecurity. When this knowledge is not present within the company, consultancy services could be used for the implementation. But due to a lack of resources within a SME, this is not possible.

ISO27001 STANDARD

As discussed, the ISO27001 standard is on a relative low level. Every step that needs to be taken for complying with the standard is given. However, the actual implementation of the step is not described. In the example given in the previous chapter for example, the step *establish the ISMS* is not further described. This means that a method of choosing can be used for establishing the ISMS. While this is more specific than the NIST framework, it still leaves a lot of the implementation open for interpretation. This means the same as it does in the NIST framework, a lot of resources are needed into figuring out which methods and techniques are suited and necessary for a company.

THE CIS CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE

The CIS controls are most similar to the ISO27001 standard. The controls are certain steps to implement, and are therefore, just like the ISO standard, on a relative low level. However, they lack the same things the standard does. As described in the previous chapter, while the measures are quite specific, they do not go into the specifics on how to implement. This means that either the knowledge has to be in-house, or that an external party has to be hired in order to do this work. This, just like the previous discussed frameworks, is not within the resources of a SME, and is therefore not suited for the use within a SME.

Conclusion

There is quite some literature on cybersecurity in SMEs. However, this literature mostly confirms the problem that cybersecurity within SMEs is not at the desired level. A lot of literature also confirms that most cybersecurity frameworks and assessments are lacking for SMEs. They are either too complex, or too expensive. Still, some frameworks can be found to fit the needs of SMEs. The NIST has adapted the NIST Framework specifically for SMEs. This framework is perfect for SMEs, as it focusses on the right scope and gives

good handlebars on how to tackle cybersecurity problems. However, it is basically a table that needs to be filled in, which indicates where the biggest assets of a company are. It does not indicate the specific weak points in the organization; something that is needed for SMEs.

The second framework specifically developed for SMEs is the ENISA Cloud Security Guide for SMEs. As the name suggests, it is only for cloud security. While the framework is indeed more suited for SMEs, the fact that it is only focused on cloud security makes it very limited. Another issue with the ENISA guide is the fact that it still requires a lot of knowledge from the cloud service providers; this knowledge is not something that always is at hand.

MODELING AND CALCULATING THE RISK

The goal of the tool is to show a company what their risks within the cyber domain are. As said, this needs to be done with few resources. In order to accomplish this, the tool has to be easily accessible, which translates to a “simple” tool. For doing calculations and determining where the risks lie, the user of the tool has to model their organization within the tool. To accomplish this, the way of modelling has to be simple, but should contain all elements that a user needs to correctly model an organization. In the coming paragraphs, these different elements of the modelling will be discussed.

Elements in the model

The goal of the tool is to model an organization in such a way that is easy to understand, easy to do, but still gives a correct representation of how the organization is structured. As discussed in the risk assessment chapter, a tool that does this as well, but is too complex for SMEs, is the attack tree navigator in TRESPASS. The goal of this tool is also to show organization their weak points and display this in a way that shows how attack might enter an organization. While this tool is well developed, it is very complex. The essence of the tool is the same as the goal of this thesis, but the complexity of the TRESPASS project makes it not suited for SMEs. While this is the case, the structure that is used can be adopted in this thesis in order to model an organization. The components used in TRESPASS are shown in Table 5 with an explanation of what each element is. In Table 6 are the real world equivalents shown with the modelling component that fits the real world component.

Component	Description
Actors	Represent human players or processes involved in the system
Assets	Can be either items or data
Locations	Represent where actors or items may be situated either physically or digitally
Edges	Describe possible relocation paths between locations
Policies	Describe access control and specify allowed actions, e.g., get some data item from a location or move between locations
Processes	Formalize certain state transition mechanisms, e.g., computer programs or virtual machines

Table 5 - Different component TRESPASS [38]

Real world	Model component
Relevant area	Locations and edges
Computer networks	Assets and edges
Human actors	Actors
Physical access control	Policies and processes
Computer access control	Policies and processes
Software processes	Processes

Table 6 - TRESPASS modeling components fitted to the real world [38]

Within TRESPASS, there is also a focus on physical access to components, this is the reason that there is a component *Location*. This component is not taken into account for this research, as it is out of the scope. The assumption is made that SMEs operate from one location or that the location aspect is negligible. This is done in order to keep the structure simple and within the constraints that a SME has. The scope of this thesis does not focus on the physical security that a company has, but only on the security that is in the cyber domain. Furthermore, the components that are described within the model of this thesis will be discussed. Important to notice in these descriptions is the fact that names of components might be the same, but the content of the

components can differ from the TRESPASS components. This is due to the simplification to fit the modelling within time constraints that fit SMEs. It also has to do with the simplification due to the technical complexity that has to be limited.

The last mentioned component, processes, are also not incorporated in this research. The inclusion of state transitions will drastically increase the complexity of the modelling. This will prevent the modelling method in reaching its goal: creating a simple graspable method for modelling an organization.

The component that remain, and of which the model will be built, are *actors, devices, assets, policies* and *edges*. These different components will all be shortly discussed as for what they will stand for in the modelling of an organization.

ACTORS

The first component is the human factor within a company. This component is the same as it is in TRESPASS, except for the fact that it cannot describe processes; it will always represent one or multiple actors. When the last is the case, actors can be grouped. In most companies there will be standard groups like HR, system admins and administrative. These groups all have different permissions which brings different risks.

It is important to notice that these are always actors within the company. These actors cannot represent the attacker.

DEVICES

While the *device* component does not exist in TRESPASS, but is an adoption of the asset component. In the devices category all hardware components of an organization are described. This is done to accomplish that the tool is easy accessible for people without cybersecurity knowledge. A separate devices component category is clear to understand and gives a good overview of what devices are present in an organization. The asset category in TRESPASS might cause confusion, as the asset category was both for data and for devices.

ASSETS

Different from the category in TRESPASS, the assets category is the value for a company. Most of the times this is data that a company has stored on their network. As described in the Devices category, in TRESPASS the Assets category consists of both the devices and the data that is at hand. For the simplification and the easiness to understand the tool, this category is divided in two. Assets can be things like medical data, credit card data or personal customer data. In this category, the thing that is most valuable for a company (in the IT area) is defined.

POLICIES

While this is again a category that has the same name as in TRESPASS, it is not the same thing. In TRESPASS the policies category is a complex one, in which very specific actions can be described. Things like access control and the movement of certain data. This interpretation of policies is too complex for the scope of this thesis and is therefore simplified. It can even be seen as a complete change of the meaning policy from the TRESPASS meaning.

Within the tool, a policy is something that influences an actor or device. This can be things like, what education does an actor have or how often is a device updated. This all influences the risk a link in the model carries, but more on that will be described later on in this chapter.

EDGES

In TREsPASS, the edges are the connections between different components of the model. While edges, in the sense of connections, exist in the models created within this research, they are simply called connections. How these connections work and what kind of influence they have will be described in the next part.

Structure of the model

The components described in the previous paragraphs can create a model that represents an organization's IT status. While the different components are simple, they still include most of the aspects of an organization that are relevant for the cybersecurity of an organization.

Still, it is important to notice that creating all different components to model an organization is not enough. These different components need connections between them in order to show the usage and data flows between the different components.

In the simplest form, the structure is: an actor has access to a device and with that device the actor can access an asset. This flow is shown in Figure 5.

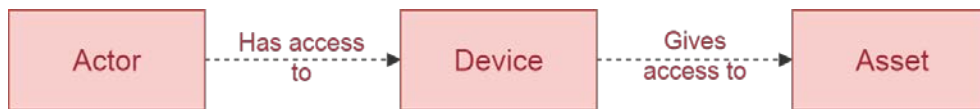


Figure 5 - Connections between different components

All of the access flows within an organization can be modelled with this structure. In a simple example, the main asset of a company is the credit card data of its customers. This data can be accessed with a certain computer. The group of system administrators has access to this type of computer, which makes that this group can access the asset (credit card data). While this is a singular flow, this model can be made more complex when for example a group support staff also has access to this computer, or when the system administrators also have a mobile phone which gives them access to the asset. No components are bound to one or two connections.

Policies come in last. When the structure of the organization is built with the actor, device and asset components, policies can influence the actor or device components. This is shown in Figure 6.

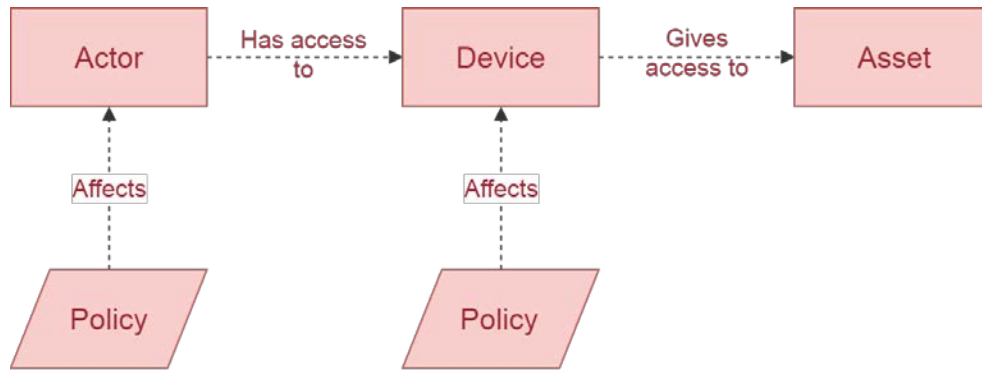


Figure 6 - Influence of policies on devices and actors

Policies have an impact on the probability of a risk firing through that component. How these calculations are done is described further on in this chapter. Examples of policies are *a device is updated every week* or *an actor is trained every year on the risks of cyberattacks*. These policies improve the security of a component, thus limiting the risk to the asset which the components are connected to.

Calculating the risk

In the structure described in the previous paragraph, paths exist. It is clear what actor can access which asset with which device. This is similar to the concept of an attack tree, as introduced by Schneier [49]. An attack tree is, as defined in the paper by Schneier: *“A way of thinking and describing security of systems and subsystems”* [49]. It represents the attacks and countermeasures on a system, displayed as a tree structure. An example of an attack tree is shown in Figure 7.

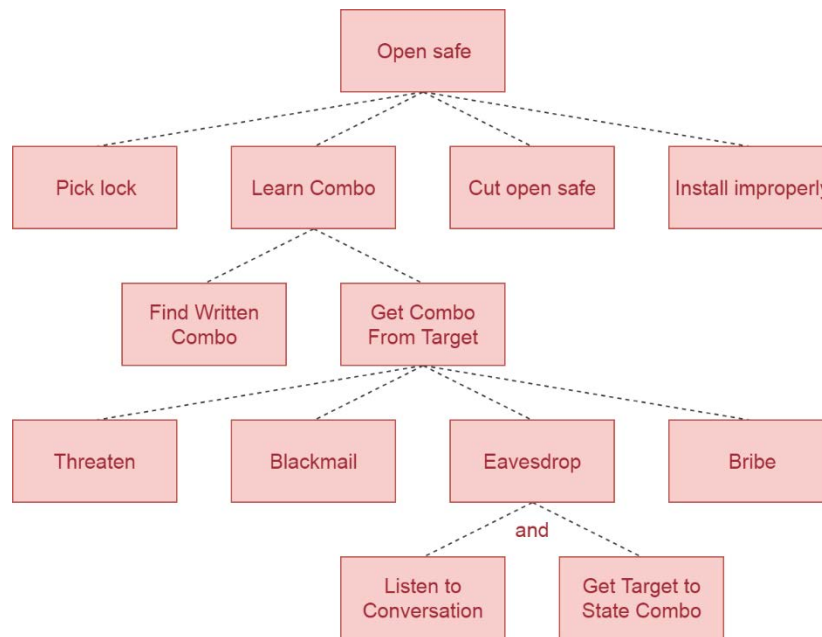


Figure 7 - Attack tree example [49]

The example shows that the main goal for the attacker is to open the safe. To do this, there are multiple options. For some options (in this case *Learn Combo*) there are again multiple options. Going down the tree it shows all possible ways for the attacker to get to their end goal of *Opening Safe*. In this case, the tree is relatively simple, but in the bottom it shows a good example of how to accomplish to *Learn Combo* by *Get Combo From Target* using *Eavesdrop*. To accomplish the *Eavesdrop* method, the attacker has to *Listen To Conversation*, but that is not all. The attacker also needs to make sure that the *Target States the Combo*. What this means for the calculations will be explained in the next paragraph.

It is important to point out that the attack tree does not fit the tool that is being created for this research. This is because the attack tree method needs the perspective of an attacker. For this research, the assumption is made that the attacker has the same capabilities for each SME, more on what this means for the calculations will be discussed later on. This means that the perspective can switch from the attacker to the defender, which means that creating a structured overview of what the vulnerabilities on the defending side are is easier. With the tool being used by people that are defending and do not have specific knowledge on the possible attacks on their system, the attacker cannot be set specific to the business. This is why the structure in the previous paragraph is chosen. However, the attack tree shows an interesting way of calculating risk; one that can be adopted into the model that is chosen for this research. Where in the attack tree the methods for entering a certain node in the systems is shown, the structure remains the same in this model, although the nodes do not represent the actions an attack does, but the defending nodes. As said, because an assumption is made on the attack strength of the attacker, these odds do not differ per attacker, and the impact of different defense strategies will remain the same. Therefore, the possible calculations that can be done with an attack tree will be discussed in the next paragraph.

CALCULATIONS IN THE ATTACK TREE

In an attack tree, there are multiple ways of calculating what the highest risks are (or what the best attack paths are). In the paper by Schneier, examples like costs, attacker-skills or probability of success are given. This last one is the one that is relevant, as the goal of this research is to create a tool that can conduct a risk assessment.

In a paper by Ingoldsby [50] this calculation method with threat probabilities is further defined. He states that every node in the tree has a certain probability of succeeding. This chance is determined by looking at multiple factors to succeed in that attack. In the example given the cost for that attack, the technical ability necessary and the noticeability that comes with the attack are taken into account. Those three factors are all a number between 0 and 1. When these three numbers are multiplied, the ease of the attack is determined. Or in other words; the probability that this attack is conducted by an attacker. This gives a probability for every node that this method is used for an attack.

ADAPTING THE ATTACK TREE RISK CALCULATIONS

As said, while an attack tree is something different than the model used in this thesis, the structure remains similar. Where an attack tree is viewed from the perspective of the attacker, the structure used in this research is on the viewpoint of the defender. This means that for an attack tree, the probabilities are displayed as a

probability that an attacker succeeds in doing that one component. In the structure that is used in this thesis, the components in the “tree” are “defending” elements while the “attack” elements are not mentioned explicit (different from for example an attack-defense tree). As stated, an actor is connected with a device, which is again connected with an asset. This creates path from the actor, through a device, to an asset. This means that if either the actor or the device is breached, the asset is accessible. This can be better explained by using an example. If an actor can access an asset via a device, this means that both the actor and the device have access to that asset. This means that even if the device is perfectly secure, if the actor gets breached, the attack can use the actor to get to the asset. The other way around this works the same way. Even if the actor does everything secure from a cybersecurity perspective, when the device is not secure and can be accessed by an attacker without the involvement of an actor, the attack can still reach the asset. So, that means the structure from the model can be translated to the diagram as shown in Figure 8.

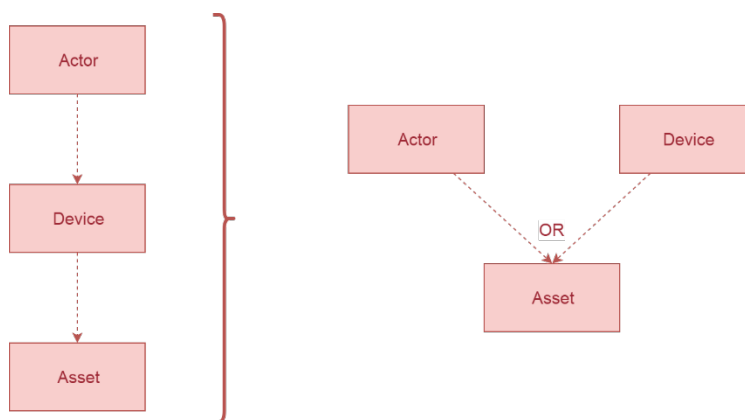


Figure 8 - Translate model to diagram for probabilities

The goal of this diagram is to calculate the probability on the asset, after which the risk on the asset can be calculated. Just like in an attack tree, every node will have a probability that it will be used for a breach. Assuming that a breach on actor and a breach on device are both mutually exclusive events, the following formula can be used in order to determine the probability that the asset will be breached:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Which translates in this particular case to:

$$P(\text{Asset}) = P(\text{Actor}) + P(\text{Device}) - P(\text{Actor} \cap \text{Device})$$

For example, if the probability that the actor in this case is breached is 0.6 and the probability that the device is breached is 0.4, the probability that the asset is breached is:

$$P(\text{Asset}) = 0.6 + 0.4 - 0.6 * 0.4 = 0.76$$

This calculation gives a probability of 0.76 (or 76%) that the asset will be breached. However, as these are calculations for a risk assessment, the risk on the asset needs to be calculated. The general formula for calculating risk is $Risk = Probability * Impact$. This formula is also used in these calculations, however,

the impact is not yet determined. The impact will be determined by the user of the tool, indicating the impact of a breach on a certain asset from 1 to 5, where the numbers 1 to 5 correspond to number between 0 and 1.



Impact inputted by user	Impact in calculation	Risk	Name	Color
1	0.20	0.00 – 0.20	Very low	
2	0.40	0.21 – 0.40	Low	
3	0.60	0.41 – 0.60	Medium	
4	0.80	0.61 – 0.80	High	
5	1.00	0.81 – 1.00	Very high	

Table 7 - User input conversion

Table 8 - Risk names and corresponding colors

In Table 7 the conversion from the user input to the number that is being used for calculation is shown. The reason that the impact is chosen from 1 to 5 is because of the ease to understand for the user. Because all calculations are done in number from 0 to 1, the conversion is also done to conform to this standard. This conversion is a linear conversion. To follow up on the example that was just given, if the asset used for calculations was given an impact score of 4, the calculation for the final risk would be:

$$Risk\ for\ Asset = 0.76 * 0.8 = 0.61$$

This means that the risk for the asset will fall in the category *High* as can be seen in Table 8, which is a severe risk and should ring a bell at the user end. Again, this conversion is done to make the interface easier for the user. This conversion is again linear.

The calculations that are done determine the probability and risk for the breach of an asset. However, these calculations are done with the probabilities of a breach of an actor or a device. How these probabilities are determined will be explained in the next paragraph.

DETERMINING THE PROBABILITIES OF COMPONENTS

As said, the different components have different probabilities of being breached. These probabilities are the base for the calculations on determining the risk on the asset (as discussed in the previous paragraph). However, the calculations that work on the different components are not yet discussed. In the *Structure of the model* part of this chapter, it is explained that different policies have an impact on the components. This impact will have an effect on the probability that a component will be breached. The probability of a component being breached will influence the probability of an asset being breached, following the structure shown in Figure 8 earlier on in this chapter. One problem with the fact that the probability of all these components need to be determined is that there is knowledge needed in order to do this. A quote from a research by McGraw illustrates this perfectly: *“The key to an effective risk assessment is expert knowledge of security”* [51]. The problem with this is that the goal of this research focusses on creating a risk assessment method that is accessible to people that do not have this particular knowledge. This means that these two aspects have to be decoupled, the knowledge of what are the probabilities that a certain node will be breached needs another origin than the user. Somehow the knowledge of certain probabilities need to be put into the system, this way the user just has to select different options that are pre-programmed in the system.

This kind of system is called a knowledge-based system (or KBS). In such a system, the knowledge that is required for making decision is put into a knowledge-base. This makes that the system can make decision without the user having to input certain knowledge, furthermore it is flexible as it can be easily extended and refined [52]. A knowledge-based system works with certain rules, most of the times these are IF-THEN rules. An example of a rule, as given by Smith [52]:

```
IF
    there exists a normal fault with class unknown, and
    there exists a red pattern
        with length < 50 ft.,
        with bottom above the top of the fault,
        with azimuth perpendicular to the fault strike
THEN
    the fault is a late fault with direction to downthrown block equal to the
    azimuth of the red pattern
```

As can be seen, the knowledge base must contain certain knowledge to conclude the fact that is written in the THEN statement. As can be seen, there are multiple conditions that conclude into the THEN statement. This is not completely in line with the structure of the model used in this research. The rule as abovementioned can be translated in the following form for this research:

```
IF
    policy 1 works on component, and
    policy 2 works on component, and
    policy 3 works on component
THEN
    the probability of a breach on the component is impacted with impact(policy
    1, policy 2, policy 3)
```

While this works, it is not a rule-based system as proposed Smith. The difference lies in the fact that the policies in the IF statement have an impact on what happens in the THEN statement. In the THEN statement, calculations are required in order to determine what the impact on the probability of a breach on the component is. While this might not be the use as Smith intended it, it still has the advantages which are needed for this model: it can use knowledge of experts and perform them on a component without the need for the user to have knowledge on the risks that work on a component or policy.

In the end, it means that it is not a rule-based system in the traditional sense of the word: it uses only one rule with different inputs. But by choosing these different inputs per policy, the rules serve the purpose of a well-structured knowledge-base than can be easily read and easily extended.

How these rules and calculations that come with the rules come together is explained in the following paragraphs of this chapter.

CALCULATIONS ON THE POLICIES

An important aspect of the knowledge-based system is how the rules are structured. Because no such a system has ever been used, it is hard to find relevant literature on this subject. Most literature found on the subject is based on fuzzy rules [53] or are hardcoded rules that do not use probabilities (just like the given example above) [54]. While this means that there are no calculations that can be used from a knowledge-based system,

the system remains suited for this purpose as the expert knowledge can be incorporated in the model. For the calculations, the Gordon-Loeb model will be used in combination with the rules [55]. This model is been widely accepted as determining what the effects on successive investments in cybersecurity are. In this case, this will be used to determine the diminished effect [55, 56] of more policies on a node, as these can be aligned: more policies is more investment.

The Gordon-Loeb model uses the formula shown below. Where *Effect* is the effect of the policy on the improvement of the probability of the breach on the component. The *impact factor* is the impact of the policy as determined by expert, on a scale from 0 – 1. Lastly, *I* is the number of the policy, where the first policy will have a bigger impact than the next one.

$$Effect = 1 - \frac{impact\ factor}{(I + 1)}$$

When plotting this formula, it shows the impact of multiple policies implemented on the same component with the same impact (0.8 for this example). The plot of this formula with *impact factor* = 0.8 can be seen in Figure 9.

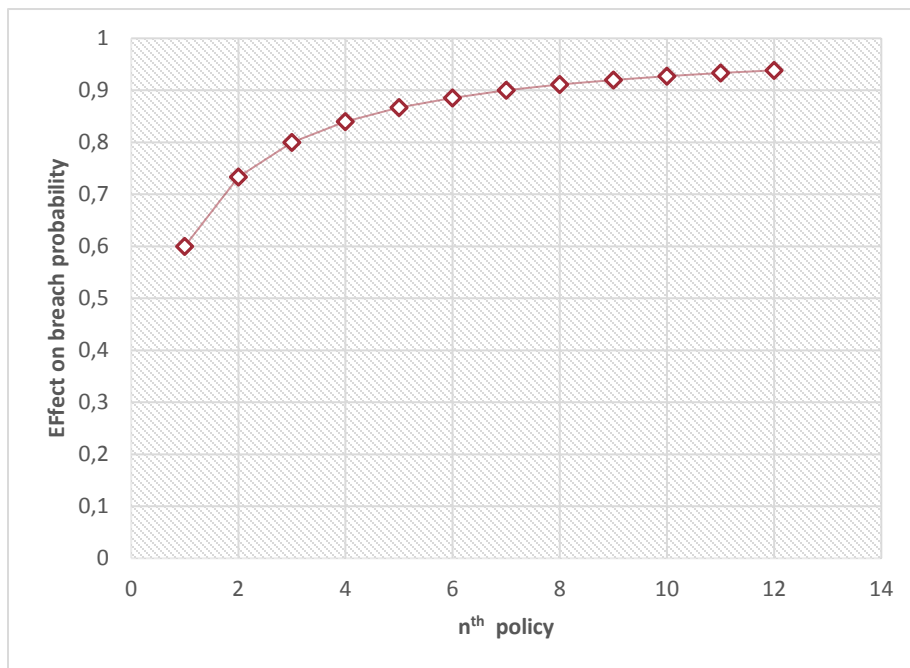


Figure 9 – Diminishing marginal returns effect of number of policies

This *Effect* will then be used to impact the probability that the component will be breached. This will look like the following formula:

$$P(device\ with\ Policy_1\ to\ Policy_n) = P(device) * Effect_1 * Effect_2 * ... * Effect_n$$

As said, and shown in Figure 9 this includes the effect of diminishing marginal returns. This means that every extra policy has relatively less impact than the previous one. Using this example of the effect of policies with

the same effect on a component with base risk 0.7 is shown in Figure 10. This graph clearly shows that the first policy has a big effect (decreasing the breach probability from 0.7 to 0.28) while the following policies have less of an effect. The second policy decreased the breach probability from 0.28 to 0.19.

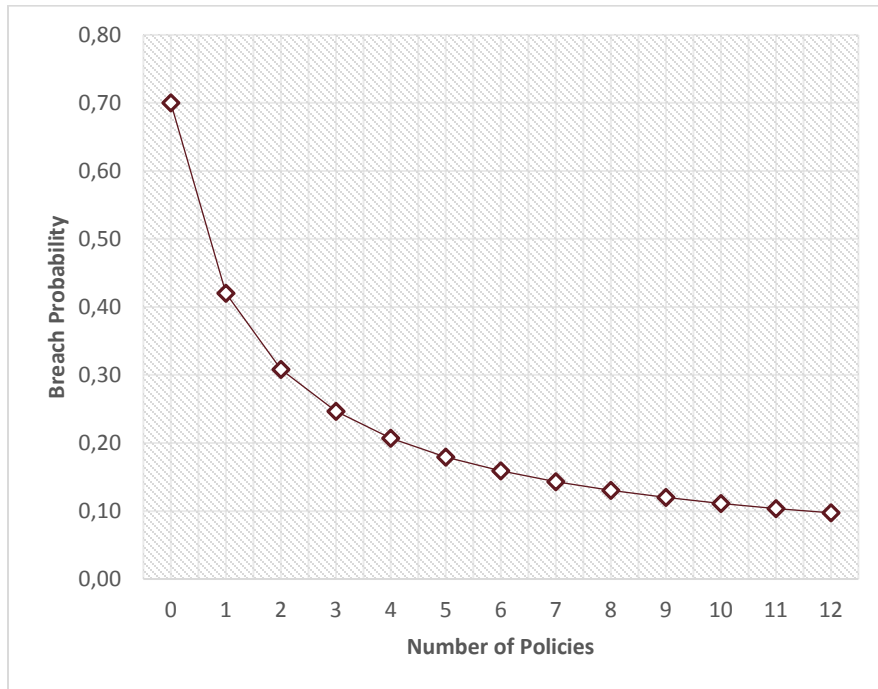


Figure 10 - Impact on breach probability

STRUCTURING OF THE RULES

To apply these calculations on the different actors and devices, a clear structure has to be defined in order to create a knowledge base. This knowledge base needs to be easy in maintenance and editing or adding rules. In order to do this, each rule has (like most KBS) an IF-THEN structure. As said, every rule will influence the actor or device with a value of 0 to 1.

IF *name* IS *value* THEN PROBABILITY ON *works on* IS DECREASED BY FACTOR *factor*

As an example, the patch frequency of a device is given. In this case the variables in the rule will look like:

```

name           = patch frequency
works on      = device
value         = weekly
factor        = 0.8

```

Which results in the following rule:

IF *patch frequency* IS *weekly* THEN PROBABILITY ON *device* IS DECREASED BY FACTOR *0.8*

Because in this case, the value and risk have multiple options (value can be weekly, monthly, yearly, etc.) this creates the following rules:

IF *patch frequency* IS *weekly* THEN PROBABILITY ON *device* IS DECREASED BY FACTOR **0.8**
 IF *patch frequency* IS *monthly* THEN PROBABILITY ON *device* IS DECREASED BY FACTOR **0.6**
 IF *patch frequency* IS *yearly* THEN PROBABILITY ON *device* IS DECREASED BY FACTOR **0.4**

These rules can be displayed in the form of a table in the following form:

#	Name	Works on	Value	Factor
1	Patch frequency	Device	Weekly	0.8
			Monthly	0.6
			Yearly	0.4

Table 9 - Policy rules in table form

Determining the rules

For a proof of concept, the knowledge base should have an initial set of rules that can be used in order to create a model. It is important to stress that the determining of the rules is not a core part of this research, it is merely intended in order to proof the model's concept. Therefore the ruleset that is created is not exhaustive in any way. The way the model was set up is in such a way that the rules in the knowledge-base can be edited or removed with ease. It is also easy to extend the knowledge base with extra actors, devices, assets or policies.

To create an initial set of rules that can be used for the proof of concept, an expert session was held. In this expert session, two KPMG consultants determined the base value of different components and the possible policies that can work on those components. These two consultants were selected on basis of their expertise. The first one is familiar with the quantification of breach probabilities for customers of KPMG while the second one has an expertise on the penetration testing of systems, and therefore can estimate what common attack vectors are. A summary of the expert session can be found in Appendix G. The results of the session are shown in Appendix H.

DEVELOPMENT OF THE TOOL

This chapter will first describe the development sprints that are made in order to determine the different requirements and design choices. After that, the implementation decision will be discussed.

First development sprint

As described in the workflow in chapter 1, based on the literature the first requirements will be set. These requirements will be used to build the first version of the tool. This version will be used as a base in the first interview with a SME. This interview will be conducted to verify the requirements that are used to create the first version. The interview will also provide more requirements that will be used for adding functionality in the next development sprint. There will be a final requirements interview after this development sprint, this sprint will be used for exactly the same purpose as the first interview. This creates three requirement definition and validation cycles.

REQUIREMENTS MODELLING

As discussed in the previous chapter, one of the practices used in the requirements engineering process will be the requirements modelling. This requirements modelling will be done according to the method proposed by Boness and Harrison [27]. The first requirements will be determined based on the literature that has been discussed in the previous chapters.

In the literature, a few shortcomings in current methods and techniques for the use in SMEs became clear. The motivation for creating a risk assessment tool for SMEs is as follows:

- I. Make cybersecurity risk assessments accessible for SMEs

Multiple constraints as found in the literature will be attached to this motivation to achieve this motivation.

- i. Keep costs low (based on finding **F2**)
- ii. No specific cybersecurity knowledge necessary (based on finding **F1, F3**)
- iii. Keep time investments low (based on finding **F2**)

The schematic version of these constraints is shown in Figure 11.

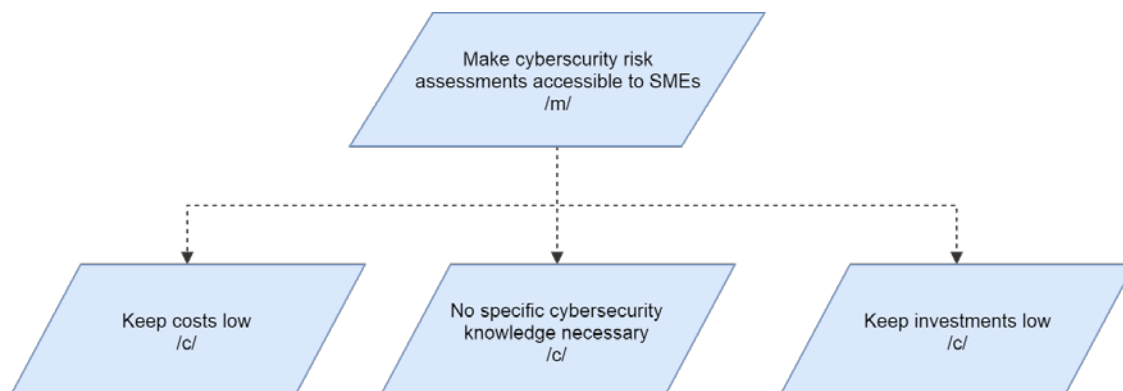


Figure 11 – First goal sketch

This goal sketch gives the first idea of what the main motivation and constraints of the tool are. To build the first iteration, these constraints have to be further defined with the help of literature. The visual representation of this goal sketch is shown in Figure 12. For each of the further defined constraints, foundation in the literature will be discussed.

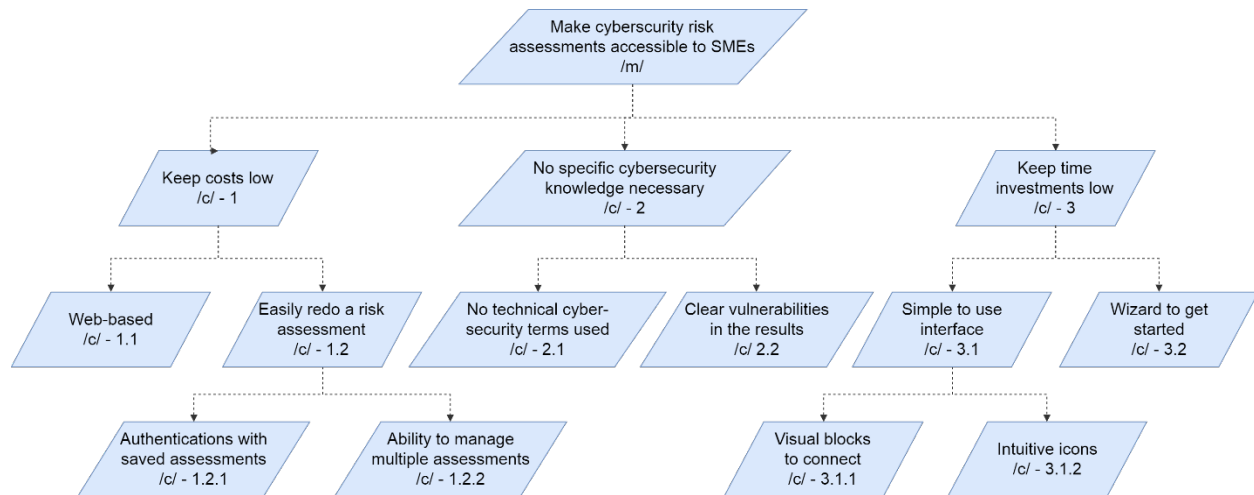


Figure 12 – Further defined goal sketched based on literature

All the constraints added in the figure are numbered. Each of these constraints will be shortly explained.

Constraint	Description	Explanation
1.1	Web-based	Making the tool web-based means that no extra hardware or software is needed in order to run the tool. This creates a tool that is low in costs to use. [57]
1.2	Easily redo a risk assessment	Because costs need to be low, the threshold for using the tool needs to be low. This means that mistakes in a risk assessment should be easily “forgiven”. By giving the option to redo an assessment, this threshold is kept low.
1.2.1	Authentication with saved assessments	To accomplish constraint 1.2, the user should be able to login. This way, risk assessments can be linked to a user, therefore an overview of what is done till that point can be easily seen.
1.2.2	Ability to manage multiple assessments	Redoing a risk assessment can be accomplished by creating multiple assessments. By keeping the old assessment still in the database, it can be used as a reference.
2.1	No technical cybersecurity terms used	As described, it must be able to conduct the risk assessment with knowledge of cybersecurity. Avoiding specific cybersecurity terms is one of the ways to accomplish this. (Finding F3)
2.2	Clear vulnerabilities in the results	To accomplish constraint 2, the results also need to be interpretable by people with little knowledge of cybersecurity. While this is a constraint, it still needs to be further defined how this is accomplished. This will be done in following design sprints. (Finding F1, F2, F3)
3.1	Simple to use interface	To keep time investments low, the interface has to be easy to use. This prevents a steep learning curve, meaning a shorter time investment into using the tool. [58]

3.1.1	Visual blocks to connect	With the help of visual blocks to compose the organization, the person using the tool can create a visual map of the organization. This helps removing abstraction and creates an intuitive way of working. [59]
3.1.2	Intuitive icons in support of text	As with the visual blocks, icons help lowering the threshold. It creates a way of providing information without reading information on beforehand. [59]
3.2	Wizard to get started	Creating a structure of an organization from scratch can be a time consuming task. Therefore a wizard can help in kick starting this project. As SMEs share similarities, a wizard can provide a starting structure that answers a lot of the questions that are relevant for all SMEs. [60]

Table 10 - Goal modelling sprint 2

REQUIREMENTS PRIORITIZATION

For the requirements prioritization, the AHP methodology is used. All the requirements will be compared to each other on the aspects of time and importance. In this case, the aspect importance is rated a bit higher than time. Table 11 shows the weights that are determined for the different aspects.

	Importance	Time	2nd root of product	Priority Vector
<i>Importance</i>	1,000	1,500	1,581	0,551
<i>Time</i>	0,667	1,000	1,291	0,449
<i>Sum</i>	1,667	2,500	2,872	1,000
<i>Sum*PV</i>	0,918	1,124		
<i>Lambda Max</i>	2,041			
<i>CI</i>	0,041			
<i>CR</i>	0,041			

Table 11 - Weights for prioritization

After the weights, the different requirements need to be compared with each other on the different aspects. This is done in a table, in which each requirement is assigned a value to compare it with the contrasting requirement. This value is 1 when it is equal, can be 2 if it is twice as important or, for example, 0.5 when it is half as important. All these values are based on what is found in the literature and on own experiences. The results of these comparisons can be found in Appendix B.

The results of these comparisons are weighted with the abovementioned weights, this is done in Table 12. These resulting scores can be sorted, resulting in Table 13 which shows the final prioritization of the requirements.

	Importance	Time	Score
	0,551	0,449	1,000
1.1	0,134	0,131	0,133
1.2.1	0,119	0,126	0,123
1.2.2	0,126	0,118	0,123
2.1	0,130	0,133	0,132
2.2	0,120	0,119	0,120
3.1.1	0,124	0,118	0,123
3.1.2	0,117	0,133	0,125
3.2	0,130	0,122	0,123
	1,000	1,000	1,000

Table 12 - Weighted scores

#	Requirement	Score
1	1.1	0,133
2	2.1	0,132
3	3.1.2	0,125
4	1.2.2	0,123
5	3.1.1	0,123
6	1.2.1	0,123
7	3.2	0,123
8	2.2	0,120

Table 13 - Final prioritization

This prioritization means that requirements 2.2 is in the bottom. This requirement (clear vulnerabilities in the results) is of less importance than the rest of the requirements in the first development sprint. While the requirements on spot 4 to 7 have the same score, it can be argued that requirement 3.2 (the wizard) can be developed in a later stage. While all other requirements are interconnected, the wizard can be seen as a separate part. This factor, and the fact that it can be separated from the rest of the requirements, makes it suitable for doing in the next development sprint. This means that both requirement 3.2 and 2.2 will be postponed to the next development sprint.

REQUIREMENTS TO DESIGN

The requirements that are set are translated into mockups. Several pages are created in order to meet the different requirements that are set. The mockup pages are shown below.



Figure 13 - Login page mockup

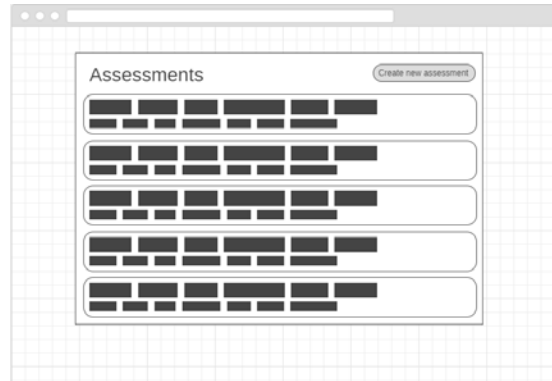


Figure 14 - Overview page mockup

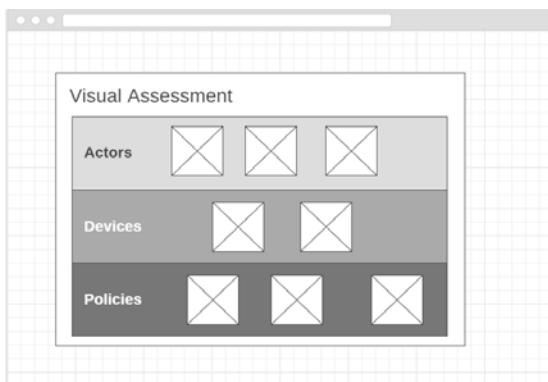


Figure 15 - Visual Assessment blocks

In order to meet the first requirement, the tool will be web-based, the mockups are created in a browser interface. All elements are web-based and can be viewed in every (modern) browser. In Figure 13 a login mockup is showed. This is the landing page for the tool on which users can login or choose to register. This functionality is created in order to meet the second requirement: the user can login with personal credentials. The second mockup in Figure 14 is an overview of all risk assessments that are created by the user. In this

overview the user can select to continue with an assessment, edit it or delete it. The user can also create a new assessment. This page meets requirement three: the user can manage multiple risk assessments at the same time. In Figure 15 the actual assessment layout is shown, this is a view in which icon blocks are used. These blocks can be added in a way that they represent devices, users or policies within the company. Blocks can be connected to shown the connections within the organization.

Second development sprint

While the first development sprint has a basis the literature, the second development sprint has an interview with an SME to check whether or not the requirements set in the first develop sprint are correct. It also has as purpose to further define the requirements that were set until this point.

FINDINGS FROM THE INTERVIEW

The first interview was conducted at a small enterprise with 8 FTE. The interview confirmed that the focus on cybersecurity is lacking within this SME. After explaining the goal of this research, the interviewee confirmed interest in the proposed tool. In the interview it came to light that the most desired way of filling in such a tool would be in a visual way. The blocks shown as developed in design sprint fell in the liking, just like the idea for a wizard to construct the first set of blocks. Concerning the knowledge required to use the tool, no specific cybersecurity knowledge should be required, but the interviewee indicated that a certain level of IT knowledge (system management) should be handy in filling in the tool. This knowledge will only improve the results of the assessment and this knowledge is practically always available in a company.

Concerning the time investments, the interviewee indicated that, in this company’s situation, a risk assessment should not take longer than half a day. When the assessments takes longer than this, outsourcing becomes a better option.

Finally, the presentation of the results was discussed. While the interviewee first suggested a list of risks, he changed his mind after showing him a sketch on a visual representation of risk attack paths. The visual approach to showing where the risks within an organization lie was desired more than a list. The results of the interview are displayed in Table 14.

#	Constraint	Finding
2.1	No technical cybersecurity terms used	Confirmed & added information on what knowledge is required
2.2	Clear vulnerabilities in the results	Confirmed & added information on the presentation of the results
3.1.1	Visual blocks to connect	Confirmed
3.1.2	Intuitive icons	Confirmed
3.2	Wizard to get started	Confirmed
New	Time investments maximum of half a day	New

Table 14 - Findings from interview

REQUIREMENTS MODELLING

With the findings from the interview and the results from the last sprint, the goal modelling can be reviewed and expanded. In the new goal sketch, the blue blocks are the new requirements while the purple blocks are the requirements that were defined in the last sprint, but due to the prioritization were not executed. Because

the *keep costs low* branch of the model has not changed, this side is cropped of. The results can be found in Figure 16.

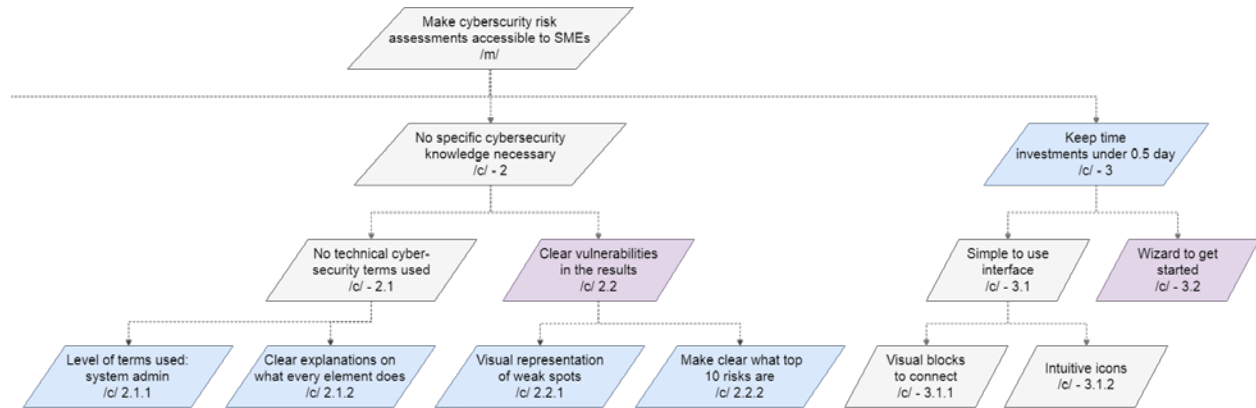


Figure 16 - Goal modelling sprint 2

The constraints shown in the model are again displayed in table-form, but in this case, only the changed and new constraints are shown.

Constraint	Description	Explanation
2.1.1	Level of terms used: system admin	An extension on the 2.1 constraint is the level of technical terms used. From the interview can be concluded that the level of system admin is a good level. (Finding from interview)
2.1.2	Clear explanation of what every element does	With the lack of cyber terminology, it might be unclear what each element in the tool does. Explanation of every element is essential in the understanding of the tool
2.2	Clear vulnerabilities in the results	This constraint was already in the previous sprint but was not included in the actual development due to a lack of definition and due to the prioritization. This sprint it is further defined. (Finding from interview)
2.2.1	Visual representation of weak spots	As said, the interviewee indicated that a visual representation of the risks is better than a simple list of risks.
2.2.2	Make clear what top 10 risks are	It also became clear that the interviewee finds value in the most crucial risks to mitigate. A top 10 list was mentioned, thus a top 10 list of risks should be clear. This can be done, not in a list style, but in a visual way to comply with constraint 2.2.1.
3	Keep time investments under 0.5 day	While this requirement was already in the goal sketch, it was described as “keep time investments low”. With the interview, this investment is narrowed down to maximum half a day. (Finding from interview)
3.2	Wizard to get started	The wizard is confirmed as a good idea and has remained the same as in the previous goal sketch. (Finding from interview)

Table 15 - Goal modelling sprint 2 - Overview

REQUIREMENTS PRIORITIZATION

Again, requirements prioritization is applied on this set of requirements. The weights shown in Table 16 in Development Sprint 1 are again used for the prioritization in this development sprint. All the determined requirements are again compared to each other on the aspects of time and importance. This results in the following prioritization:

	Importance	Time	Score
	0,551	0,449	1,000
2.1.1	0,197	0,220	0,207
2.1.2	0,173	0,185	0,178
2.2.1	0,203	0,208	0,205
2.2.2	0,203	0,200	0,202
3.2	0,223	0,187	0,207
	1,000	1,000	1,000

Table 16 - Weighted scores sprint 2

#	Requirement	Score
1	2.1.1	0,207
2	3.2	0,207
3	2.2.1	0,205
4	2.2.2	0,202
5	2.1.2	0,178

Table 17 – Final prioritization sprint 2

As can be seen in the final prioritization in the Table 17, requirement 2.1.2 scores a lot lower than the rest of the requirements. Due to this reason, the requirement 2.1.2 (clear explanation of what every element does) is not incorporated in the development of this sprint.

REQUIREMENTS TO DESIGN

Again, for the requirement, different mockups are made. In this case, the requirements that can be converted into visual mockups are 2.2.1, 2.2.1 and 3.2. The mockups are shown below.

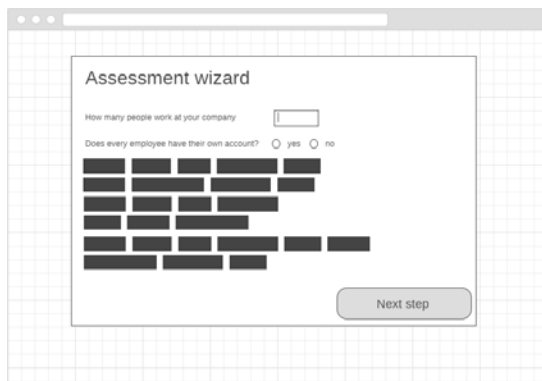


Figure 17 - Assessment wizard mockup

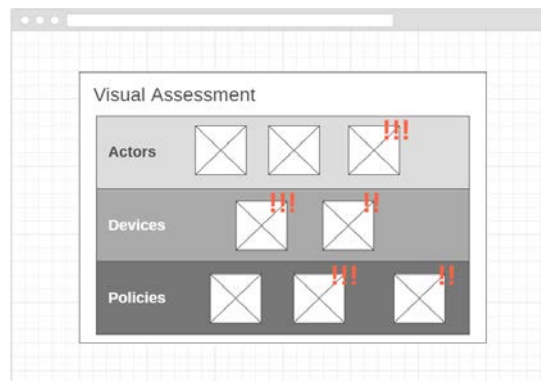


Figure 18 - Risks in visual assessment mockup

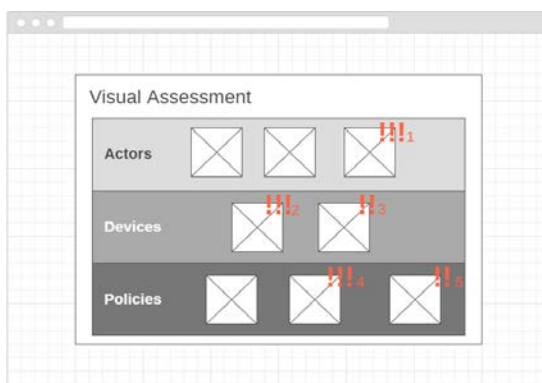


Figure 19 - Numbered risks in visual assessment mockup

Figure 17 is created to fit requirement 3.2, the user can use a wizard-like interface to create the first structure for a risk assessment. The page is designed to create a wizard-like feeling and let the user answer the most important questions for the base of the assessment. Figure 18 shows the risks within the visual representation

of the system. This way, the risks can be shown at the exact spot where they are caused. In the mockup, the severity of the risk is shown with the amount of exclamation marks that are displayed. In the implementation this will be translated into the colors of Table 8. Due to the simplicity that can be shown in a mockup, this is not yet incorporated. Also there will be an indicator for the severity of each risk.

While Figure 19 looks similar to Figure 18 it has one important addition to fulfill requirement 2.2.2: all the risks are numbered. With this numbering, a top 5 or top 10 risks can be easily displayed. This means that both the visual representation and the top 10 list-like representation will be in the design. These numbers will correspond to the spot in the top 10 risks. This means that the number 1 risk in the visual representation will also be the most severe risk.

Design implementation

While the previous discussed development sprints focus on the requirements and the visual aspects of those requirements, there are also choices made in the technical implementation of these requirements. These choices will be discussed in this paragraph, alongside with how the tool can be used by SMEs to do a risk assessment.

LANGUAGES AND FRAMEWORKS

The implementation of the tool will be done with PHP as main language. This is done due to the prior knowledge and experience with this language. It also is a perfect language for a web-based tool, as the language is designed for web development. For the database, MySQL will be used. The front-end will be programmed in HTML in combination with JavaScript. The frameworks that will be used are Laravel for PHP and jQuery for JavaScript. These choices are based on prior experiences and due to the fact that these are among the most used frameworks at the time of writing this. The tool will be open source and will be hosted on GitHub (thus using the version management software Git). The repository can be found at <https://github.com/roebenk/thesis>.

MODEL TO IMPLEMENTATION

The discussed model in the previous chapter needs implementation in the code. Because the components of the model are literally implemented in the design of the tool (actors, devices, assets, policies and the connections between them), this makes the implementation of the model relatively easy. An important aspect of the model is the knowledge base. The policies need to be stored in the database. For this purpose a table in the database is created that is similar to the structure that is shown in the appendix. The schema for this table is as follows:

Column name	Column type
id	INTEGER(11)
name	VARCHAR(255)
variant_name	VARCHAR(100)
variant_impact	DECIMAL(4,2)
works_on	VARCHAR(50)

Table 18 - Policies database schema

When using this schema, the table will be populated in the following way:

id	name	variant_name	variant_impact	works_on
1	Patch management	Weekly	0.9	device
2	Patch management	Monthly	0.8	device
..

Table 19 - Population of the policies schema

As can be seen, every policy has a *works_on* value, this can be an actor of device. The value of the policy will have an impact on the base value of the device. This base value is defined for every device and actor in the database as well.

USE OF THE TOOL

The source code of the tool is open source and can be downloaded from the GitHub repository. Before use, this however means that the code needs to be run on a web server with PHP installed. The documentation on how to install the tool on a web server can be found on the GitHub repository.

After installation, the crucial part of the effectiveness of the tool is the knowledge base. As described, the knowledge base is filled with rules to run a proof-of-concept, but these rules are not meant for a production environment. Because the tool is open source, the tool can be implemented and adapted by everyone that sees fit. This means that the knowledge base can be filled by individuals and used for their own purpose, keeping the structure of the tool. It of course also means that the knowledge base can be extended in the open source repository. Details on how to add value to the knowledge base can also be found in the repository.

SCREENSHOTS

The results of the development cycles give a proof of concept. In order to give an idea on how the translation from requirements to actual design is done, screenshots from the actual proof of concept are shown below.

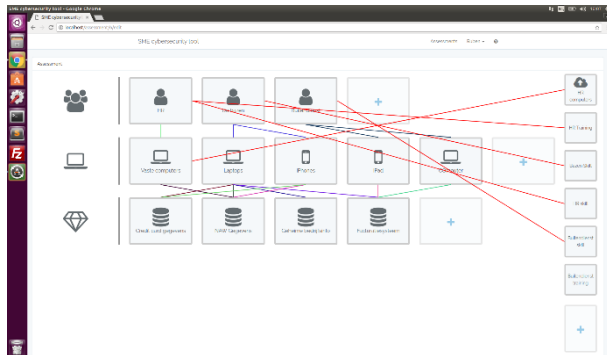


Figure 20 - Complete modelling overview

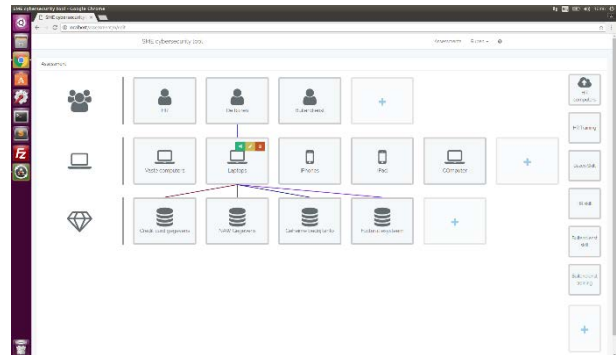


Figure 21 - Partial modelling overview

Figure 20 shows the overview in which the user can model the structure of the company. On the left side, from top to bottom, the actors, devices and assets are shown. On the right side, the policies are shown. The colored lines are the connections between these different blocks. Because the image can get cluttered due to the amount of connections, an extra option is built, in which the view can be uncluttered. Figure 21 shows that when hovering one of the blocks, only the connections for that specific block become visible.

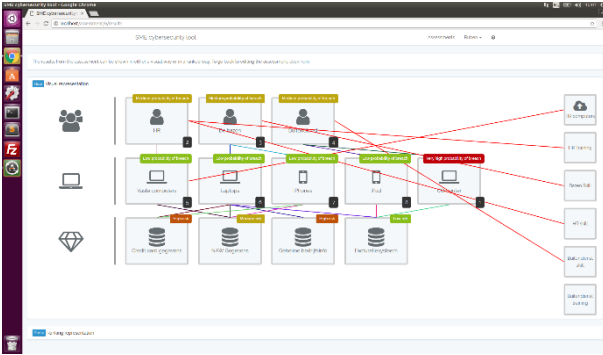


Figure 22 - Complete risk assessment overview

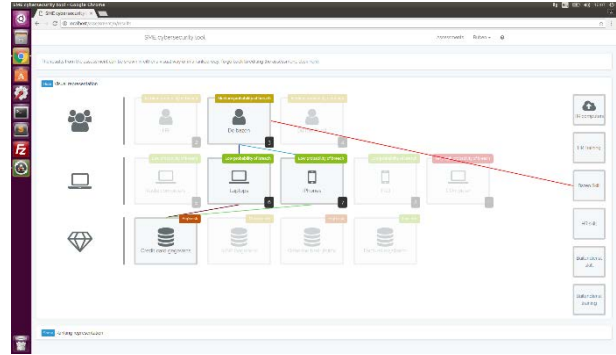


Figure 23 - Partial risk assessment overview

The same principle works for the risk assessment results page. In Figure 22 the different blocks are shown with the corresponding risks. The connections between the different blocks can clutter the view, thus a similar feature as in Figure 21 is implemented. When hovering over an asset, the complete influence on that asset can be viewed. This is shown in Figure 23.

As an addition to the visual representation in the results screen, a list with the different risks can also be shown. This can be seen in Figure 24. On the left, all the actors and devices with their corresponding breach probability are shown. On the right, the assets with their corresponding risks are shown.

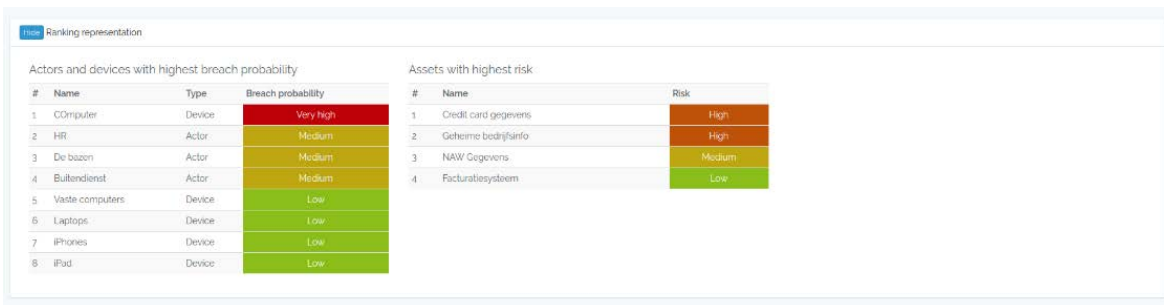


Figure 24 - Ranked visualization of risks

VALIDATION

The goal of this chapter is to validate the requirements that are created from literature and those that are created after the interview with the SME. The final requirements will also be validated by a final interview with a SME. The chapter also serves as a validation of the model that is created in order to calculate the risks that work on the modelled organization. This is done via an expert session with two information security consultants from KPMG. In this session the different design choices are made clear and both experts will give their insights on whether they think these requirements and choices make sense.

First the different requirements will be discussed, after which the validation of the model will be discussed.

Extracting findings

From the two interviews that are conducted and the expert session, certain findings are done. These are extracted from the summaries of the sessions and listed here. These findings can be used in order to validate the different requirements and model choices.

INTERVIEW 1

A summary of the interview can be found in Appendix E. The different statements that contribute to the validation of requirements are stated below.

- IV1 - a. A visual representation of the company was a preferred way
- IV1 - b. Block are a good way to construct the company in a visual manner
- IV1 - c. Icons were received as a good way to support the text in the blocks
- IV1 - d. No specific cybersecurity knowledge is present – and nor should it be required in order to use the proposed tool
- IV1 - e. It can be expected from the user that the user has a decent IT knowledge (described as the interviewee as medium-level system administrator)
- IV1 - f. The maximum time the SME is willing to invest is half a day, otherwise outsourcing is a better option
- IV1 - g. Visual representation of the risks is preferred – showing where in the system lie the weak spots
- IV1 - h. A top 10 list of these risks is also a good addition to the visual representation

In the conclusion of the validation of the requirements these statements will be linked to the different requirements that are validated.

INTERVIEW 2

A summary of the interview can be found in Appendix F. Just like the previous interview, the statements that are relevant for the validation of the requirements or the model will be listed.

- IV2 - a. A visual representation of the company structure is a good way
- IV2 - b. Blocks will support the visual representation

- IV2 - c. It is wise to separate the cybersecurity knowledge from the company structure
- IV2 - d. Visual representation and a top 10 lists are a good idea
- IV2 - e. Calculating the risks with the help of experts is a good idea
- IV2 - f. A web based application is a good choice for accessibility, but should be well secured in order to protect the data of users
- IV2 - g. The different components of the model are well chosen
- IV2 - h. The asset aspect of the model is less relevant according to the interviewee

EXPERT SESSION

The expert session gave insights into what experts think of the designed system, rather than what users think. This gives an idea of the actual functionality of the system, and if the requirements set will have the desired effect from a cybersecurity perspective. Again, the different statements are listed.

- ES - a. It is a good idea to make the tool web-based, this is proposed by one of the experts
- ES - b. The visual way of connecting blocks is seen as a good idea.
- ES - c. The combination with an initial wizard could have clear added value, as general questions (for example industry of the SME) can be asked
- ES - d. The level of expertise needed is seen as good for this tool, it is accessible enough for a SME to use
- ES - e. The separation of the different components should be adequate, but could use expansion
- ES - f. The way of estimating the probabilities is good and this method is used in big corporate settings as well
- ES - g. There is doubt about the fact that assets are breached in case one of the other components is breached. This is perspective question, but is agreed upon as adequate

Validating the requirements

The validation of the requirements will be done partly by doing interviews with SMEs and partly by the conducted expert session. The first interview conducted was for getting new requirements, but was also conducted in order to validate the set requirements as constructed from the literature. These statements all confirmed different requirements that are set. These requirements are listed in Table 20 with the corresponding statements.

Constraint	Description	Validated by
1.1	Web-based	ES – a IV2 – a
1.2	Easily redo a risk assessment	-
1.2.1	Authentication with saved assessments	-
1.2.2	Ability to manage multiple assessments	-
2.1	No technical cybersecurity terms used	ES – d IV1 – d IV1 – e IV2 – c

2.1.1	Level of terms used: system admin	IV1 – e
2.1.2	Clear explanation of what every element does	-
2.2	Clear vulnerabilities in the results	IV1 – g IV1 – h IV2 – d
2.2.1	Visual representation of weak spots	IV1 – g IV2 – d
2.2.2	Make clear what top 10 risks are	IV1 – h IV2 – d
3	Keep time investments under 0.5 day	IV1 – f
3.1	Simple to use interface	ES – b IV1 – a IV2 – a
3.1.1	Visual blocks to connect	ES – b IV1 – b IV2 – b
3.1.2	Intuitive icons in support of text	IV1 – c
3.2	Wizard to get started	ES – c

Table 20 - Validation of requirements

Validation of the model

The validation of the model could have been done with a case study. However, because of time constraints and the complexity of this way of validation, this is out of the scope of this research. With the help of the second interview and the expert session, the model is validated. In the expert session, it was confirmed that the structure of the proposed model is good (ES – e). While it could use expansion, due to the simplicity and scope this is a good start. This is also confirmed in the second interview (IV2 – g). In the second interview it also was stated that the asset component might be of less value than the other components (IV2 – h). Also the way of using experts in order to determine the probabilities of different aspects is one that is already been used in production, as confirmed by the expert session (ES – f). This separation of knowledge is also confirmed to be a wise modelling decision by the second interview (IV2 – c). In order to calculate the probability that an asset is breached, the assumption is made that when the device or actor that is connected to that asset is breached, the asset is breached as well. While there is some doubt about this structure, it is agreed upon that it is a perspective issue.

Conclusion

While most the requirements are confirmed by either the interviews or the expert session, some requirements remain unconfirmed. The requirements that were not validated should be looked at in possible future development sprints. But for now, they only find their origin and support in the existing literature.

Concerning the model, different aspects of the model were confirmed, but not the model as a whole. This has to do with that some aspects of the model cannot be validated by an expert session. This needs to be done with the help of data or a use case. Because this does not fit within the set time frame of this research, it is left out of the scope.

SYNTHESIS

In this chapter the conclusions, limitations and recommendations will be described.

Conclusions

With the help of the different research questions, the main research question will be answered. Each paragraph will handle one or more research questions and discusses how these questions are answered.

WHAT ARE THE MOST COMMONLY USED CYBERSECURITY FRAMEWORKS AND RISK ASSESSMENTS?

Based on a survey, the most used cybersecurity frameworks were discussed. These frameworks were the NIST Framework for Improving Critical Infrastructure Cybersecurity, the ISO27001 standard and the CIS Critical Security Controls for Effective Cyber Defense. The frameworks all have the similarity that they need to be used by people with knowledge of cybersecurity. The first two (NIST and ISO27001) are high level frameworks that only give areas in which a company should investigate; how this is done or how problems are solved is not discussed. The third framework (CIS controls) is different in that perspective, it is quite specific. While it is not as high level as the previous frameworks, it still requires a lot of knowledge, because controls cannot just be implemented without investigation on the vulnerable areas in IT security within the organization. This means that these most commonly used frameworks are not suited for SMEs, due to the required knowledge for using these frameworks.

Concerning the risk assessment part, there are a lot of methods available. To make a selection from these methods, a research by Dan Ionita is used. This research discusses a lot of different risk assessments methods and scores them on what the applicability of the method is. Based on the criteria of *suitable for SMEs* and *low level implementation* four methods remain. From these four (CORAS, Cramm, Mehari and NIST SP800-30) the Cramm and Mehari methods are both not actively supported anymore. This means that only the CORAS and NISTSP800-30 methods remain. In addition to these two methods, the TRESPASS method is added. This is done on the basis on another comparative study that compares CORAS to TRESPASS. What can be concluded is that all of the risk assessments provide clear steps in what to do in order to conduct the assessment. The thing all the methods have in common is the fact that the probabilities of the risks determined in the method need to be determined by the assessor. This requires a lot of knowledge on the subject and on the risks.

WHAT DOES THE EXISTING LITERATURE SAY ABOUT CYBERSECURITY FOR SMES?

There is quite some literature on cybersecurity in SMEs. However, this literature mostly confirms the problem that cybersecurity within SMEs is not at the desired level. A lot of literature also confirms that most cybersecurity frameworks and assessments are lacking in applicability for SMEs. They are either too complex, or too require an external expert, something that is too expensive. Still, some frameworks can be found to fit the needs of SMEs. The NIST has adapted the NIST Framework specifically for SMEs. This framework is perfect for SMEs, as it focusses on the right scope and structures this in such a way on how to tackle cybersecurity problems in the SME setting. However, it is basically a table that needs to be filled in, which indicates where

the most valuable assets of a company are. It does not indicate the specific weak points in the organization; something that is needed for SMEs.

The second framework specifically developed for SMEs is the ENISA Cloud Security Guide for SMEs. As the name suggests, it is only for cloud security. While the framework is indeed more suited for SMEs, the fact that it is only focused on cloud security makes it very limited. Another issue with the ENISA guide is the fact that it still requires a lot of knowledge from the cloud service providers; this knowledge is not something that always is at hand.

HOW CAN EXISTING FRAMEWORKS AND ASSESSMENT METHODS BE TAILORED FOR SMES?

The conclusion from the previous paragraphs is that both the existing risk assessments and frameworks do not fit SMEs. To fit the needs of SMEs, the method to model the structure of a company is adapted from the TRESPASS project. Because TRESPASS has a lot of options that are not relevant for SMEs, parts of the structure are used to fit the scope of SMEs better. The structure that remains consists of *policies*, *actors*, *devices* and *assets*. With these components, an organization can be structured. With this structure, the risks on the different assets needs to be determined. This is done by determining a base probability for a device that it will be breached, after which policies will decrease that breach probability. The calculations for this improvement are based on the Gordon-Loeb model, which states that every extra investment in cybersecurity will (relative to the previous) have less effect. This means that every extra policy will have less of an improvement than the previous one. In order to calculate the probability that works on the asset, the probabilities of all the actors and devices that work on the asset will be combined in order to determine the final probability. This probability will be multiplied with the value of the asset, which gives the final risk.

An important conclusion of this model is that the base probabilities and policy probability improvements need to be determined by experts. It cannot be expected that the user has the knowledge to estimate these numbers. Therefore, only the structure and the value of the assets needs to be determined by the user. This ensures that the knowledge of the risk probabilities is separated from the knowledge of the company.

WHAT ARE THE DESIGN REQUIREMENTS FOR A TOOL TO DO CYBERSECURITY RISK ASSESSMENTS SPECIFIC FOR SMES?

First the literature was used in order to determine requirements for the tool. What came to light was that SMEs do not have the time, resources or awareness to conduct a cybersecurity risk assessment. To overcome these issues, the requirements have to be aligned with the needs of SMEs. The first requirements, determined with literature, were validated and extended by means of an interview. The final list of requirements that was implemented in the tool can be found in Table 21.

Constraint	Description
1.1	Web-based
1.2	Easily redo a risk assessment
1.2.1	Authentication with saved assessments
1.2.2	Ability to manage multiple assessments

2.1	No technical cybersecurity terms used
2.1.1	Level of terms used: system admin
2.1.2	Clear explanation of what every element does
2.2	Clear vulnerabilities in the results
2.2.1	Visual representation of weak spots
2.2.2	Make clear what top 10 risks are
3	Keep time investments under 0.5 day
3.1	Simple to use interface
3.1.1	Visual blocks to connect
3.1.2	Intuitive icons in support of text
3.2	Wizard to get started

Table 21 - Final requirements

All of the requirements are aimed on the scope of SMEs. This means that all requirements ensure that SMEs do not need specific cybersecurity expertise, a lot of time or an external consultant in order to conduct this assessment.

HOW CAN THE TOOL BE BUILT?

Based on the requirements that were set, the best approach was a web-based tool. By keeping the interface intuitive by using visual elements, the use of the tool remains easy enough for SMEs. By implementing the knowledge base in such a way that it can be extended with ease, the tool can be used by anyone who sees fit. For this reason, the source code is open source, meaning that structure and calculations of the tool can be used in order to improve the results of a risk assessment.

DOES THE TOOL MEET THE REQUIREMENTS OF SMES?

The validation of the requirements is done with the help of interviews. These interviews do indeed confirm (most of) the requirements that are set. However, some requirements remain invalidated by means of the interviews. These requirements have their base in the literature, but need further validation in possible next development sprints.

WHAT WOULD A TOOL LOOK LIKE THAT HELPS SMES DO CYBER-RISK ASSESSMENTS AND POINT OUT THE WEAKNESSES IN THEIR CYBERSECURITY?

Finally, the main research question of this thesis needs an answer. It can be concluded that no tool exists that fills the void of cybersecurity assessments coming SMEs. To create a tool that is suited for SMEs, the different requirements as determined should be met. But more importantly, the knowledge for estimating the probabilities and risks of the system should be included in the tool. With other words, the user should not have to worry about this, but should only construct a model of their company. With the created model, this constraint is met, and it is possible for SMEs to do this risk assessment themselves. With the visual representation of both the model and the risks, a clear understandable risk assessment can be executed.

Discussion

The added value of this research lies in the structuring of a model (and tool) that can be used by SMEs. While there is a lot of literature on the fact that SMEs are lacking in the cybersecurity aspect [19, 40, 42-45, 61], there

is nothing that solves this problem. These researches indicate that the problems lies within the scope, resources and knowledge that are required for the current methods. However, this problem still remains not solved in the scientific literature. This research focusses on determining what requirements are necessary in order to create a tool that fits SMEs and thus overcomes the limitations that are already found in existing literature. It is important to notice that this is in no way an exhaustive set of requirements, as not all sectors or different kinds of SMEs are included in the research. However, it does provide a good start on which cybersecurity assessments for SMEs can be build.

The second part that adds value is the model that calculates the risks for the different components. While there were existing methods available, they were not suited for SMEs due to complexity reasons. For this reason, the adaption of these models creates a simplification that can be used specifically for SMEs. This is the reason that TRESPASS is used as a basis [37]. The essence of TRESPASS is the same, but SMEs require a simplified version for their use. This is combination with the adapted Gordon-Loeb model [55] makes it a suited risk calculation method specifically for SMEs.

Limitations

Even though the research brings forward meaningful results, compromises have been made in order to stay within the scope and time-limit. First, the determining of the requirements is done on the basis of literature and interview. This means that the requirements are not determined within a wide spectrum of different SMEs in different industries. This means that additional or changed requirements could be possible when expanding this process.

Concerning the model that determines where the risks in the system lie, this has not been validated by means of a case study. To do a case study, it would require the full cooperation of an SME, a lot of data concerning possible breaches or attacks, a complete mapping of their IT structure and a long period of time to confirm results. These were all aspects that would not fit in the scope of this research, therefore a case study is not done and the validation is done with the help of experts. In this validation session, different aspects came forward that additions to the model could be done, but that this should be done carefully in order to ensure the accessibility for SMEs.

In the calculations of the model, the assumption is made that probabilities are independent. This is done in order to keep the model simple. However, it might not be that these probabilities are independent. Because the relations between these probabilities is not within the scope of this research, the probabilities are seen as independent.

Furthermore, the rules that fill the knowledge base are not exhaustive. This is a clear limitation of the working of the tool right now, but is not limitation for the theory and workings behind the model and tool. While the tool delivered for this thesis merely serves as a proof of concept, with the expansion of the knowledge base, the tool could be more widely used. Again, this is a clear choice in this research, as the creation of a big knowledge base would have been out of the scope and would not contribute to the validation of the proof of concept.

Recommendations and future work

Based on the conclusion, discussion and limitations there are recommendations for future research.

With the end product of this research, a validation by the means of a case study should give insights in the actual effectiveness of the model and tool. What kind of effect does it have on SMEs and are those positive effects? This will also give insights in whether the model should be expanded or not. When using the model with SMEs in a real situation, the need for extra components will become clear.

As mentioned in the limitations, the perspective of the attacker should be incorporated (implicitly) in the model. In the expert session it was addressed that one solution to keep it generic (and thus accessible) is the implementation of what the industry of the SME is. This is more specific than the implementation now, as it gives more information on who the possible attacker might be, but still keeps it generic enough to be used by SMEs. The structure of the model and tool are created in such a way that the implementation of an attacker profile is easy to do, however, it should be confirmed in future research how to take this into the calculations.

Because of time limitations, the determining of the rules is a brief process in this research. In future research this knowledge base could be extended in such a way that the risk assessment process will be more complete. With the addition of extra rules, this tool could go in production and could be tested by real SMEs.

The model is a very simplified view of the reality. In this model, the value of an asset can be indicated. This means that risk is calculated on the basis of that value. However, it could be incorporated that when an asset is breached, this has a severe impact on the image of the company. The impact on the image is something that needs further research.

What is not included in this research is the risk that incorrect data brings. When the data that is inputted by the user is not correct, this has impact on the results of the tool. How big this impact is, is not researched. A sensitivity analysis could give insights in the impact of wrong inputs and show how big this impact is.

REFERENCES

- [1] CBS. (2016). *Acht procent van de Nederlanders nooit op internet*. Retrieved from: <https://www.cbs.nl/nl-nieuws/2016/22/acht-procent-van-de-nederlanders-nooit-op-internet>.
- [2] Eurostat, "Digital economy and society statistics - households and individuals," 2016, Retrieved from: http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage, Accessed on: 08-06-2017.
- [3] Google. (2017). *Google Trends - Cyber Security*. Retrieved from: <https://trends.google.nl/trends/explore?q=cyber%20security>. Accessed on 08-06-2017.
- [4] Cambridge University, "Cambridge Business English Dictionary," in *Cambridge Business English Dictionary*, C. U. Press, Ed., ed. Cambridge: Cambridge University Press, 2011, p. 958.
- [5] T. R. Peltier, *Information Security Risk Analysis*. Boca Raton: Auerbach Publications, 2005.
- [6] J. A. Jones, "An Introduction to Factor Analysis of Information Risk (FAIR)," in "Risk Management Insight," 2005.
- [7] CBS, "De staat van het MKB 2015," 2015, Retrieved from: <https://www.cbs.nl/nl-publicatie/2015/48/de-staat-van-het-mkb-2015>, Accessed on: 07-03-2017.
- [8] Eurostat, "Dependent and independent SMEs and large enterprises," 2015, Retrieved from: http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises#Main_statistical_findings, Accessed on: 08-06-2017.
- [9] Interpolis, T. Nipo, and Capgemini, "Cybersecurity in het MKB," 2015, Retrieved from: https://www.interpolis.nl/~media/files/ebook_cybersecurity_in_het_mkb.pdf, Accessed on: 07-03-2017.
- [10] S. Veenstra, R. Zuurveen, and W. Stol, "Cybercrime onder bedrijven," 2015, Retrieved from: <https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/Cybercrime%20onder%20bedrijven%20definitief%20rapport.pdf>, Accessed on: 07-03-2017.
- [11] KPMG, "Small Business Reputation & The Cyber Risk," 2015, Retrieved from: <https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf>, Accessed on: 07-03-2017.
- [12] Experian, "SME's under threat," Experian, Nottingham 2017.
- [13] NCSC, "Cybersecuritybeeld Nederland 2016: Beroepscriminelen steeds groter gevaar voor digitale veiligheid in Nederland | NCSC," 2016, Retrieved from: <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2016/1/CSBN2016.pdf>, Accessed on: 07-03-2017.
- [14] I. Ilvonen, "Information security management in Finnish SMEs," in *Proceedings of the 5th European Conference on Information Warfare and Security, Helsinki, Finland, 1-2 June 2006*: Academic Conferences Limited, 2006, pp. 161-168.
- [15] Ponemon Institute LLC, "2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)," 2016, Retrieved from: https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf, Accessed on: 07-03-2017.
- [16] T. Kurpjuhn, "The SME security challenge," *Computer Fraud & Security*, vol. 2015, no. 3, pp. 5-7, 3// 2015.
- [17] B. Blakely. (2002). *Lock IT Down: Consultants can offer remedies to lax SME security*. Retrieved from: <http://www.techrepublic.com/article/lock-it-down-consultants-can-offer-remedies-to-lax-sme-security/>. Accessed on 03-04-2017.
- [18] D. Kelleher. (2009). *SME security: SME mindset must change*. Retrieved from: <https://www.scmagazine.com/sme-security-sme-mindset-must-change/article/555835/>. Accessed on 03-04-2017.
- [19] V. Dimopoulos, S. Furnell, M. E. Jennex, and I. Kritharas, "Approaches to IT Security in Small and Medium Enterprises," presented at the 2nd Australian Information Security Management Conference, Perth, 2004.
- [20] A. Smears, "Information Security Management Systems in Small & Medium Sized Enterprises," in "GIAC Security Essentials Certification," SANS Institute 2003.
- [21] H. Verhagen, "De Economische en Maatschappelijke Noodzaak van meer Cyber Security," Cyber Security Raad 2016.

- [22] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly: Management Information Systems*, Article vol. 28, no. 1, pp. 75-105, 2004.
- [23] M. Stoica, M. Mircea, and B. Ghilic-Micu, "Software development: Agile vs. traditional," *Informatica Economica*, vol. 17, no. 4, p. 64, 2013.
- [24] C. Wohlin and A. Aybuke, *Engineering and Managing Software Requirements*. Springer-Verlag New York, Inc., 2005.
- [25] I. Inayat, S. S. Salim, S. Marczak, M. Daneva, and S. Shamshirband, "A systematic literature review on agile requirements engineering practices and challenges," *Computers in Human Behavior*, vol. 51, pp. 915-929, 2015/10/01/ 2015.
- [26] J. Karlsson, C. Wohlin, and B. Regnell, "An evaluation of methods for prioritizing software requirements," *Information and Software Technology*, vol. 39, no. 14-15, pp. 939-947, 1998.
- [27] K. Boness and R. Harrison, "Goal sketching: Towards agile requirements engineering," in *Software Engineering Advances, 2007. ICSEA 2007. International Conference on*, 2007, pp. 71-71: IEEE.
- [28] Dimensional Research, "Trends in Security Framework Adoption - A Survey of IT and Security Professionals," Dimensional Research2016.
- [29] NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. Accessed on 10-03-2017.
- [30] *ISO 27001*, 2015.
- [31] CIS, "The CIS Critical Security Controls for Effective Cyber Defense," The Center for Internet Security2016.
- [32] CIS. (2017). *About us*. Retrieved from: <https://www.cisecurity.org/about-us/>. Accessed on 22-05-2017.
- [33] D. Ionita, "Current Established Risk Assessment Methodologies and Tools," Master, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, 2013.
- [34] O. Gadyatskaya, K. Labunets, and F. Paci, "Towards empirical evaluation of automated risk assessment methods," in *International Conference on Risks and Security of Internet and Systems*, 2016, pp. 77-86: Springer.
- [35] M. S. Lund, B. Solhaug, and K. Stlen, *Model-Driven Risk Analysis: The CORAS Approach*. Springer Publishing Company, Incorporated, 2010, p. 400.
- [36] NIST, "Guide for Conducting Risk Assessments," NIST, Gaithersburg2012.
- [37] The TRESPASS Project. (2017). *The TRESPASS Project*. Retrieved from: <https://www.trespass-project.eu/>. Accessed on 09-10-2017.
- [38] W. Pieters, C. W. Probst, and J. Willemsen, "The Attack Navigator," in *Graphical Models for Security: Second International Workshop, GraMSec 2015, Verona, Italy, July 13, 2015, Revised Selected Papers*, S. Mauw, B. Kordy, and S. Jajodia, Eds. Cham: Springer International Publishing, 2016, pp. 1-17.
- [39] S. Parkin, A. Fielder, and A. Ashby, "Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes," presented at the Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, Vienna, Austria, 2016.
- [40] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13-23, 2016.
- [41] CREST. (2017). *Cyber Essential Scheme*. Retrieved from: <http://cyberessentials.org>. Accessed on 14-08-2017.
- [42] J.-Y. Park, R. J. Robles, C.-H. Hong, S.-S. Yeo, and T.-h. Kim, "IT Security Strategies for SME's," *International journal of software engineering and its applications*, vol. 2, no. 3, pp. 91-98, 2008.
- [43] S. Pritchard, "Navigating the black hole of small business security," *Infosecurity*, vol. 7, no. 5, pp. 18-21, 2010/09/01/ 2010.
- [44] I. Lopes and P. Oliveira, "Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises," in *WorldCIST (1)*, 2015, pp. 459-468.
- [45] L. E. Sánchez, A. Santos-Olmo, E. Fernández-Medina, and M. Piattini, "Security Culture in Small and Medium-Size Enterprise," in *ENTERprise Information Systems: International Conference, CENTERIS 2010, Viana do Castelo, Portugal, October 20-22, 2010, Proceedings, Part II*, J. E. Quintela Varajão, M. M. Cruz-Cunha, G. D. Putnik, and A. Trigo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 315-324.
- [46] C. Paulsen and P. Toth, "Small Business Information Security: The Fundamentals," NIST2016, Retrieved from: <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>, Accessed on: 10-03-2017.

- [47] D. Assante, M. Castro, I. Hamburg, and S. Martin, "The Use of Cloud Computing in SMEs," *Procedia Computer Science*, vol. 83, pp. 1207-1212, 2016/01/01/ 2016.
- [48] ENISA, "Cloud Security Guide for SMEs," European Union Agency for Network and Information Security 2015.
- [49] B. Schneier, "Attack trees," *Dr. Dobbs's journal*, vol. 24, no. 12, pp. 21-29, 1999.
- [50] T. R. Ingoldsby, "Attack tree-based threat risk analysis," *Amenaza Technologies Limited*, pp. 3-9, 2010.
- [51] G. McGraw and J. Viega, "Building secure software," in *RTO/NATO Real-Time Intrusion Detection Symp*, 2002.
- [52] Smith, Reid G., "Knowledge-Based Systems - Concepts, Techniques, Examples ", ed, 1985.
- [53] K. Goztepe, "Designing fuzzy rule based expert system for cyber security," *International Journal of Information Security Science*, vol. 1, no. 1, pp. 13-19, 2012.
- [54] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach," *IEEE transactions on software engineering*, vol. 21, no. 3, pp. 181-199, 1995.
- [55] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438-457, 2002.
- [56] L. A. Gordon, M. P. Loeb, and L. Zhou, "Investing in Cybersecurity: Insights from the Gordon-Loeb Model," *Journal of Information Security*, vol. 7, no. 02, p. 49, 2016.
- [57] A. A. Lazakidou, *Web-based applications in healthcare and biomedicine*. Springer Science & Business Media, 2009.
- [58] H. H. Chang and S. W. Chen, "The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator," *Computers in Human Behavior*, vol. 24, no. 6, pp. 2927-2944, 2008.
- [59] C. Egido and J. Patterson, "Pictures and category labels as navigational aids for catalog browsing," presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Washington, D.C., USA, 1988.
- [60] J. Tidwell, *Designing interfaces: Patterns for effective interaction design*. " O'Reilly Media, Inc.", 2010.
- [61] A. Santos-Olmo, L. Sánchez, I. Caballero, S. Camacho, and E. Fernandez-Medina, "The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets," *Future Internet*, vol. 8, no. 3, p. 30, 2016.

APPENDIX A – LITERATURE RESEARCH

Search engine used	Terms used
Google Scholar / Scopus	<ul style="list-style-type: none">• (Cybersecurity OR cyber security OR security) <i>AND</i><ul style="list-style-type: none">○ Risk assessment○ Framework○ SME○ SMB○ Small medium enterprise• Design science• Agile <i>AND</i><ul style="list-style-type: none">○ Software development○ Development○ Requirements engineering• Requirements <i>AND</i><ul style="list-style-type: none">○ Engineering○ Elicitation○ Prioritization○ Modeling• Attack tree <i>AND</i><ul style="list-style-type: none">○ Cybersecurity <i>AND</i><ul style="list-style-type: none">▪ Risk○ Security <i>AND</i><ul style="list-style-type: none">▪ Risk

APPENDIX B – REQUIREMENTS PRIORITIZATION SPRINT 1

	Importance	Time	2nd root of product	Priority Vector
Importance	1,000	1,500	1,581	0,551
Time	0,667	1,000	1,291	0,449
Sum	1,667	2,500	2,872	1,000
Sum*PV	0,918	1,124		
Lambda Max	2,041			
CI	0,041			
CR	0,041			

Importance

	1.1	1.2.1	1.2.2	2.1	2.2	3.1.1	3.1.2	3.2	8th root of product	Priority vector
1.1	1,000	3,000	2,000	1,000	2,000	1,000	3,000	1,500	1,397	0,134
1.2.1	0,333	1,000	0,500	0,500	1,000	0,333	1,000	1,000	1,242	0,120
1.2.2	0,500	0,500	1,000	1,000	1,000	2,000	2,000	1,000	1,316	0,127
2.1	1,000	1,000	1,000	1,000	2,000	2,000	2,000	1,500	1,357	0,131
2.2	0,500	0,500	1,000	0,500	1,000	1,000	1,000	0,500	1,251	0,120
3.1.1	1,000	1,000	0,500	0,500	1,000	1,000	2,000	2,000	1,316	0,127
3.1.2	0,333	0,333	0,500	0,500	1,000	0,500	1,000	1,000	1,228	0,118
3.2	0,667	0,667	1,000	0,667	2,000	0,500	1,000	1,000	1,286	0,124
Sum	5,333	8,000	7,500	5,667	11,000	8,333	13,000	9,500	10,394	1,000
Sum*PV	0,717	0,956	0,950	0,740	1,324	1,055	1,536	1,176	8,453	
Lambda	8,453									
CI	0,065									
CR	0,046									

Time

	1.1	1.2.1	1.2.2	2.1	2.2	3.1.1	3.1.2	3.2	8th root of product	Priority vector
1.1	1,000	1,500	2,000	0,500	2,000	3,000	1,000	2,000	1,378	0,131
1.2.1	0,667	1,000	2,000	0,333	2,000	2,000	0,500	1,000	1,325	0,126
1.2.2	0,500	0,500	1,000	0,500	1,000	1,000	0,500	0,500	1,238	0,118
2.1	2,000	2,000	2,000	1,000	2,000	2,000	1,000	2,000	1,391	0,133
2.2	0,500	0,500	1,000	0,500	1,000	1,000	0,333	1,000	1,247	0,119
3.1.1	0,333	0,333	1,000	0,500	1,000	1,000	0,333	1,000	1,238	0,118
3.1.2	1,000	1,000	2,000	1,000	3,000	3,000	1,000	2,000	1,391	0,133
3.2	0,500	0,500	2,000	0,500	1,000	1,000	0,500	1,000	1,275	0,122
Sum	6,500	7,333	13,000	4,833	13,000	14,000	5,167	10,500	10,482	1,000
Sum*PV	0,855	0,927	1,535	0,641	1,546	1,653	0,686	1,278	9,120	
Lambda	9,120									
CI	0,160									
CR	0,113									

	Importance	Time	Score
	0,551	0,449	1,000
1.1	0,134	0,131	0,133

#	Requirement	Score
1	1.1	0,133
2	2.1	0,132

1.2.1	0,119	0,126	0,123
1.2.2	0,126	0,118	0,123
2.1	0,130	0,133	0,132
2.2	0,120	0,119	0,120
3.1.1	0,124	0,118	0,123
3.1.2	0,117	0,133	0,125
3.2	0,130	0,122	0,123
	1,000	1,000	1,000

3
4
5
6
7
8

3.1.2	0,125
1.2.2	0,123
3.1.1	0,123
1.2.1	0,123
3.2	0,123
2.2	0,120

APPENDIX C – REQUIREMENTS PRIORITIZATION SPRINT 2

	Importance	Time	2nd root of product	Priority Vector
Importance	1,000	1,500	1,581	0,551
Time	0,667	1,000	1,291	0,449
Sum	1,667	2,500	2,872	1,000
Sum*PV	0,918	1,124		
Lambda Max	2,041			
CI	0,041			
CR	0,041			

Importance

	2.1.1	2.1.2	2.2.1	2.2.2	3.2	5th root of product	Priority vector
2.1.1	1,000	2,000	0,750	0,750	0,333	1,370	0,197
2.1.2	0,500	1,000	0,333	0,333	0,333	1,201	0,173
2.2.1	1,333	1,333	1,000	1,000	1,000	1,415	0,203
2.2.2	1,333	1,333	1,000	1,000	1,000	1,415	0,203
3.2	3,000	3,000	1,000	1,000	1,000	1,552	0,223
Sum	7,167	8,667	4,083	4,083	3,667	6,953	1,000
Sum*PV	1,413	1,497	0,831	0,831	0,818	5,390	
Lambda	5,390						
CI	0,097						
CR	0,069						

Time

	2.1.1	2.1.2	2.2.1	2.2.2	3.2	5th root of product	Priority vector
2.1.1	1,000	3,000	1,000	1,000	2,000	1,516	0,220
2.1.2	0,333	1,000	0,500	0,500	1,000	1,272	0,185
2.2.1	1,000	1,000	1,000	1,000	2,000	1,431	0,208
2.2.2	1,000	1,000	1,000	1,000	1,000	1,380	0,200
3.2	0,500	0,500	0,500	1,000	1,000	1,285	0,187
Sum	3,833	6,500	4,000	4,500	7,000	6,883	1,000
Sum*PV	0,844	1,201	0,832	0,902	1,306	5,086	
Lambda	5,086						
CI	0,021						
CR	0,015						

	Importance	Time	Score
	0,551	0,449	1,000
2.1.1	0,197	0,220	0,207
2.1.2	0,173	0,185	0,178
2.2.1	0,203	0,208	0,205
2.2.2	0,203	0,200	0,202
3.2	0,223	0,187	0,207
	1,000	1,000	1,000

#	Requirement	Score
1	2.1.1	0,207
2	3.2	0,207
3	2.2.1	0,205
4	2.2.2	0,202
5	2.1.2	0,178

APPENDIX D – INTERVIEW GUIDE

1.1. Part A, Introduction

- The interviewer shortly present the topic and the research question.
- The interviewer points out that the interview is anonymous
- The interview asks for permission to record the interview, in order to facilitate data analysis later on.
- The interviewer also points out that the interview will receive the transcribed interview once it is available and may review it and/or object to some of the stated points.

1.2. Part B, Demographic Questions

1. In which role do you work at [company]?
2. Could you shortly introduce your work at [company]?

1.3. Part C, Topic Questions

GENERAL

1. How many employees does your company have?
2. How many of these employees use computers / smartphones for their work?
3. Are the devices used company owned or personally owned?
4. Are their policies on cyber security within the company?
 - a. Access and identity management?
 - b. Software update?
 - c. Server management?
 - d. Password policies?
 - e. Pen testing on systems?
5. Is someone responsible for the cyber security within the company?
6. Have you ever done an analysis of the cyber security state within your company?
 - a. Yes, how?
 - i. Tool? Consultancy?
 - b. No, why not?
7. Are you facing problems with cybersecurity right now?
 - a. If so, what are those problems?

TOOL

1. Would you use a tool to map the state of the cyber security within your company?
 - a. What requirements can you think of when you think of such a tool?
2. What would you like to be the results of such a tool?
 - a. As a result, would you like to see the threats with the highest risk only, of do you want general recommendations in solving these risks as well?

3. How much time would you be willing to invest in using this tool?
4. Do you prefer a checklist style tool or a more graphical interface?
5. How would the input look like?

Explain how the tool should look and show example images

6. What is your first impression of the example images?
7. Does this look like a good interface for such a tool?
 - a. If not, what would be better?

APPENDIX E – SUMMARY FIRST INTERVIEW

The interview is conducted at a small IT oriented company. The interviewee is, together with one other, responsible for the management of the whole company. He is responsible for the technical aspects of the company; including the IT. The company creates sensors that are used in all kinds of applications and is a company with 8 FTE. These sensors collect a lot of data, which is all stored by the company. The interview starts with an introduction on what the research is and what the goal of the interview is.

Every employee uses a computer or smartphone for their work. All these devices are company-owned. There are no policies concerning cyber security in the company. He states that all devices are company owned, and users cannot access these outside of work hours. Policies is defined as certain rules that employees have to follow; those are non-existent. There are however certain policies on IAM and patch management. Every user uses their own account. File structure is configured in such a way that not everybody has access to all data. This goes for all data. The system admin ensures that virus scan is updated and software is updated. Password manager is used, but every employee has access to this manager. Servers for web applications are used, patches are done, but there is no clear policy on this. No penetration testing is done. No one is explicitly responsible for the cybersecurity, the owners (/ directors) are responsible. No tool or consulting has ever been used to check on the cybersecurity of the company. This is mainly due to lack of resources and time. The company has never been breached.

If a tool proposed in the research should be available, the tool would be used. Expertise to use the tool needs to be set on medium system admin level, so an employee that has knowledge of the IT in the company. Time used for the tool, maximum of half a day; otherwise the assessment will be outsourced due to lack of resources. At first, the results should be shown in a top 10 list, and explicitly show what is the impact of such a risk. Show different aspects of the company in the results. When given the choice, a graphical way of building the company within the tool is a better way than just questions. This has a bigger preference and is easy to extend. Checklist is not appealing enough. When showing the mockups of the tool, these were confirmed as being suitable and appealing. In the results mockup, the attack tree result was experienced as a good alternative to a list of risks. In the visualization of the company, this could be a good way of showing the risks. Visual = more attractive.

Overall, wrapping up, the idea and visualization of the tool is a great way of mapping the organization and seeing where the risks are.

APPENDIX F – SUMMARY SECOND INTERVIEW

The interview is conducted with a security officer of a SME with approximately 40 FTE. The company is a software vendor and is thus IT oriented.

When asked what the first expectations of such a tool are from the side of the interviewee two sides are mentioned. On the one hand the side of the simple policies in a company (think of firewalls, updates, and exit policy). On the other hand, the human side. This is according to the interviewee even more important. This is the awareness and skills that employees have. The model that is created in this research is presented and the interviewee confirms that this is exactly what he is been talking about. Also the fact that it is a visual representation is very good. The asset part of the model is less relevant for him, he describes that the assets should be inherent. The interviewee states that there do not need to be concrete solutions within the tool, it is about creating awareness and showing that there are weaknesses. The concrete implementations of those solutions should always be done by experts. He confirms that the probabilities of these implementations should not be determined by the user, because they will not estimate it right. The way this is implemented in the model right now (by means of experts) is a good implementation according to the interviewee. The fact that it is a web based app is also good, as it is accessible. Displaying the results in the visual structure that is proposed is also seen as good, just like the top 10 risks.

APPENDIX G – SUMMARY EXPERT SESSION

The idea is introduced and the base for the idea is explained. In this introduction the idea that the interface is web based, is seen as a good idea. Roy shows a project they are working on right now. In this project, they are quantifying risk in the same way I propose to do it today. They look at the different things that can go wrong, and different controls (policies in this research) lower the chance of a breach with 2.7%. They state that if an attacker is inside the system, the attacker can access all. In the project Roy describes, the impact of a breach is described in different aspects. The percentages of breaches are determined with subject matter experts – like this session. This validates the core idea of this model, as the way KPMG is handling these calculations is similar to what this research proposes, only on a smaller scale to keep it within the scope. The assumption is stated that an attacker is the same for every SME, in order to keep the research within the scope. It is mentioned that SMEs exist in all different industries, and while the idea is good, what kind of attacker is in a lot of cases determined by the industry a company works in. This could be something for future research. This can be implemented with different sectors or with values for the assets. This value for different assets is already implemented in the current model, this idea is proposed and confirmed as added value for an asset. The question is posed if servers are incorporated in the model. This is not the case. It is stated that an attack path is often via a server. Assets or often on servers, so how to classify it. The problem that is stated that when incorporating servers into the model, this makes it more complex. The question is if this is within the scope of the research or if it fits in the model. Another thing that is important are intrusion detection or network segregation, how are these implemented. This can also be implemented as a policy. It might be a good addition of policies can have an effect on the whole company.

The next question is, why is the structure actor -> device -> asset? When explained that this is because this makes in tangible for the user of the tool. This sounds logical to the experts, and could work in their opinion. The problem with the structure is that it implicitly states that the actor and device should both be breached in order to get to the asset. But the conclusion is that when one of both need to be breached in order to get to the asset. This is confirmed by the experts. The implementation of the model is correct.

- In the final part of the expert session, the rules for the knowledge base were determined. For an overview of what the rules that are determined are, see appendix H.

APPENDIX H – RULES FROM EXPERT SESSION

Different devices

ID	Device	Variant	Risk
d1	Computer	Windows XP	0.95
d2	Computer	Windows 7	0.75
d3	Computer	Windows 8	0.65
d4	Computer	Windows 10	0.3
d5	Computer	Mac	0.3
d6	Phone	Android	0.25
d7	Phone	iPhone	0.25
d8	Phone	Windows	0.25
d9	Tablet	Android	0.25
d10	Tablet	iPad	0.25
d11	Tablet	Windows	0.25

Rules on devices

ID	Works on	Name	Value	Risk
rd1	Computer	Patch Frequency	Weekly	0.8
rd2	Computer	Patch Frequency	Monthly	0.7
rd3	Computer	Virus Scan	Yes	0.3
rd4	Computer	2FA	Yes	0.5
rd5	Computer	Password policy	Yes	0.1
rd6	Computer	Only allow encrypted USB	Yes	0.1
rd7	Computer	VPN required	Yes	0.1
rd8	Computer	Disable old protocols	Yes	0.4
rd9	Computer	User permissions configured	Yes	0.4
rd10	Phone/Tablet	Patch Frequency	Weekly	0.5
rd11	Phone/Tablet	Patch Frequency	Monthly	0.5
rd12	Phone/Tablet	VPN required	Yes	0.1
rd13	Phone/Tablet	Password policy	Yes	0.1
rd14	Phone/Tablet	Jailbreak / Root policy	Yes	0.2
rd15	Phone/Tablet	Remote wipe	Yes	0.4

Rules on actors

ID	Works on	Name	Value	Risk
ar1	Actor	Cybersecurity Training	Yearly	0.5
ar2	Actor	Cybersecurity Training	6 monthly	0.8
ar3	Actor	IT Skill	High	0.8
ar4	Actor	IT Skill	Medium	0.6
ar5	Actor	IT Skill	Low	0.4