TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Risto Kasepuu 192562IVCM

DESIGNING AN ARTIFACT TO SUPPORT CYBERSECURITY POLICY DEVELOPMENT IN SMALL AND MEDIUM ENTERPRISES

Master's thesis

Supervisors: Mika Juha Kerttunen
Andro Kull
PhD

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Risto Kasepuu 192562IVCM

VÄIKESTES JA KESKMISE SUURUSEGA ETTEVÕTETES KÜBERTURBE REEGLITE ARENDAMISEKS ETTE NÄHTUD ABIVAHENDI LOOMINE

Magistritöö

Juhendajad: Mika Juha Kerttunen
Andro Kull
PhD

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the materials used, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Risto Kasepuu

14.05.2021

Abstract

Cybersecurity responsibilities and risks in small and medium businesses are often blurred, without a responsible person assigned to them. They are frequently neglected based on the hope that cybersecurity-related incidents would not occur. There is a presumption that a small enterprise is not an attractive enough target for adversaries due to its size. However, sometimes crucial risks are missed entirely. What happens when a company's business-critical data is lost, inaccessible, or finds itself in the possession of a competitor? What circumstances can occur, and is the risk acceptable?

Meanwhile, cyberattacks escalate every year, and adversaries possess a growing arsenal of different attack tools.

It is more important than ever to use every solution available to understand the primary cybersecurity risks, their mitigations, and to form them into a document used in different organisational structures.

This thesis proposes a software artefact that helps SMEs establish a baseline security document by compiling a cybersecurity policy.

Keywords: information security, cybersecurity, policy, rules, computerised tool, SME, tool for small and medium businesses.

The thesis is written in English and is 75 pages long, including 7 chapters, 14 figures, and 10 tables.

Annotatsioon

VÄIKESTES JA KESKMISE SUURUSEGA ETTEVÕTETES KÜBERTURBE REEGLITE ARENDAMISEKS ETTE NÄHTUD ABIVAHENDI LOOMINE

Küberturvalisuse vastutus ja riskid on väikestes ja keskmise suurusega ettevõtetes sageli defineerimata ja ilma konkreetse vastutajata, ajendatud lootusest, et nendega küberintsidente ei juhtu. Valitseb eeldus, et väikeettevõted pole ründajatele atraktiivne sihtmärk. Kuid tihti hinnatakse neid riske valesti. Mis juhtub, kui ettevõtte ärikriitilised andmed on kadunud, ligipääsmatud või konkurendi valduses? Milline on sellisel juhul ettevõtte jätkusuutlikus? Kas sellised riskid on aktsepteeritavad?

Küberrünnakute sagedus kasvab aastalt aastasse ja ründajate käsutuses on aina laiem arsenal erinevaid ründevahendeid.

Olulisem kui kunagi varem on kasutada kõiki olemasolevaid lahendusi peamiste küberturvalisuse riskide ja nende vältimise lahenduste mõistmiseks ning teabe vormistamiseks dokumentideks, mida saavad kasutada erinevad organisatsiooni osad.

Selles magistritöös pakutakse välja abivahend (tehis), mis aitab väikestes ja keskmise suurusega ettevõtetes luua küberturbe eeskirjade algdokumendi.

Märksõnad: infoturve, küberturve, küberturvalisus, poliitika, reeglid, arvutipõhine tööriist, VKE, tööriist väikeste ja keskmise suurusega ettevõtetele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 75 leheküljel, 7 peatükki, 14 joonist, 10 tabelit.

List of abbreviations and terms

CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIS	Centre for Internet Security
DS	Design Science
DSRM	The design science research methodology
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
EU	European Union
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
ISO	International Organization for Standardisation
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISP	Information security policy
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
POS	Point of sales
SME	Small and medium-sized enterprises
TUT	Tallinn University of Technology

Table of contents

List of figures

List of tables

1 Introduction

Cybersecurity-related incidents are continuously growing and causing more financial and data losses than ever. As ENISA [1] Threat Landscape Report 2020 reveals, adversaries are launching better targeted and more complex cyberattacks than before. The attacks are extensive, and what is the most concerning factor: most of the victims do not know they were involved in any of the cybersecurity incidents. The same study explains that the top motivation of cyberattacks is monetary. Adversaries are also targeting state secrets and intellectual property that indicates state-sponsored interests.

At the same time, SMEs are more reliant on IT systems than ever. As the systems grow and become more complex, the state of mind remains mostly the same: that because of their size, they are not a worthy target. Unfortunately, SMEs are an easier target since they use minimum cybersecurity standards [2]. This is because SME size usually employs outsourced IT management services, and sometimes there are no IT management services. These factors might delay preventive measures or mitigations of cybersecurity incidents when a real-life event occurs.

As the research of this thesis found, most companies do not have any regulation or an enforced action plan, which can cause serious problems for business continuity. The thesis demonstrates that some of the SMEs are missing cybersecurity knowledge and are therefore more likely victims of cyberattacks. This is caused by the nature of SMEs—they are small and medium enterprises whose primary goal is to manage the company at the best levels and pass any overheads.

The thesis draws inspiration from conversations with several SMEs who confirmed that Cybersecurity related topics and documentation are often neglected. There are no reasonable solutions with limited resources and limited knowledge in such enterprises, sometimes only with one or two employees to help create even a basic cybersecurity policy template. Most of the software tools available focus on the cybersecurity risks assessment part and are targeted at advanced users.

This thesis provides a novel and easy-to-use software prototype artefact that SMEs with no previous cybersecurity experience can use to compile a cybersecurity policy template. The provided novel template can be the cornerstone or a source of ideas for building a customised and more complex document, where required.

The author would like to thank the supervisors Mika Juha Kerttunen and Andro Kull, for their comprehensive guidance, and the reviewer for the thorough feedback and recommendations.

The author thanks the cybersecurity expert Sille Laks from Clarified Security. The author also thanks Margus Danil from Telia for providing further feedback.

The author also thanks Henrik Aavik from Applaud and another SME for taking part in the interviews conducted for the thesis.

Furthermore, the author is thankful to all SMEs that participated in the survey.

1.1 Ethics

As T. W. Edgar and D. O. Manz described in the Research Methods for Cyber Security [4], “the data is a vital component of the research”. Collected data gives the researcher the necessary knowledge, but some additional information is not suitable in the research context. The researcher must be conscious of how to use the collected data ethically.

The survey questions were designed to be general, and participants were informed about the anonymity of it. For example, any personal data collection was voluntary, entering the email address was done to receive an overview of the survey. There was no private data collected or analysed during the survey.

All the interview data was collected with the participant's consent. It was confirmed to the participants that the information is used only in the research. Business-critical data exposed during the interviews was excluded and deleted from the results after it was identified.

1.2 Identifying the problem and motivation

1.2.1 Research motivation

According to the European Commission User guide to the SME Definition [3], SMEs (small and medium-sized enterprises) are the essence of the European Union economy. They are responsible for creating 85% of new jobs in the EU. The SME classification includes micro, small and medium-sized companies. In the EU, SMEs represent 99% of the entire business population. Knowing the SME definition is vital because it enables organisations to access different EU support programs targeted at SMEs [4].

As the EU Commission's [3] recommendations state, SMEs are differentiated by annual turnover, staff headcount, and the annual balance sheet total.

The smallest of the three micro-enterprises employ fewer than ten people, and annual turnover or balance sheet total does not exceed 2 million euros [4].

Small enterprises employ fewer than 50 persons, and, annual turnover or balance sheet total does not exceed 10 million euros [4].

Medium-sized enterprises employ fewer than 250 persons, and either has an annual turnover that does not exceed EUR 50 million or an annual balance sheet not exceeding EUR 43 million [4].

How is cybersecurity defined in the context of this thesis? It is assumed that cybersecurity is information security in cyberspace.

What is the cybersecurity policy in the context of this thesis? It is an internal company document that covers different cybersecurity risks and possible mitigations. The document is written in general and understandable language that aims to bring clear explanations to its reader.

One of the primary motivations for this research is the author's own experiences during many years of managing and consulting different SMEs.

This thesis assesses cybersecurity's organisational part. D. Fujs et al. [4] divides organisation cybersecurity into three categories: technical, organisational, and socio-psychological. The organisational part covers various policies, procedures, and processes.

SMEs rely more on information security and network solutions to provide better services to customers and to fulfil business goals. As the reliance on technology strengthens, cybersecurity-related risks are growing as well. Nevertheless, addressing cybersecurity-related risks is more demanding than securing, for example, a physical shop door.

ENISA recommendations [5] reveals that company-wide established security and privacy policies help to mitigate cybersecurity-related risks.

The main missing components of setting a company-wide cybersecurity policy are the lack of financial resources and knowledge of the subject. The latter is a consequence of the first. The same conclusion was reported by A. Alahmari and B. Duncan [6], C. Kent et al. [2] researches and by ENISA [5]; moreover, the SMEs are more exposed to cybersecurity risks because financial resources are limited, and this leads to minimal applied standards.

Another option is to outsource cybersecurity policy development and implementation services, but the client must understand that the organisation owns the risks, not the outsourcing partner. It is paramount to have management commitment behind the cybersecurity policy development.

As mentioned prior, the missing knowledge originates from granulated information about cybersecurity standards or rules. At first, it was studied what different options for cybersecurity policy the EU provides and whether it is possible to find a ready-to-use solution. The European Union provides various legislative sources, for instance, GDPR [7] and NIS [8] directives.

GDPR [7] focuses on protecting individuals who live in the EU. It is a legal framework that regulates collecting and processing personal information on the internet. Although the framework requires SMEs to comply with it, it does not provide information on internal cybersecurity policies.

NIS Directive is divided into three parts [9]. The first part requires that every EU country must have specific national cybersecurity capabilities. The second part, cross-border collaboration, defines how EU states work together in selected cybersecurity fields. The third part defines the EU's critical market sectors in each country and how local governments must coordinate these segments' supervision.

Both directives address high-level cybersecurity-linked challenges, but the documents do not provide any guidelines for tackling specific cybersecurity issues that SMEs might encounter.

Lack of frameworks for SMEs is endorsed by the ENISA report [5] that indicates, "There are limited European or international standards designed to assist small organisations towards ensuring appropriate protection of personal data".

All this leaves SMEs in a desolate area. As the report is a few years old, this paper researches how the situation might have improved.

This work researched different well-known cybersecurity governance frameworks, including ISO/EIC ISO 27001, ISO/EIC 270032, NIST, CIS Small Business.

This thesis's motivation is to discover whether a tool can aid SMEs in creating a cybersecurity policy, and whether through this, SMEs can improve their cybersecurity level and mitigate risks.

1.2.2 Research novelty

Academic research offers various analysis sources about the cybersecurity challenges in the small and medium business sectors [2], [5]. Most of them verify that there is a challenge with the cybersecurity approach in SMEs, but limited clarifications on improving the SMEs’ position are provided.

In the Rostami et al. [10] research, ISP's necessity is confirmed as one of the vital elements in the organisation’s information security management. It is verified that the task is challenging to handle, and software is often used to solve this challenge. As [10] summarises its findings to different system requirements that can also be used with different agile methods.

Furthermore, the literature research showed that if the study offers a software-based solution to tackle the cybersecurity problem, most of the prototype tools developed address risk-modelling parts or do not cover the full spectrum of security governance frameworks.

The research was widened outside the academic field. It was discovered that different sets of documents provided could be used for policy creation. Nevertheless, the research did not provide a software solution that helps start building a ready-to-use cybersecurity policy.

This study proposes a novel, easy-to-use, low threshold prototype artefact for compiling a cybersecurity policy used in real-world situations. The proposed cybersecurity policy structure and the content itself are novelties as this model of approach is innovative. Further novelty originates from the focus on the policy value proposal to the SMSs cybersecurity knowledge and core impact on SMEs cybersecurity state. Software development is in the supporting role of this thesis. The prototype artefact model can be expanded to different parts of cybersecurity policies and other documents. Also, the same applies to national strategies as there are standards and guidance available.

1.2.3 Research questions

Based on the literature research and expert opinions, there is no easy-to-use software tool to help SMEs create a cybersecurity policy.

As E. Rostami, F. Karlsson, and S. Gao [10] adds, "First, existing research has traditionally focused on manual design work, and there is a lack of studies on computerised tools that support ISP management". This work is intended to fill this knowledge gap.

The research question (RQ) is: can the absence of cybersecurity knowledge in SMEs be supported by the tool to aid in developing cybersecurity policy?

The following sub-research-questions (SQ) will help to answer the research question:

SQ1 – Research most common cybercrime threats in the EU SME sector.

SQ2 – Research the most common information security governance frameworks and, if possible, select appropriately for SMEs.

SQ3 – Collect knowledge about the functionality and content of the prototype tool by using a survey.

1.2.4 Research goal

Develop a prototype artefact that supports compiling a cybersecurity policy and via this help SMEs to mitigate cybersecurity-related issues.

The research goal (RG) is: make the compiling of cybersecurity policy available for SMEs.

1.2.5 Research domain

Henry Jiang published a mind map in 2017 named "The Map of Cybersecurity Domains (v1.0)". The map was later updated to version 2.0 [11]. The map shows graphically how diverse, integrated, and complex the cybersecurity domain is. This map was applied to show the different sub-domains this thesis is connecting.

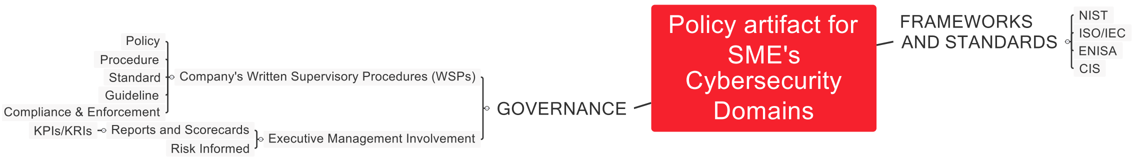


Figure 1 - Policy artefact for SME's Cybersecurity Domains

1.2.6 Stakeholders

The proposed artefact influences multiple stakeholders. Stakeholders may have a different level of awareness of a problem, possibly treatments [12]. Primary stakeholders are the SMEs who are impacted by cybersecurity harms. They are the artefact's actual users.

2 Topic of the thesis

Designing an artefact to support cybersecurity policy development in small and medium enterprises.

3 Methodology

Design Science was selected to be the research methodology in this paper. Therefore, as Hevner et al. “Design Science in Information Systems Research,” [13] identify “Design science, as the other side of the IS research cycle, creates and evaluates IT artifacts intended to solve identified organisational problems”.

3.1 Design science

The thesis follows Design Science Research Methodology (DSRM). Using DSRM gives the advantage of requirements mapping and prototype evaluation as applicable methods. In this thesis, Peffers et. al. provided a DSRM model [14].

The entry point for research is **defining the objectives of a solution** by gathering the requirements of the artefact.

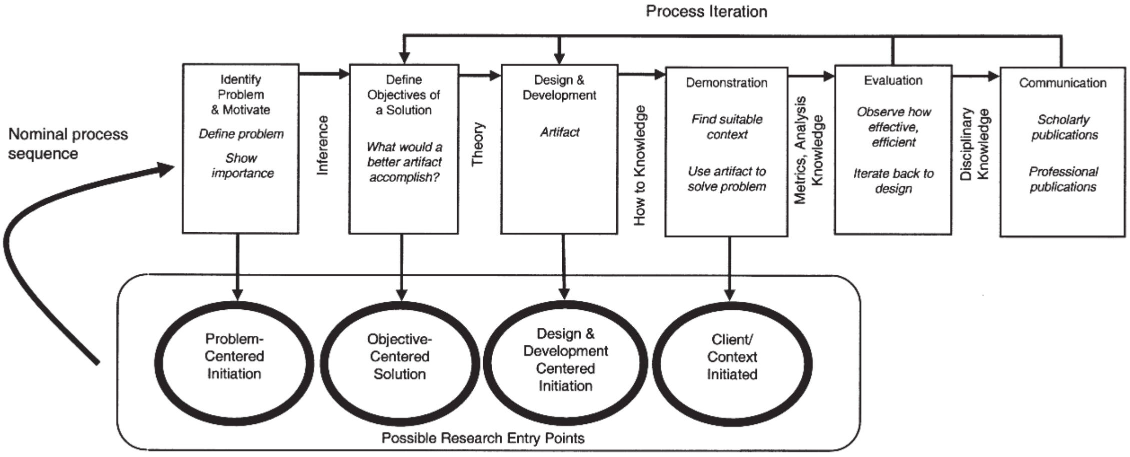

Process Iteration
Nominal process sequence
Identify Problem & Motivate
Define problem
Show importance
Inference
Define Objectives of a Solution
What would a better artifact accomplish?
Theory
Design & Development
Artifact
How to Knowledge
Demonstration
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
Evaluation
Observe how effective, efficient
Iterate back to design
Disciplinary Knowledge
Communication
Scholarly publications
Professional publications
Problem-Centered Initiation
Objective-Centered Solution
Design & Development Centered Initiation
Client/ Context Initiated
Possible Research Entry Points

Figure 2 - DSRM process model

Peffers et. al. model was applied to the thesis. It follows the six-step process: problem identification and motivation, the objective of the solution, design and development, demonstration, evaluation, and communication. The process is exhibited in Table 1.

Table 1 - Design science process

Step 1: Problem identification and motivation • Literature review and expert opinions.
Step 2: Objective of the solution • Literature review: research most common information security governance frameworks, discover the common risks and mitigations, and use the gathered knowledge for artefact requirements. • Conduct quantitative survey: o Gather SME's cybersecurity knowledge level. o Gather SME's cybersecurity necessities. o Gather SME's different requirements of the artefact.
Step 3: Design and development • Define requirements. • Select suitable platform. • Design and development of a prototype artefact.
Step 4: Demonstration. • Present artefact to stakeholders. • Gather feedback by interviewing the stakeholders. • Modify artefact.
Step 5: Evaluation • Gather feedback by interviewing the stakeholders. • Implement the changes. • Validate the artefact.
Step 6: Communication • Thesis defence and presentation.

This paper is linked to R. Koeze, “Designing a cyber risk assessment tool for small to medium enterprises,” [15] as in the same research field of work. Both of the researches are exploring options to create a more secure cybersecurity environment for SMEs.

3.2 Literature review

Sub-questions 1 and 2 will be answered by studying literature. The search for literature will be conducted using Google Scholar and Scopus. The discovered literature references will be forward and backwards snowballed to discover more materials.

Sample keywords: SME cybersecurity risk management, cybersecurity small and medium enterprises, designing an artefact to support cybersecurity policy development in small and medium enterprises, cybersecurity awareness.

3.3 Agile software development

A vital part of this research is the design and development of an artefact. Because of the limited resources and time, it is required to be adaptable and fast.

A comprehensive overview of traditional and agile software development was explored by M. Stoica, M. Mircea, and B. Ghilic-Micu in Software Development: Agile vs. Traditional [16]. It describes different software development methods; for instance, the waterfall model is advised when software requirements are well known and clearly defined. In the research of this thesis, this area is yet to be discovered.

Another option is to use an agile approach; for instance, the user requirements are gathered interactively by communication and development directions are easily changeable [16]. The agile approach is also studied in A. Aurum and C. Wohlin, Eds. [17], Engineering and managing software requirements. The study emphasised that agile development is adaptive. All the practices can be adjusted to fit the specific project on hand. Agile development is incremental by its nature, and development is reduced to iterations to provide more value. Completed iterations are delivered to the customer as fast as possible to get a valuable response and avoid various problems. Agile is also known for requirements prioritisation before every iteration to make sure of the client's wishes.

Using the agile method is also encouraged in A. Hevner and S. Chatterjee, Design Research in Information Systems [32], “Agile software development espouses a philosophy of building software systems where requirements and working software evolve through interactions among self-organising, cross-functional developer teams”.

Taking the information available under consideration, it was decided to use the agile approach in this research—agile development itself originates from the Agile Manifesto [16] established in 2001. The Agile Manifesto declares individuals and interactions over processes and tools, working software over comprehensive documentation, customer collaboration over contract negotiation, responding to change over following a plan. The paper is using the same principles in software development as part of the research.

3.3.1 Agile method

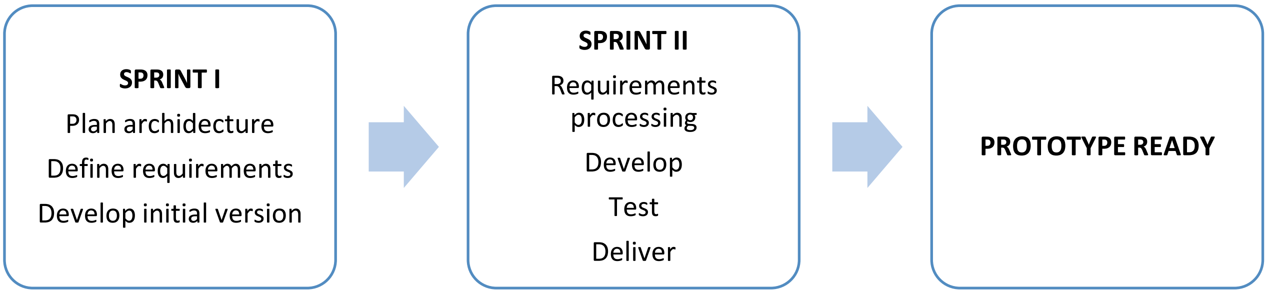
There is a different choice of agile development frameworks. Some of the popular ones are Scrum [18], Extreme programming (XP) [19], Crystal methodologies [20]. All the methods are primarily directed at working in teams. For instance, in XP and Scrum, the proposed team size is three to twelve people per project. Therefore, Scrum defines three team roles: Scrum Master, Product Owner, and the Development Team. Together they combine a Scrum Team [21]. Since there is no team to endorse this research, it is essential to consider the frameworks' constraints and gather the best suitable options from different methods to accomplish the goals. This option is supported by the fact that Agile development is adaptive [17].

3.3.2 Iterative workflow

Agile development is established on an iterative software development approach. The elements of Scrum sprints are used, also known as iteration or timebox, in this development workflow. The goal is defined before starting the project. Each iteration specifies the next task. Collecting feedback with every iteration approximately after two to four weeks and making continuous updates, the software will be completed.

Because of the time constraints, it was opted to keep our sprint count at two.

The software part of the Cybersecurity policy development artefact research workflow is displayed in Figure 3.



SPRINT I

Plan archidecture

Define requirements

Develop initial version

SPRINT II

Requirements processing

Develop

Test

Deliver

PROTOTYPE READY

Figure 3 - Agile software development process

As agile development is divided into several iterations, the cycles are described separately.

Scrum agile development model relies on the contribution of the customer and the company's sales, marketing, customer support departments, or software developers to provide requirements and priorities [22].

Because there was no direct communication with any SMEs, the findings from the literature review, information security governance frameworks analysis, and survey results are used in the planning phase to develop an initial version.

New requirements are gathered using interviews, prioritising, modelling, and implementing the requested changes into the artefact and delivering them to the SMEs in the sprint cycles.

After the final sprint is completed, the artefact prototype is ready.

3.3.3 Requirements engineering

Engineering requirements are essential for a software project to succeed. The core of agile development is to mitigate the risks of doing the wrong things in the wrong way by directly communicating with the customer and presenting ready work in a short period of time so that the deviations can be adjusted. After the keyword research, I. Inayat et al. [23] "A systematic literature review on agile requirements engineering practices and challenges," was studied. In this review, various agile requirements engineering practices and challenges are explored. The most common practice, according to the research, was requirements prioritisation. It was analysed in five different studies. The second general practice was testing before coding, and the topic emerged in four types of research. Third place with three studies was shared between face-to-face communication, customer involvement, iterative requirements, and retrospectives. The fourth place with two research mentions was user stories, change management, prototyping, requirements modelling, requirements management, review meetings, and acceptance tests. Each of the practices was analysed—to decide which ones have included the agile development process. Different methods are portrayed in L. Cao and B. Ramesh, [24], "Agile Requirements Engineering Practices: An Empirical Study" and M. Daneva et al. [25], "Agile requirements prioritisation in large-scale outsourced system projects: An empirical study," papers.

Each of the findings was examined.

Requirements prioritisation in agile software development is a technique of deciding which requirements are most relevant at this iteration. Compared to traditional software development, the requirements are defined once, at the beginning of the project [24].

Testing before coding is an approach when the test is written before the new software functionality exists. In this method, the requirements are transferred to test cases. This method allows for getting fast feedback about software functionality [24].

Face-to-face communication is a process when parties meet and discuss the requirements; it can be the primary source for requirements. This informal approach reduces the time of creating documents and getting approvals. It has its risks, and for example, it requires intensive interaction between both parties and a certain level of established trust [24].

Customer involvement is an agile development model principle to keep the customer up-to-date with the development process to get faster feedback and to provide more value by reduced costs and better commitment [25].

Iterative requirements describe a model where requirements are not defined and occur during software development and are specified after every interaction. In some instances, this is associated with design [24].

User stories are designed to define customer requirements. User stories help different stakeholders to better understand each other and provide further communication inputs [24].

Change management in agile development is a process through which the users can communicate changes, mostly adding or removing the requirements. This is accomplished using face-to-face meetings between clients and the development team. Fast validation has simplified managing changes [24].

Prototyping means that before building the actual product, there will be a pilot application released with limited features for testing and, in some cases, released to the market [24].

Also, D. Carlson and P. Matuzic, [26] in “Practical agile requirements engineering and [24], explain retrospectives are follow-up a type of meetings that occurs after every iteration. It stands utilised for reviewing completed tasks and planning for the next steps.

Requirements modelling is an agile method applied to model requirement visually by goal-sketching. Its goal is to make the requirements easy to read for different stakeholders, and this method is termed by K. Boness and R. Harrison, “Goal Sketching: Towards Agile Requirements Engineering [27].

Requirements management is a technique to keep track of product features as a list and index cards. In Scrum, it is applied to keep track of requirement changes [24].

Review meetings and acceptance tests are methods when agile project stakeholders meet and review the delivered software features. Occasionally, these meetings reveal new functionality. Acceptance tests are applied for software functionality validation. In some cases, these tests are bound with requirements [24].

Each of the practices was analysed to select suitable ones for this thesis.

Requirements prioritisation practice guides the research through different requirements, extracted from the source and selecting the most important ones. In this paper, the testing before the coding principle is not used. This is due to the inexact requirements in the development phase.

Face-to-face communication was used during the validation interviews, but in the concept of agile development, the SMEs were not involved in the process at the beginning. Customer involvement is also an essential part of agile, but this research is not frequently connecting to SMEs. Iterative requirements are part of the design sprints, and it was incorporated in the development process.

Retrospectives cannot be applied because they are used for follow-up meetings, but the follow-ups are not planned after the validation interviews. The user stories and change management techniques are not included because the interview structure is used to gather this type of information. As this is a limited functionality prototype, this interview method is included in the research.

Requirements modelling provides the goal-sketching model to present requirements in the easy-to-read graph; this is included in the research. Requirements management is not going to be utilised as the full agile model is not adopted. Review meetings and acceptance are not included because the interviews are selected for gathering the required information.

3.3.4 Requirements prioritisation

It is required to find a prioritisation method that best fits prototype needs and is lightweight enough to use for a team of one. There is numerous literature about the necessity of requirements prioritisations, but few excellent examples of real-life scenarios exist.

At first, the keyword research was performed about different software requirement prioritisations models to find a suitable one for this thesis. After analysing the keyword search results, the most noticeable result was J. Karlsson, C. Wohlin, and B. Regnell, “An evaluation of methods for prioritising software requirements, [28]"; the study describes six different methods for prioritising software requirements. The most referenced one is the analytic hierarchy process (AHP). As the study is analysing the traditional view of software development, the research was expanded. The Z. Bakalova et al. [29] "Agile Requirements Prioritisation: What Happens in Practice and What Is Described in Literature," in Requirements Engineering: Foundation for Software Quality was located. This paper compares different agile requirements engineering methods.

Approaches are compared by prioritisation method: intuitive prioritisation, prioritisation criteria, e.g. value risk, project context, size/effort estimation, input from developers, learning, external changes, project constraints, dependencies, project backlog, the value of requirements, prioritised project backlog, and iteration/sprint backlog.

The research requires methods with the following characters: prioritisation criteria, size/effort estimation, input from developers, the value of requirement. These criteria are sufficient to develop the artefact. Two methods were discovered that answer this criterion.

XP: planning game/poker is studied by V. Mahnič and T. Hovelja, "On using planning poker for estimating user stories," Journal of Systems and Software [30] is an agreement based gamified technique, primarily used in agile software development, for estimating the effort of development goals. The strong points are that the group has to have a face-to-face meeting to play this game. This increases teamwork and collaboration between stakeholders. This method is an excellent way to prioritise teams, but it is not usable in this research case.

Wieger´s matrix approach was researched by K. E. Wiegers, "First Things First: Prioritising Requirements," p. 6, 1999. [31], is another technique to prioritise software requirements.

It offers a straightforward method of how to prioritise software requirements. Its approach is established on prioritisation based on value, cost, and risk.

The study recommends keeping priorities as plain as possible to make the essential development decisions. This model should also be used to evaluate additional features, not the base functionality of the software. Typical participants can be project manager, customer and developer. The method does not expect all the participants to be involved as the project manager can adjust inputs as necessary.

The model proposes a semi-quantitative method that is not mathematically rigorous. Its limitations are based on projecting the estimates of benefit, penalty, cost, and risk of each feature requested.

It is necessary to follow seven steps for using this model. Step one, list all of the features that need to be prioritised. Step two, estimate the relative benefit that each feature provides on a scale of one to nine, where one is low on benefit and nine the highest benefit. The benefits are related to business requirements. Step three, assess the relative penalty client will endure if the software feature is not included, on a scale of one to nine, where one is no penalty and nine the most severe. Step four, the total value, is the sum of the benefit and penalty. Step five, project the project's cost of implementing each feature on a range where one is low and nine is high. Step six, developer projects technical or other risks bonded with each requested feature by cost and risk are weighted equally. On a range where one is easy to implement, nine is hard and might require additional competencies or human resources. Step seven, calculate priorities for each feature. The formula for the priority is: priority = value %/ (cost % * cost weight + risk % * risk weight). The output will be expressed in the form of a table.

After analysing and using the model on test data, it was found that this method is suitable for the research needs. The Wieger’s matrix is used in the software development cycle.

3.3.5 Prototype

This research aims to build a functional prototype to test its functionality and prove that artefact can help SMEs compile a Cybersecurity policy. Because of the time constraints, it is required to build the artefact from ready to be used components that can be assembled to reach the research goal. Multiple different programming language frameworks were examined, for example Django, a high-level Python Web framework, and the most popular PHP framework Laravel. The WordPress platform is also known for flexibility and offers a different choice of plugins that can be utilised.

3.3.6 Requirements modelling

Analysis of Inyat et al, [23] brings out two agile requirements modelling methods. Goal sketching is analysed in K. Boness and R. Harrison, “Goal Sketching: Towards Agile Requirements Engineering,” in International Conference on Software Engineering Advances (ICSEA 2007) [27]. The objective of the method is to give an easy to recognise visual overview of where software development is advancing. Iterations are Scrum, the sketch is started with high-level goals, usually partial, and it will evolve after each iteration into a tree structure.

The second model was researched by N. A. Ernst et al. [32], in “Agile requirements engineering via paraconsistent reasoning”. It proposes the RE-KOMBINE framework to express the requirements. This model is not suitable for our research because it focuses on a scale bigger than this research.

It was decided to use [27] in the requirements modelling part of the thesis to fit the development cycle.

4 Objective of the solution

Design science projects can be complicated, as there are many different angles and theories for problem-solving, so the researcher must select the variables and methods that bring the most valuable knowledge to the research. As A. Hevner and S. Chatterjee, Design Research in Information Systems, observed, "It is important to keep in mind that every design science project requires a certain level of creativity" [33].

4.1 Information security governance frameworks

It was decided that SMEs' usable frameworks must be easy to evaluate, easy to comprehend, easy to enforce, easy to renew, and effective.

Each framework was analysed with its pros and cons in the context of this thesis. The focus was on the framework versions that are designed exclusively for SMEs. Each keyword was extracted and added in the comparison table to find common nominators for each governance framework. Another goal was to seek common principles throughout the documents to build a more effective cybersecurity policy.

The most popular information governance frameworks are PCI DSS [34], ISO [35], CIS [36], NIST [37], ENISA [38].

4.1.1 PCI DSS

PCI DSS or The Payment Card Industry's Data Security Standard framework handles credit card information: accepting credit cards, processing the transactions, storing data, or transmitting credit card data. The PCI DSS covers the whole process of secure card payments. The PCI DSS offers tools to provide necessary security evaluation information for payment data theft focused on small merchants. Nevertheless, the standard itself is directed to payment processors, not SMEs; and for this reason, we exclude the PCI DSS from our research.

4.1.2 ISO

ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) [39] is one of the most popular information security frameworks. It is developed by the International Organization for Standardisation. The framework is growing consistently: its YOY growth in 2018 vs. in 2019 was 3,8%. Based on the 2019 ISO survey, there are a total of 36362 valid [40] ISO/IEC 27001 certificates. For reference, in Estonia, the certificate count in 2019 was 10 [41].

ISO/IEC 27001 is a systematic collection of processes, documents, technology, and people. It helps the organisation to manage, monitor, and improve information security.

The core of the ISO/IEC 27001 is an ISMS constructed on business risks and displays diverse security threats.

ISO/IEC 27032 (Information technology - Security techniques - Guidelines for Cybersecurity) [42] is another ISO family framework focused on cybersecurity. Its crucial objectives are safeguarding confidentiality, integrity, and availability of information in cyberspace.

At first, ISO/IEC 27001 and ISO/IEC 27032 documents were researched using the iso.org website to assess the standards themselves. The papers are not easy to evaluate because the standard documents are behind the paywall, and each document requires a payment; without paying, only a short preview is available. The evaluation was performed on the available previews. Based on the results, it is possible to claim that it does not offer enough information for SMEs to justify the document purchase without an expert involved in the standard development process.

Alternatively, the full text of ISO/IEC 27001, was researched; the whole paper is 36 pages, and ISO/IEC 27032, full paper 60 pages. The goal: to find out how easy it is to comprehend and how SMEs can improve their cybersecurity policy development process.

As the requirements name in the ISO/IEC 27001 standard references, it specifies different requirements for establishing, implementing, maintaining, and continually improving an ISMS system within the organisation's context. The ISMS preserves the confidentiality, integrity, and availability of information by applying risk management and confidentiality to interested parties that risks are adequately managed [39]. The standard structure includes ten sections and one Annex plus a biography.

To be compliant and certified by the ISO auditor, the company is required to compile the following list of mandatory documents [43]: Scope of the ISMS (clause 4.3) Information security policy and objectives (clauses 5.2 and 6.2), Risk assessment and risk treatment methodology (clause 6.1.2), Statement of applicability (clause 6.1.3 d), Risk treatment plan (clauses 6.1.3 e, 6.2, and 8.3), Risk assessment report (clauses 8.2 and 8.3), the definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4), Inventory of assets (clause A.8.1.1), Acceptable use of assets (clause A.8.1.3), Access control policy (clause A.9.1.1), Operating procedures for IT management (clause A.12.1.1), Secure system engineering principles (clause A.14.2.5), Supplier security policy (clause A.15.1.1), Incident management procedure (clause A.16.1.5), Business continuity procedures (clause A.17.1.2), Statutory, regulatory, and contractual requirements (clause A.18.1.1).

The listed documents are the first part of the initial policy requirements. If the company's business requirements are different, the document list will expand as requested. The core decisions about the risk treatment are rendered at the management level. As the framework does not always require mitigating the risks, it is up to management to decide if it is worth managing. Primarily the risk should be defined as avoided, shared, or accepted. If the decision is to mitigate the risk, Annex A can help with predefined controls.

In ISO/IEC 27001 case, 114 Annex A controls are partitioned into 14 categories. Annex A provides a valuable structure for controls, and it is not vital to use all of them in an organisation, because several of them are not information security-related. The controls are presented in a well-read list with a description that gives the organisation an option to select the risks and find the preferred option. However, Annex A offers only a brief overview of specific control; the detailed action plan is up to the organisation to resolve. As the standard is slow to update, some of the controls are dated; for example, malware control does not include an antivirus implementation recommendation.

The objective is to locate the policy selections that can be used to develop an artefact. As analysing Annex A, the resulting keywords were added to the shortlist of topics that an artefact must include to build a usable and effective cybersecurity policy. The topics included are asset management, information security policy, mobile devices and teleworking, media handling, access control, backup, logging, and monitoring.

ISO/IEC 27032 [42] offers a good set of building bricks to lay the company's cybersecurity policy. The framework defines specific technical guidelines for addressing common cybersecurity risks such as social engineering, hacking, malware, spyware, and other potentially undesirable software. Furthermore, technical guidance and controls addressing for following risks are provided: malware attacks, individual miscreants or criminal organisations on the internet, detecting, monitoring, and responding to attacks.

The second part of ISO/IEC 27032 deals with collaborations and information sharing coordination, and incident handling among shareholders in cyberspace. The standard offers comprehensive terms and explanations that help the reader to understand the subject.

The objective is to locate the policy selections that can be used to develop an artefact. As analysing the ISO/IEC 27032, the resulting keywords were added to the shortlist of topics that the artefact must include to build a usable and effective cybersecurity policy. Included topics are stakeholders and cybersecurity controls.

The ISO/IEC 27001 standard compilation is flexible and offers different guidelines. It does not require certification if this is decided. On the other hand, the standard update is slow and relies on generic guidance but not on cyberspace's operational risks.

In conclusion, ISO/IEC 27001 is a set of high-level processes and guidelines, but it lacks operational and easy access criteria. Also, compiling the standard documents into cybersecurity regulations is an overwhelming amount of information to process without prior knowledge or expertise in the field.

ISO/IEC 27032 is centred on the cybersecurity aspect, and various sets of controls are at the disposal of policy creator. Its main weaknesses are the same as 27001; the standard is slow to update and does not cover the operational risks.

Nevertheless, the amount of information and connection to other parts of the standard is vast and requires a portion of work hours, and this time resource is often unavailable to SMEs.

4.1.3 CIS Controls

The Center for Internet Security develops CIS Controls, Inc. [36], the project originates in 2008 and is a community-driven and non-profit organisation, focused on cyber defence.

The analysis was done on CIS Controls Implementation Guide for SMEs [44], as its name implies, is addressed at SMEs. The guide was released in 2017 and was designed to help organisations with small budgets, and limited employees to shield their businesses.

CIS Controls Implementation Guide for SMEs provides a tangible approach. It recommends using the phases approach [44]. The guide identifies three phases: know, protect and prepare.

Phase 1: Know. In this chapter, it is vital to understand and gather information about the environment. It expects to gather knowledge about what type of devices are connected to the network and what software is used. Whether the critical data is defined, and where is this type of data stored. It is suggested to create hardware, software, and critical data inventory lists that should be regularly updated. The guide explains how to scan a network and check for locally installed software. In cooperation with company employees, all the online services in use must also be identified. Computer administrator privileges must be given to a limited number of users. Passwords must be hard to guess, and for casual computer usage, non-administrative user accounts should be used.

Phase 2: Protect. This section focuses on the protection of computers and how users should be educated about cybersecurity. The paramount goal is to establish a baseline security level. For this, every computer should be installed as securely as possible, all installed software must be updated, and malware/antivirus scanners installed. The users must pass a training program, which includes best practices.

It is crucial to keep in mind that cybersecurity goes beyond technological solutions. The training program should propagate the cybersecurity mindset within a company. Key people who are responsible for critical data should know the role of protecting the information. All the ordinary attack methods (such as phishing and phone call attacks) must be explained and played out if possible. The common sense paradigm must be propagated within a business; if something appears excessively excellent, dangerous, or dubious, it is an assault and should be reported. Moreover, the cyber hygiene aspects like automatic locking of the mobile screens, using unique passwords, multi-factor authentication, and keeping devices updated must be included and reminded in the training program.

Phase 3: Prepare your organisation. The last phase identifies two sections. The first is managing backup. Every organisation should have a backup management plan. It should be understandable reading the plan when the last time backup was made; it is suggested that backups are made weekly. The backups must be restored periodically to verify their trustworthiness. One backup must always be disconnected from the network to prevent network attacks by means such as malware.

The second section guides how to prepare for a cybersecurity incident. Every company must have a single point of contact who is responsible when a cybersecurity incident occurs. Contacts of the local IT support and the contacts of the outsourced IT partners must be made available. Also, a list of legal, insurance, and external cybersecurity experts must be prepared and, in addition to knowing how the state expects the corporation to react. In some countries, it is essential to get in touch with a local CERT or an authority body that serves the same purpose.

The objective is to locate the policy selections that can be used to develop an artefact. As analysing the CIS Controls Implementation Guide for SMEs, the resulting keywords were added to the shortlist of topics that an artefact must include to build a usable and effective cybersecurity policy. Included topics are baseline security, gathering information.

In conclusion, CIS Controls Implementation Guide for SMEs offers a very down-to-earth and hands-on perspective on cybersecurity. At the end of every section, there is a shortlist of recommendations and links to cost-effective tools. It gives detailed guidelines and tools to SMEs to handle cybersecurity issues.

4.1.4 NIST

The National Institute of Standards and Technology (NIST) [37] was founded in 1901 and is now part of the US Department of Commerce.

In 2017, NIST [45] released, together with the U.S. Small Business Administration and the Department of Homeland Security, cybersecurity-focused documents for helping SMEs protect their business. The thesis research analysed NIST Cybersecurity Framework for Small Businesses. The framework is divided into five areas: identify, protect, detect, respond, and recover.

The identify part guides to make a list of all equipment, software, and data. It is mandatory to include different mobile devices, computers, and point of sale devices. Moreover, the identify part requires compiling a cybersecurity policy that covers the roles and tasks of employees, partners, and all other parties who have access to critical data.

The protect section targets the network and device users. Also, procedures for using secure software, encrypt confidential data at every stage of the transfer, managing regular backups, taking care of automated software updates, and having a safe disposal plan of old electronic devices are provided. Finally, an employee training plan must be established and promoting the paradigm that everyone is a part of establishing a better cybersecurity state.

The detect topic gives a general overview of monitoring computers from forbidden access to physical devices, like USB drives and software. Monitoring internal and external network connections and probing bizarre patterns is a necessity.

The respond section details creating a plan for responding to a cyber incident. The main goal is to keep business impact to a minimum when trying to mitigate and investigate the attack and to give authorities enough information. Communication about the incident with employees and partners is vital. After the attack, the cybersecurity policy must be revised according to conclusions drawn from the incident.

Recover. The company must own a plan for what to do after a cyberattack has occurred. The plan must include a part on how affected devices are planned to be brought back online and if there are any damages then how to replace faulted hardware All the info gathered during the attack must be formed into the document and added to the cybersecurity policy to store the knowledge to best prevent the attacks in the future.

NIST Cybersecurity for Small Business [45] has additional elements that can be used as a source for compiling a cybersecurity policy. It contains different parts where topics are clarified in more detail.

For example, the physical security part is including on how to protect devices and documents. All documents and devices must be stored securely with restricted physical access. Personnel must be notified to lock physical file cabinets and never leave devices with sensitive data unattended. Also, it makes sense to have an overview of devices that are used for gathering client information. Only vital files must be preserved. For protecting the devices, a complex password, multi-factor authentication, limited login attempts, and encrypting portable media is essential.

The following parts of NIST specify different risks and controls. The provided risks/controls are ransomware, phishing, business email imposters, tech support scams, cyber insurance, email authentication, vendor security, hiring a web host, and secure remote access.

The objective is to locate the policy selections that can be used to develop an artefact. As analysing the NIST Cybersecurity for Small Business, the resulting keywords were added to the shortlist of topics that an artefact must include to build a usable and effective cybersecurity policy. Included topics are physical security, equipment list.

In conclusion, NIST for Small Businesses offers easy-to-read documents that define all the necessary components to compile a cybersecurity policy and provide a clear set of selected risks with recommended controls. Risk mitigations and recommendations are presented at the end of every chapter, although they are not as detailed as CIS provided.

4.1.5 ENISA

The European Union Agency for Cybersecurity [38], abbreviated as ENISA was established in 2004 and focuses on establishing a high cybersecurity level in the EU. The about section of the agency's website summaries its objectives: "Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure" [46].

As ENISA [5] stated before, there is a constrained set of cybersecurity policies for SMEs. The ENISA Cloud Security Guide for SMEs [47] was added to this research to verify the probability of discovering a suitable framework. This paper reveals network information security-related opportunities and risks in cloud computing. Nevertheless, it does not offer guidelines for the thesis objectives.

On the other hand, ENISA is providing regular information about cybersecurity issues. ENISA Threat Landscape 2020 [1] was inspected and revealed a top 15 cyber threat list, containing comprehensive descriptions with proposed mitigations. This list is used to select top threats and to use the documents compiling the cybersecurity policy.

The objective is to locate the policy selections that can be used to develop an artefact. As analysing the ENISA Threat Landscape 2020, the resulting keywords were added to the shortlist of topics that an artefact must include to build a usable and effective cybersecurity policy. Included topics are cybersecurity risks and mitigations and up-to-date threat information. The framework's pros and cons are displayed in Table 2.

Table 2 - Pros and cons of frameworks

Name	**Easy to access**	**Costs of implementation**	**Cons**	**Pros**	**Effective**
ISO/IEC 27001	Essential documents are behind the paywall	Higher, compared to others	Too abstract for SMEs. Slow to update. Too complex to understand	Flexible, free to select risk-driven options. Offers acceptable abstraction to fit different organisation sizes. The controls structure is well presented	Low from a cybersecurity point of view
ISO/IEC 27032	Essential documents are behind the paywall	Higher, compared to others	Too abstract for SMEs. Slow to update. Too complex to understand	Flexible, free to choose risk-driven options. Offers acceptable abstraction to fit different organisation sizes.	Low from a cybersecurity point of view
CIS Controls	Documents are free to download	Low	Some of the recommended tools are not active. Some web links are out of date	Policy chapters are provided	High

ENISA	Documents are free to download	Low	No policy provided	Provides updated risks with detailed descriptions	High from risks perspective
NIST	Documents are free to download	Low	Policy structure is not provided	Policy chapters are provided	High

4.1.6 Conclusions

The following conclusions were drawn from the analysis of information security governance frameworks.

Most online tools that can be found from the frameworks homepages or performing an internet search are focused on self-assessment tools, useful and easy to understand. However, this overlooks the problem: that everything starts with policy creation, as it was discovered during the standards research. The standard itself is a set of building blocks that SMEs must put together to meet the business requirements. Regrettably, there is no example of what chapters or steps the cybersecurity policy should include. The second factor is that most established frameworks are intended for larger organisations, and SMEs lack the resources or even the organisational structure to implement the policy.

In this part of the research, the analysis of different information governance frameworks was performed. Research extracted the underlying principles from different frameworks and risks and controls, and the findings are presented in the following paragraphs. Findings are domain-level requirements [17] because it relates to the problem area and principles will be used for the artefact development.

All hands on deck. Every person working in a company who has access to a computer is a part of the cybersecurity policy. Developing a cybersecurity culture must be taken at every level of the company hierarchy. It is not the project of the IT department or an outsourced partner.

Everything flows from the top. If the company's management is not actively involved in the policy development process and its implementations, it is not worth spending the resources.

Cybersecurity (information security) is a process, not a state that gets established. It requires continuous analysis, modification, updates, and implementation at all levels of the organisation.

Baseline security. The basic security level that the company must have to operate. Baseline objectives must have a clear purpose and easy-to-understand objectives. For example, all computers must have an antivirus installed and updated daily.

Common sense. From cybersecurity's perspective, the principle of common sense can be treated as follows: before deciding, the information must be evaluated to make the right decision. If something seems too good, bad, or confusing, it is probably a cyberattack attempt. For example, suppose someone calls an accountant and says that the company's management has ordered a quick transfer to a specific account, and he or she cannot confirm it himself or herself. In that case, such information must be ignored and reported in accordance with the principle of common sense. Framework keywords findings are displayed in Table 3.

Table 3 - Framework keywords research findings

ISO 27001	ISO 27032	NIST	CIS	ENISA
Asset management	Stakeholders	Equipment list	Gathering information (Know)	Cybersecurity risks and mitigations
Information security policy	Cybersecurity controls	Physical security	Baseline security	Up to date threat information
Mobile devices and teleworking	No value	Critical data	Common sense	No value
Media handling	No value	No value	No value	No value
Access control	No value	No value	No value	No value
Backup	No value	No value	No value	No value
Logging and monitoring	No value	No value	No value	No value

Keyword findings list.

FK1: Asset management/equipment list

FK2: Information security policy

FK3: Mobile devices and teleworking

FK4: Media handling

FK5: Backup

FK6: Logging and monitoring

FK7: Stakeholders

FK8: Cybersecurity controls

FK9: Physical security

FK10: Critical data

FK11: Gathering information

FK12: Baseline security

FK13: Common sense

FK14: Cybersecurity risks and mitigations

FK15: Up to date threat information

4.2 Survey

This research is about providing an artefact to compile a cybersecurity policy for SMEs. The first set of information was collected by completing a study of different information security governance frameworks. After discussion with experts, it was decided that more information was required to build an artefact.

To achieve this goal, it was decided to conduct a survey performed by utilising a quantitative research method. Using a survey to gather more knowledge was also encouraged by Wieringa in Design Science Methodology for Information Systems and Software Engineering [12]. The survey helps connect research to a real-world environment and to provide essential information that may get overlooked.

The survey is associated with the positivist tradition. As Easterbrook et al. Selecting Empirical Methods for Software Engineering Research [48] states, "Positivitism states that all knowledge must be based on logical inference from a set of basic observable facts."

The preferred method was a web survey [49]. Web surveys operate by inviting potential respondents to visit a survey page where the questions are presented in a structured order. Before the survey was sent out, the quality of the questions was validated with an SME representative. The survey was created on the Google Forms platform, and sent out by email, shared in social media groups and chat channels. At the beginning of the survey, there was an introduction that the survey is directed to SMEs. For this research, non-probability sampling types of convenience and snowballing sampling were applied. The target population was SME representatives, responsible for business decisions involving business risks and continuity. The survey was active from January 15, 2021 until February 25, 2021. It managed to collect 21 unique responders; after applying SME parameters, 17 answers were included in the study. Survey questions are included in Appendix 1.

4.2.1 Data

The survey was created to be balanced, easy to answer and understand. The survey length was estimated between five to ten minutes, to gather quality data. The questions were debated with experts and self-designed.

The survey consists of 25 questions, divided into five parts. The first part covers the survey's introduction and necessary company information to identify its size and questions about the digital information's worth. The second part covers specific cybersecurity questions about the company's cybersecurity and whether it uses any information governance frameworks; and whether it needs a better solution for this issue. The third part contains questions related to whether the prospects need a better tool for compiling information security regulation and how much time prospects are willing to spend learning the proposed artefact. Also, questions about policy development budget and training are incorporated. The fourth part includes questions about devices and operating systems. Also, does the company use an operating system with built-in security solutions; are employees using their own devices at work; which different security products is the company using. The fifth part contains a Likert scale [49] set of questions to gain knowledge about the artefact’s functionality.

4.2.2 Structure of the survey

As reported, the survey consisted of 25 questions that were partitioned into five sections.

The first section featured five questions.

- The first two questions provided the necessary background information to identify the company belonging to the SME sector. If the answers were outside the SME definition, results were excluded from the analysis.

- Questions number three, four, and five provided background for standard cybersecurity knowledge level and data value understanding.

- Question five appeared only when question four was answered with “yes”.

  The second section consisted of six questions.

- Question number six asked about information security analysis.
- Question seven provided insight into cybersecurity planning in the organisation, and whether there is a person responsible for it.
- Question eight showed whether the company is keeping a register of hardware and software assets.
- Question nine was concerned with probing: is the company using an outsourced partner for IT services and if yes, its form of collaboration.
- Question ten asked whether the company is using any information security governance frameworks.
- Question eleven asked the prospects whether the firm needs a better solution for managing information security governance frameworks.

The third section had five questions.

- Question twelve queried whether if a better tool for managing information security governance frameworks were provided, would the prospect consider using it.
- Question thirteen asked whether regular information security training is conducted in the company.
- Question fourteen asked how much time the prospect can invest in learning the artefact usage.
- Question fifteen specified the range of financial values the company is willing to invest in developing the information security governance framework.
- Question sixteen asked about the rules of using devices outside the office.

The fourth section contained five questions.

- Question seventeen asked what type of devices the company is using.

- Question eighteen investigated whether the employees are using their own devices for work purposes.
- Question nineteen requested information about the operating systems in use.
- Question twenty asked whether the company is using security products that are integrated into the operating systems.
- Question twenty-one surveyed what additional information security devices and tools the organisation is using.

The fifth and last block contained four Likert scale-type questions, numbered twenty-two to twenty-five.

- The participants were first asked to rank software ease of use quality on a scale of one (not important) to five (important).
- Secondly, the participants were asked to rank the ease in understanding policy compiling (as software quality) on a scale of one (not important) to five (important).
- The third question: rank the quality of a ready-to-use policy as software on a scale of one (not important) to five (important).
- The last question measured the compliance with information security governance frameworks (ISO, CIS, NIST, etc.) as software quality on a scale of one (not important) to five (important).

4.2.3 Survey analysis

The data was analysed using Microsoft Excel software. The selected method was the univariate [49] analysis because it was required to analyse one variable at a time to extract the required input for the artefact. The frequency table was utilised to show the percentage of entities in different categories of a variable. In the last section, the answers were analysed using descriptive statistics. The mean value calculations were used on the dataset.

From all participants, 13 (or 76,5%) answered that they have a maximum of 10 employees in their company. Furthermore, 70,6% had a turnover less or equal to 2 million euros per year. Cybersecurity affected or involvement was reported by 23,5% of participants. From respondents, 29,4 % had calculated their business data value, and 75% of the estimated data value to be between 100 000 – 1 000 000 euros. 25% projected the value to be 50 000 – 100 000 euros.

Information security analysis was performed in 41,2% of companies, and 35,3% had a person appointed responsible for information security. Different hardware and software assets are mapped in 52,9% of companies. More than half of the companies, 64,7%, were not outsourcing IT management services. Hardware management services were used by only 11,8%, and a service combining both hardware and software was used by 5,9%. Full responsibility was outsourced by 17,6% of companies.

The ISO framework was the most popular option in our survey, with 11,8%. ISO, combined with its own internal rules was used in 5,9% of companies. The amount of companies with their own internal rules was 23,5%. The majority of companies, 58,8% answered that they were not using any information security governance frameworks at all.

A better solution for managing information service policy was requested by 70,6% of the respondents. Furthermore, 88,2% would utilise a tool that provides the possibility of compiling a set of information security regulations. Regular information security training was conducted in 23,5% of businesses. Investing time to learn a provided tool functionality was divided; 35,5% would spend 1 hour to learn, 35,5% could spend one working day, 23,5% could allocate 3 hours, and 5,9% would take no time at all.

The question regarding the company's information security budget allocation, 64,7% answered that they have less than a thousand euros per year to spend. More than ten thousand euros per year could be spent by 17,6% of the companies. More than thirty thousand euros per year could be invested by 5,6% of the participants. Procedures for devices that are outside an office, 52,9% answered they have no procedures in place. Notebook computers are the most popular device; 58,8% are using them. Desktop computers are second, by 17,6%, phone and tablet combination are operated by 17,6%.

Companies that only use phones had 5,9% of answers. In the question, are users using their own devices (BYOD) for work, 64,7% answered yes.

The most popular operating system was Microsoft Windows with 35,5%; the second was a combination of Microsoft Windows, Android, and iOS, 23,5%. A third was a combination of Microsoft Windows and Android by 17,6%. Forth was a combination of Microsoft Windows, macOS, Android, iOS 11,8%. The final place 5,9% was divided by Microsoft Windows, iOS and Microsoft Windows, macOS, Linux, Android, iOS.

It is common to use OS integrated security products like Microsoft Defender Antivirus or similar. To this question, 94,1% of the participants answered yes.

Antivirus and anti-malware software are the most popular tools companies are using; 23,5% are applying this. Antivirus and anti-malware, and firewall combined are used in 11,8% of the companies. The same outcome, 11,8%, was used in a pattern of antivirus and anti-malware software, Mobile device security, two-factor authentication (2FA), email security, access control, data loss prevention, firewall, data encryption. All the other combinations received 5,9% of the answers.

The last part, Likert scale questions, were measured on a scale of one (not important) to five (important). For the first question, please rank “easy to use” as a list of qualities of information security regulation tool, statistics mean value was 4,88. For the second question, please rank "easy to understand policy compiling" as a list of qualities of information security regulation tool, statistics mean value was 4,59. For the third question, please rank "offers ready to use policy" as a list of qualities of information security regulation tool, statistics mean value was 3,82. For the fourth question, please rank "compliant with information security governance frameworks (ISO, CIS, NIST, etc.)" as a list of qualities of information security regulation tool, statistics mean value was 3,18.

The statistical presentation of all survey responses is presented in Annex 7.

4.2.4 Limitations of the survey

The response rate for the survey was lower than expected. COVID-19 might have influenced the response rate since SMEs are working hard to maintain their businesses. Therefore, the survey results are used for artefact software development input and can not draw any statistical relevance based on the dataset. Survey research always poses a risk for sampling bias because the respondents might not represent the target population. The target population was intended to be a diverse one. Therefore, not all the questions might be understandable by all participants.

5 Design and Development

This chapter describes the design and software development part of the research. In addition, it explains how the different methods are applied to the artefact development research.

5.1 Requirements

The requirements are provided as descriptive definitions about what the software system should do. The requirement is defined in IEEE/ISO/IEC 24765-2017 [50] as a “statement that translates or expresses a need and its associated constraints and conditions”.

This paper uses different methodologies to present and explain various requirements.

5.1.1 Non-functional requirements

E. Rostami’s [10] research provided us with a list of general requirements. The following list was selected to be applied as the paper’s non-functional requirements for developing the artefact—clear communicative objectives, clear structure, clearly defined concepts, keep up-to-date. This list was added to literature research findings: FK13, FK15, FK7. The list of non-functional requirements is not included in the priority list or sketch goal;

instead, it is considered as non-functional requirements when preparing other artefact development-related decisions.

5.2 Structure of the policy

During the creation of the cybersecurity policy, it was taken into account that somebody who is not a specialist in the field must understand and be able to enforce the document.

The suggested cybersecurity policy is divided into dynamic and static paragraphs.

The dynamic paragraph content includes data selection or content based on the user input when using the artefact.

The static paragraph is always included in the document as a constant to ensure the integrity of the policy.

The proposed policy is structured by: assets policy, physical security policy, baseline system security policy, access controls and accounts management policy, password policy, training policy, BYOD and mobile devices policy, critical data policy, backup policy, software update policy, incident handling policy, logging and monitoring policy, and the mitigation chapter.

Policy content is inspired by “NIST CSF Policy Template Guide 2020” [51], and it is linked in related documents. The [51] template guide collects different policy sources and standards; the main contributors being SANS Institute and NIST.

An additional source for the policy data is CIS Benchmarks [36], which provide a deep level configuration manual for various operating systems and devices.

The logical base structure was added, and explanations to the policy questions compiler to provide the first-time policy compiler with an overview of the topic. This additional information provides more insight into the variety of cybersecurity topics. The last part of the policy document includes TOP ENISA Cyber risks with their mitigations. The policy structure is displayed in Figure 4.

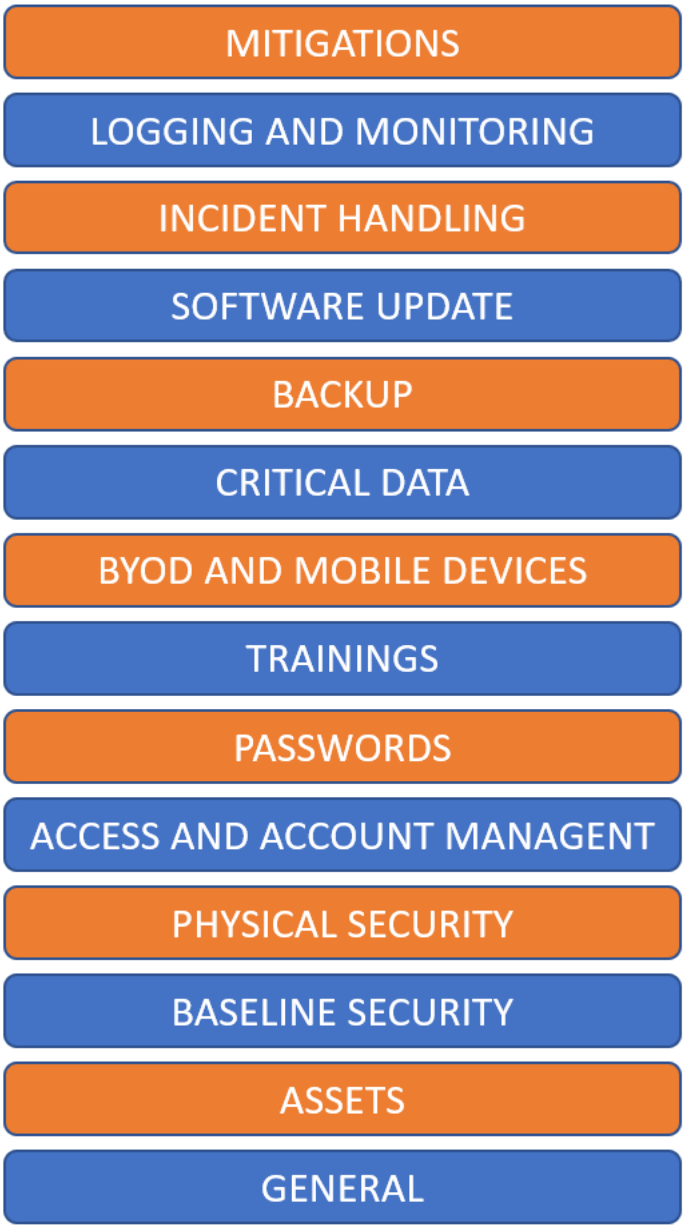


Figure 4 - Cybersecurity policy structure

5.3 Sprint I

Sprint I is following the process described in the Iterative workflow chapter. At first, the software architecture will be planned. Second, identifying primary requirements and building the initial version of the artefact can be presented to SMEs to verify the requirements implemented.

5.3.1 Requirement modelling

As was learned during this research, it is necessary to use requirement modelling as a part of requirements engineering before software development can begin. The K. Boness and R. Harrison's method researched, "Goal Sketching: Towards Agile Requirements Engineering," [27] was used.

It is vital to define the high-level motivation when using this model. The motivation of this research is:

I. Make cybersecurity policy compiling available to SMEs

Several constraints from the survey responses, Annex 7, will be bound to this motivation.

II. Software should be easy to learn and use (based on findings F5, F7, F13, F14, F15)

III. The policy should include various segmented topics (based on findings F1, F2, F3, F4, F6, F8, F10, F12, FK1, FK3, FK4, FK5, FK6, FK9, FK10, FK12, FK14)

IV. The software should work on different devices (based on F9, F11 findings)

Framework research findings labelled as prefix FK are excluded from Sprint I to keep the scope concentrated.

The schematic version of constraints is shown in Figure 5.

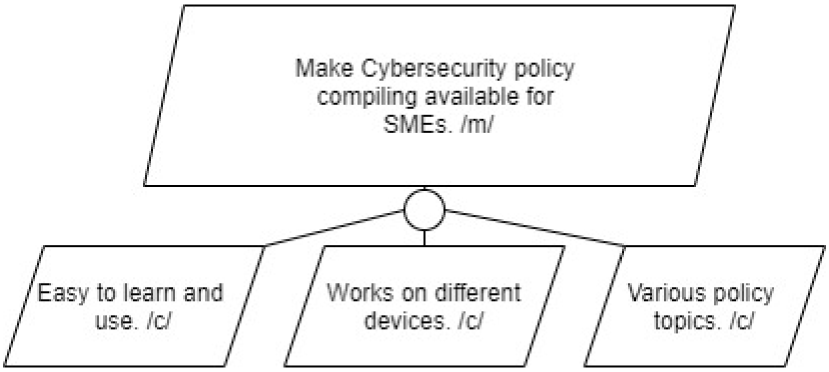

Make Cybersecurity policy compiling available for SMEs. /m/
Easy to learn and use. /c/
Works on different devices. /c/
Various policy topics. /c/

Figure 5 - Primary concern (goal sketching)

This figure gives a summary of the primary concern and constraints of the software artefact.

The Sprint I must include a more detailed set of constraints, provided in Figure 6.

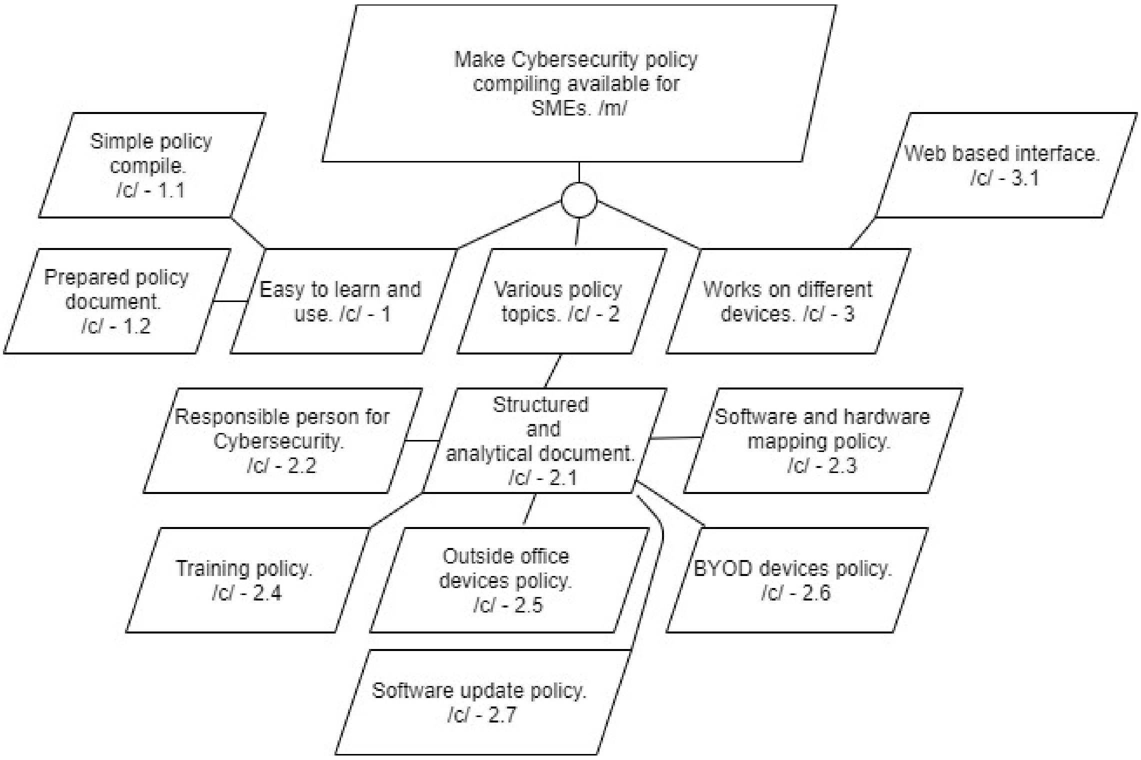

Make Cybersecurity policy compiling available for SMEs. /m/
Simple policy compile. /c/ - 1.1
Web based interface. /c/ - 3.1
Prepared policy document. /c/ - 1.2
Easy to learn and use. /c/ - 1
Various policy topics. /c/ - 2
Works on different devices. /c/ - 3
Responsible person for Cybersecurity. /c/ - 2.2
Structured and analytical document. /c/ - 2.1
Software and hardware mapping policy. /c/ - 2.3
Training policy. /c/ - 2.4
Outside office devices policy. /c/ - 2.5
BYOD devices policy. /c/ - 2.6
Software update policy. /c/ - 2.7

Figure 6 - Extended primary concern (goal sketching)

Constraints are displayed in Table 4 to provide more detailed information to clarify the development needs.

Table 4 –Sprint I constraints

Constraint	Description	Explanation
1.1	Simple to compile	Compiling a policy must be straightforward and rational
1.2	The prepared policy document	The system must produce a full policy document
2.1	The structured and analytical document	The policy must be compiled using structured and analytical logic
2.2	Responsible person for cybersecurity	The policy document must include a responsible person section
2.3	Software and hardware mapping policy	The policy must include a hardware and software mapping section
2.4	Training policy	The policy must include a training policy section
2.5	Outside office devices policy	The policy must include a section on outside office devices
2.6	BYOD device policy	The policy must include a BYOD device section
2.7	Software update policy	The policy must include a software update section
3.1	Web-based user interface	The software must work on mobile devices and computers

5.3.2 Requirements prioritisation

Wieger´s matrix approach was selected for requirements prioritisation. As the model requires, each dimension was rated on a relative scale between 1-9 (1 being low and 9 being high), the dimensions including benefit, penalty, cost, risk, values. These were used to calculate the prioritisation order. Furthermore, each weighting factor was set to one as they benefit equally to the risk formula. As the user interface requirements are the ones that give the first impression of the software, their requirements were prioritised as the highest in Sprint I. The Sprint I requirements are displayed in Table 5.

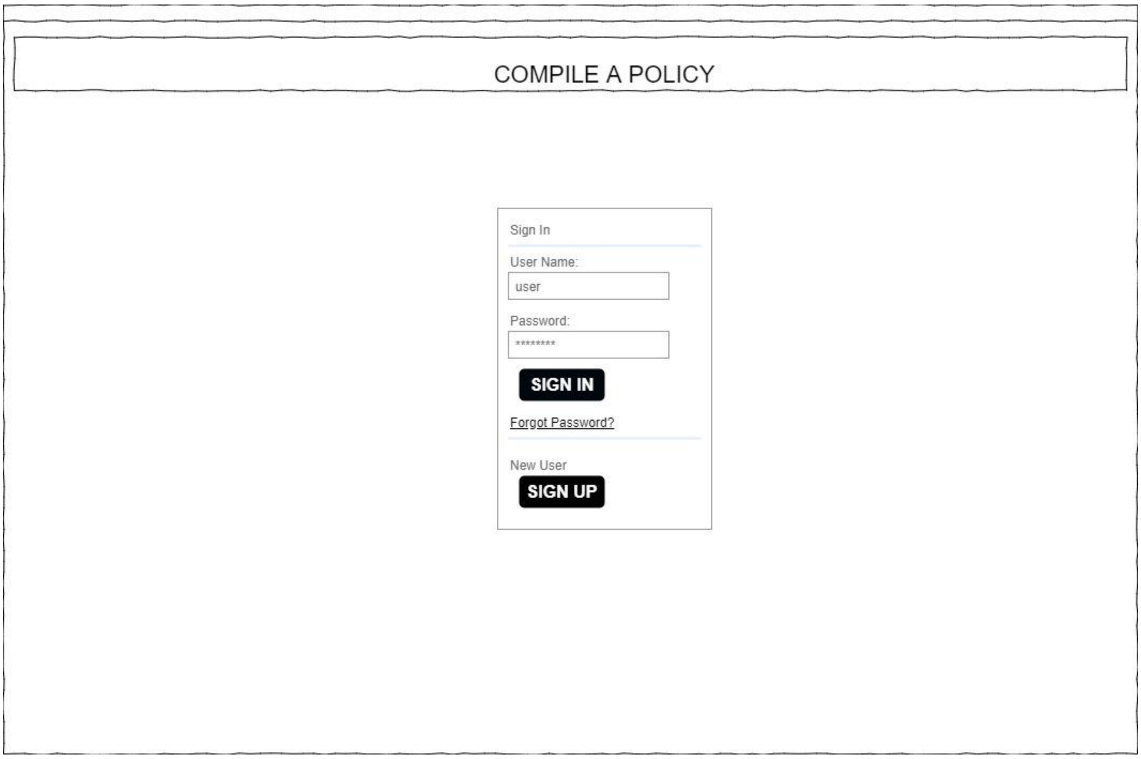
Table 5 –Sprint I requirement prioritisation

Feature	**Relative Benefit**	**Relative Penalty**	**Total Value**	**Value %**	**Relative Cost**	**Cost %**	**Relat ive Risk**	**Risk %**	**Priorit y**
1.1	9	9	18	13,8	1	2,4	1	2,6	2,762
1.2	9	9	18	13,8	1	2,4	1	2,6	2,762
3.1	9	9	18	13,8	5	11,9	1	2,6	0,953
2.1	7	7	14	10,8	1	2,4	5	13,2	0,693
2.2	7	7	14	10,8	3	7,1	5	13,2	0,530
2.3	6	6	12	9,2	5	11,9	5	13,2	0,368
2.5	5	5	10	7,7	6	14,3	5	13,2	0,280
2.7	5	5	10	7,7	6	14,3	5	13,2	0,280
2.4	4	4	8	6,2	7	16,7	5	13,2	0,206
2.6	4	4	8	6,2	7	16,7	5	13,2	0,206
Totals	65	65	130	100,0	42	100,0	38	100,0	9,042

The table is ordered by priority. As requirements 1.1, 1.2, and 3.1 are related to usability and software development, they were considered cross-related objectives and added to the first iteration. The lower priority requirements were standalone because they represent different policy content parts and can be incorporated independently. It was decided to include all Sprint I requirements since it is required for the first interview to give the comprehensive impression of the artefact as possible.

5.3.3 Visual design requirements

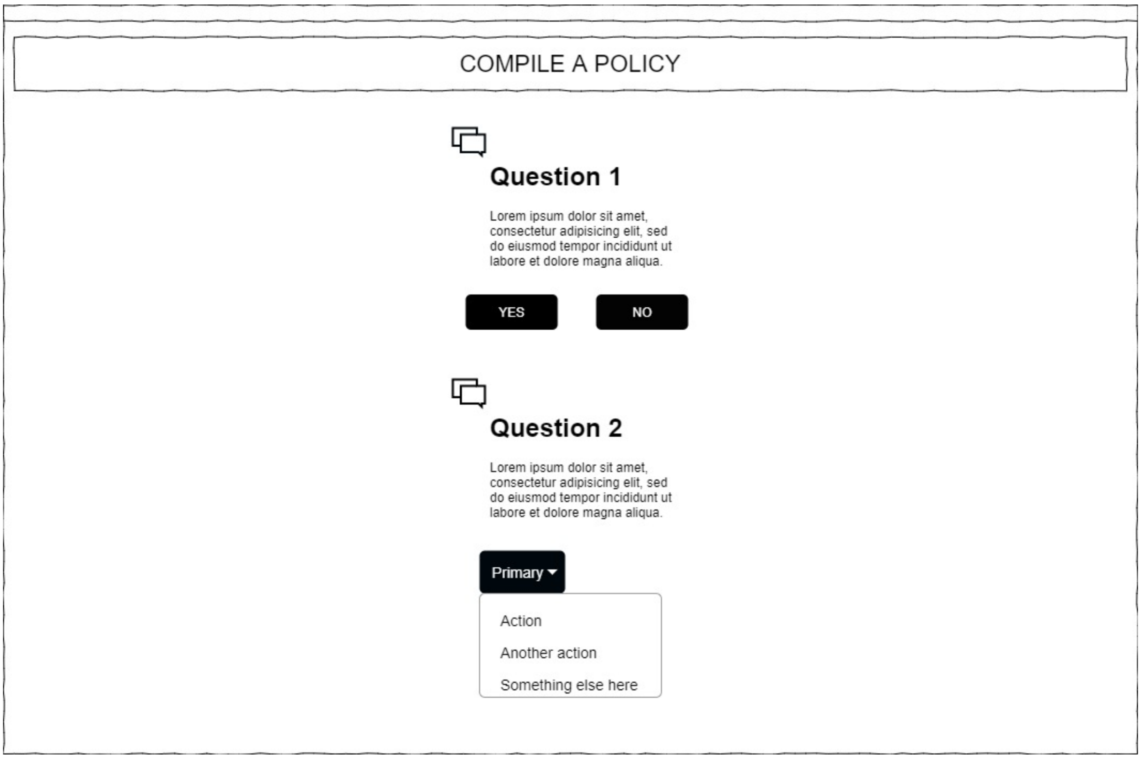
A visual design mockup was proposed based on requirements. The mockups display each view as they are characterised by their purpose. The design style for policy creation is to gather most of the information by answering survey-type questions. This approach ensures that there is only one way to interpret the answer. The artefact will be web-based, using the responsive design framework to ensure maximum compatibility. The user must register an account to access the artefact. After registration, the user must use the checkboxes or different input fields to complete the form. In the last step, the policy is displayed to the user. The mockups are displayed in Figures 7, 8 and 9.



User Name: user

Password: ********

Figure 7 - Login page (mockup)



COMPILE A POLICY
Question 1
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
YES
NO
Question 2
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
Primary
Action
Another action
Something else here

Figure 8 - Compile a policy (mockup)

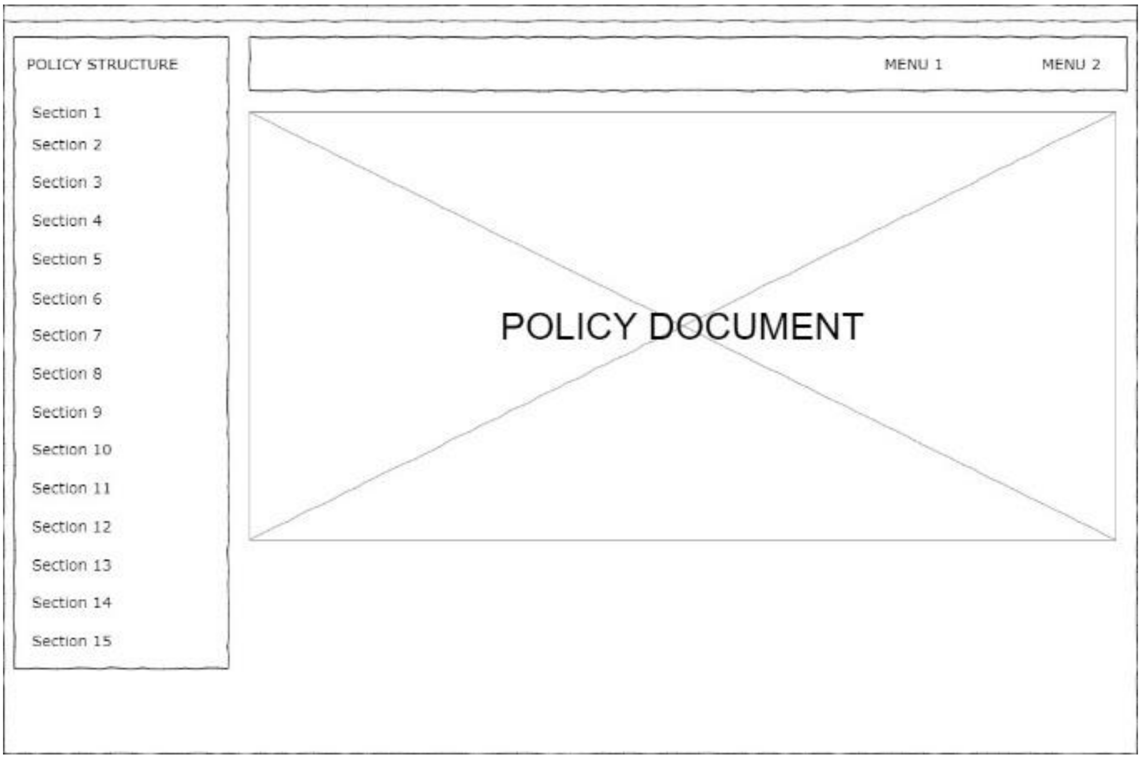


Figure 9 - Policy overview (mockup)

5.4 Sprint II

Sprint I was based on literature research and data provided by the survey. Sprint II includes an interview with an SME representative to verify the extracted requirements and artefact development roadmap.

5.4.1 Findings from the interview

The first interview was conducted with an SME that qualified as a micro-enterprise. The interview confirmed the necessity for a presented artefact in some cases and the SME’s general limited knowledge about cybersecurity topics. The interview confirmed the need for the policy chapters, introduced from the first iterations, and added risk presentation options. As the literature review findings were introduced that were not included in Sprint I, it was confirmed that the additional policy chapters that are on a more technical level should be added.

One of the security governance findings was controls [39], extracted from ISO/IEC 27032, but all the frameworks encouraged utilising it. However, as this approach needs a very company-specific approach, it was decided to include the ENISA [1] top risks to the policy to provide real examples and up-to-date information to the policy users. The first interview findings are presented in Table 6.

Table 6 - First interview findings

Constraint	**Description**	**Finding**
1.1	Simple to compile	Confirmed
1.2	Prepared policy document	Confirmed
2.1	Structured and analytical document	Confirmed
2.2	Responsible person for cybersecurity	Confirmed
2.3	Software and hardware mapping policy	Confirmed

2.4	Training policy	Confirmed
2.5	Outside office devices policy	Confirmed
2.6	BYOD device policy	Confirmed
2.7	Software update policy	Confirmed
3.1	Web-based user interface	Confirmed
3.2	Policy edit feature	New & confirmed
3.3	Critical data policy	New & confirmed
3.4	Passwords policy	New & confirmed
3.5	Incident handling policy	New & confirmed
3.6	Physical security policy	New & confirmed
3.7	Logging and monitoring policy	New & confirmed
3.8	ENISA cybersecurity risks	New & confirmed
3.9	Backup policy	New & confirmed
3.10	Baseline policy	New & confirmed
3.11	ENISA risks headers in a different colour	New & confirmed

5.4.2 Requirements modelling

The new findings from the first interview and literature review were added to the model and not included in Sprint I. They were included into the Sprint II goal modelling. The goal sketch includes new findings displayed on the green background. The sketch is displayed in Figure 10.

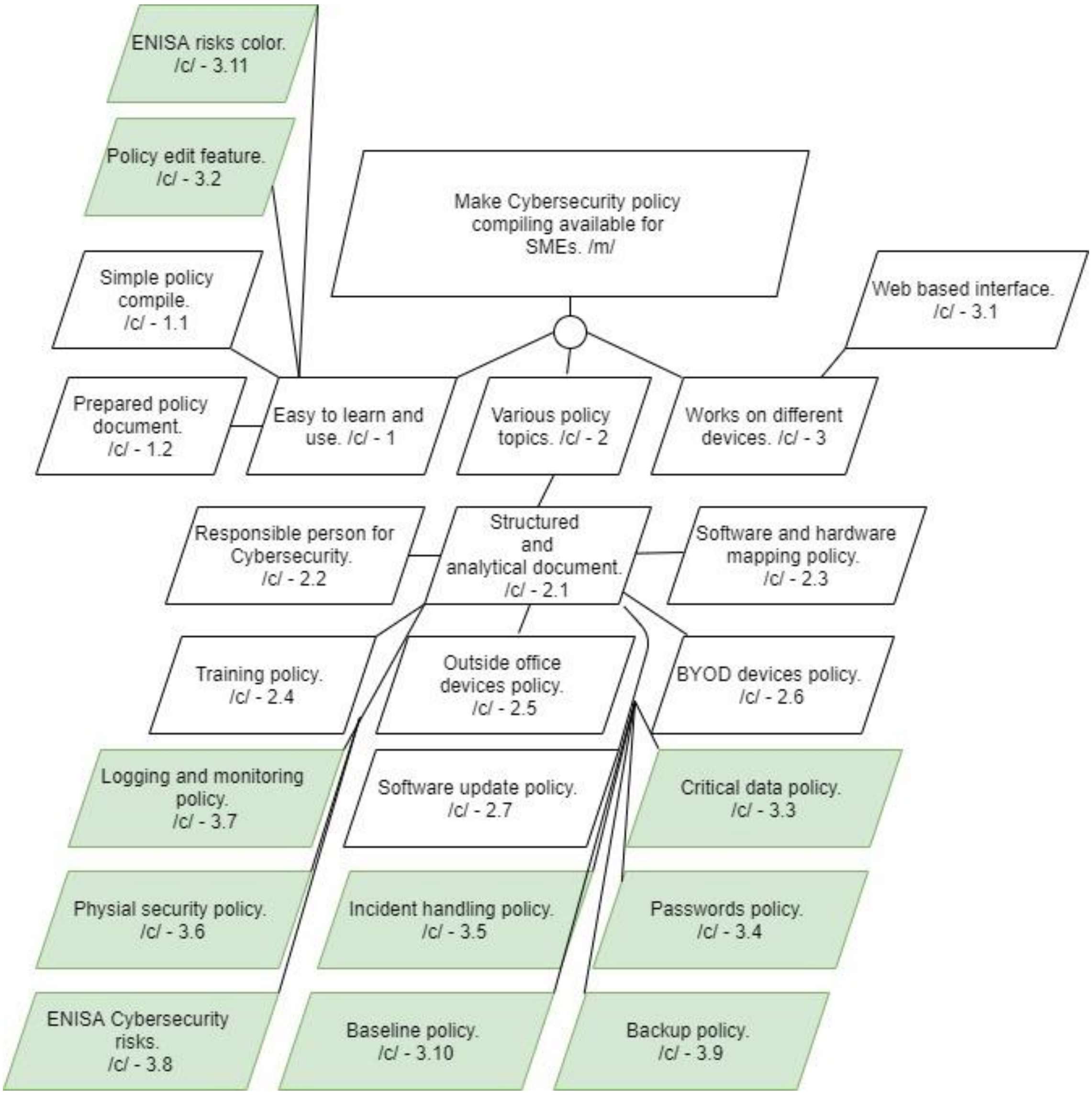

ENISA risks color. /c/ - 3.11
Policy edit feature. /c/ - 3.2
Make Cybersecurity policy compiling available for SMEs. /m/
Simple policy compile. /c/ - 1.1
Web based interface. /c/ - 3.1
Prepared policy document. /c/ - 1.2
Easy to learn and use. /c/ - 1
Various policy topics. /c/ - 2
Works on different devices. /c/ - 3
Responsible person for Cybersecurity. /c/ - 2.2
Structured and analytical document. /c/ - 2.1
Software and hardware mapping policy. /c/ - 2.3
Training policy. /c/ - 2.4
Outside office devices policy. /c/ - 2.5
BYOD devices policy. /c/ - 2.6
Logging and monitoring policy. /c/ - 3.7
Software update policy. /c/ - 2.7
Critical data policy. /c/ - 3.3
Physial security policy. /c/ - 3.6
Incident handling policy. /c/ - 3.5
Passwords policy. /c/ - 3.4
ENISA Cybersecurity risks. /c/ - 3.8
Baseline policy. /c/ - 3.10
Backup policy. /c/ - 3.9

Figure 10 - New findings (goal sketching)

The findings are displayed in Table 7 to describing the definition and explanation.

Table 7 - Second interview findings

Constraint	Description	Finding
3.2	Policy edit feature	The system must have the option to edit the policy document.
3.3	Critical data policy	The policy must include a critical data policy section

3.4	Passwords policy	The policy must include a password policy section
3.5	Incident handling policy	The policy must include an incident handling policy section
3.6	Physical security policy	The policy must include a physical policy section
3.7	Logging and monitoring policy	The policy must include a logging and monitoring policy section
3.8	ENISA cybersecurity risks	The policy must include an ENISA TOP Cybersecurity risk section
3.9	Backup policy	The policy must include a backup policy section
3.10	Baseline policy	The policy must include a baseline security policy section
3.11	ENISA risks in a different colour	The risk header must be in a different colour

5.4.3 Requirements prioritisation

In Sprint II, the Wieger's matrix approach was applied for a second time to the requirements defined. As the model requires, each dimension was rated on a relative scale of 1-9 (9 denoting high), including benefit, penalty, cost, risk, values to calculate our prioritisation order. Furthermore, each weighting factor is set to one as they contribute equally to the risk formula.

Sprint II has two types of requirements—software development and policy content. At first, the software development will be prioritised because the SME requests the functionality. Secondly, all the policy chapters from interview findings will be prioritised. Priorities are displayed in Table 8.

Table 8 - Sprint II requirement prioritisation

Feature	Relative Benefit	Relative Penalty	Total Value	Value %	Relative Cost	Cost %	Relative Risk	Risk %	Priority
3.2	9	1	10	10,9	9	16,7	1	6,7	0,466
3.3	8	1	9	9,8	5	9,3	2	13,3	0,433
3.4	8	1	9	9,8	5	9,3	2	13,3	0,433
3.5	8	1	9	9,8	5	9,3	2	13,3	0,433
3.6	8	1	9	9,8	5	9,3	2	13,3	0,433
3.7	8	1	9	9,8	5	9,3	2	13,3	0,433
3.8	8	1	9	9,8	5	9,3	2	13,3	0,433
3.9	8	1	9	9,8	5	9,3	2	13,3	0,433
3.10	8	1	9	9,8	5	9,3	2	13,3	0,433
3.11	9	1	10	10,9	5	9,3	1	6,7	0,683
Totals	82	10	92	100,0	54	100,0	15	113,3	3,930

The table is ordered by priority, and software development related 3.2 and 3.11 is prioritised higher due to the software functionality. All other constraints are related to policy content development and are prioritised equally.

5.4.4 Visual design requirements

The policy overview document is updated to be compliant with the edit requirement. The edit and preview pages are merged into one, and a WYSIWYG editor is added for keeping the interface simple. The updated mockup view is presented in Figure 11.

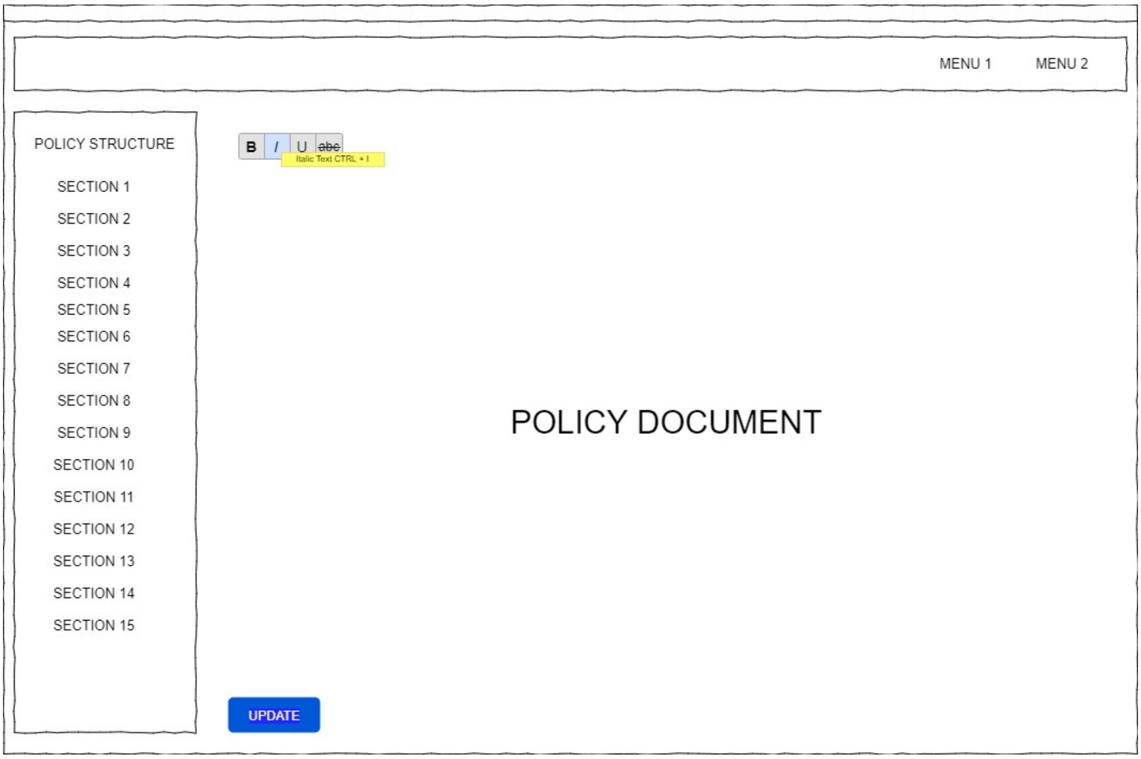


Figure 11- Policy overview update (mockup)

5.5 Software development

PHP [52], Python [53], and WordPress [54] were explored as the choices for prototype development. An active discussion was held with different software developers and research was conducted within online development forums and websites.

PHP and Python are programming languages, and WordPress is a popular open-source platform built on PHP, which is used to develop websites or blogs.

WordPress is used in 40% of websites and features a vast list of plugins. Numerous WordPress plugins that could meet the development needs were analysed, but the search did not return enough compact ones. The choice of the different plugins that have to be used for prototype development does not justify the management overhead and complexity.

Python is known for its clean syntax and easy to learn basics. Django [55] is one of the popular Python web frameworks, and it grows more popular and is utilized in several big software projects. It was decided not to use Python for development because the options to host the Python applications are more limited and could add more cost than PHP alternatives.

It was agreed that the artefact would be developed in the PHP [52] programming language, using the Laravel [56] framework. The PHP language popularity justifies this choice in web applications and it is easy to find a compatible hosting platform. The Laravel framework was selected because of its popularity in the development community and due to the existence of various ready-to-use components for this type of project. The MySQL [57] database was selected for data storage as this is the most popular and proven option for this type of web application. Jay Paul Aying from Blend IT OÜ consulted on the PHP Laravel development.

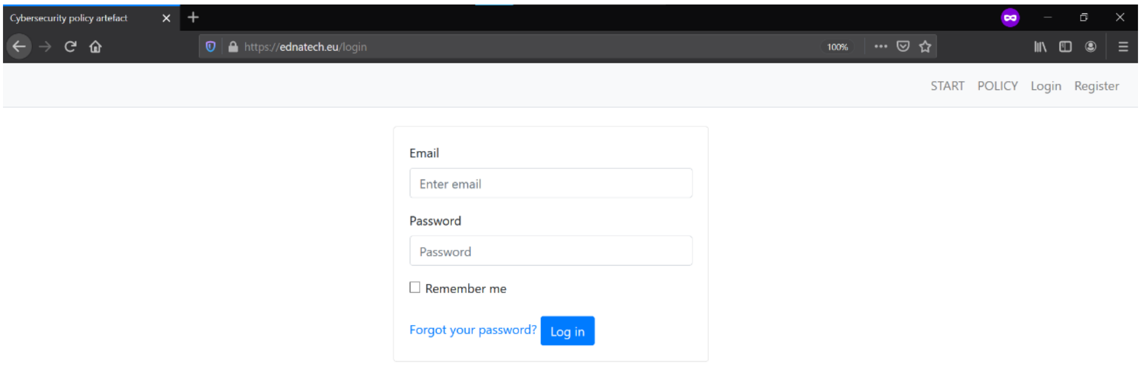
5.5.1 Use of the artefact

The prototype artefact is accessible on the http://www.ednatech.eu domain.

The tool is free to use, but it is intended to continue the development in order to make the tool available for commercial usage. If the commercial development should fail to start, the source code will be made available for free.

5.5.2 Screenshots of the artefact

In this chapter, the pictures of the actual prototype artefact are presented.



Email

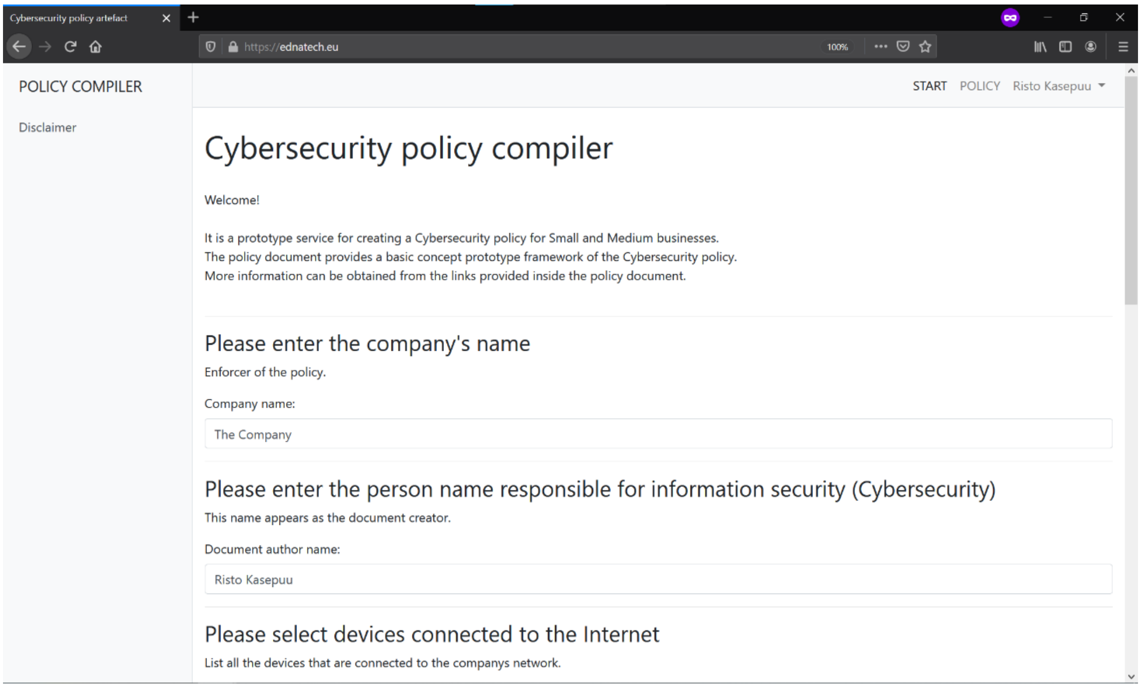
Enter email

Password

Password

□ Remember me

Figure 12 – Login page (screenshot)



Cybersecurity policy compiler

Welcome!

It is a prototype service for creating a Cybersecurity policy for Small and Medium businesses.
The policy document provides a basic concept prototype framework of the Cybersecurity policy.
More information can be obtained from the links provided inside the policy document.

Please enter the company's name

Enforcer of the policy.

Company name:

The Company

Please enter the person name responsible for information security (Cybersecurity)

This name appears as the document creator.

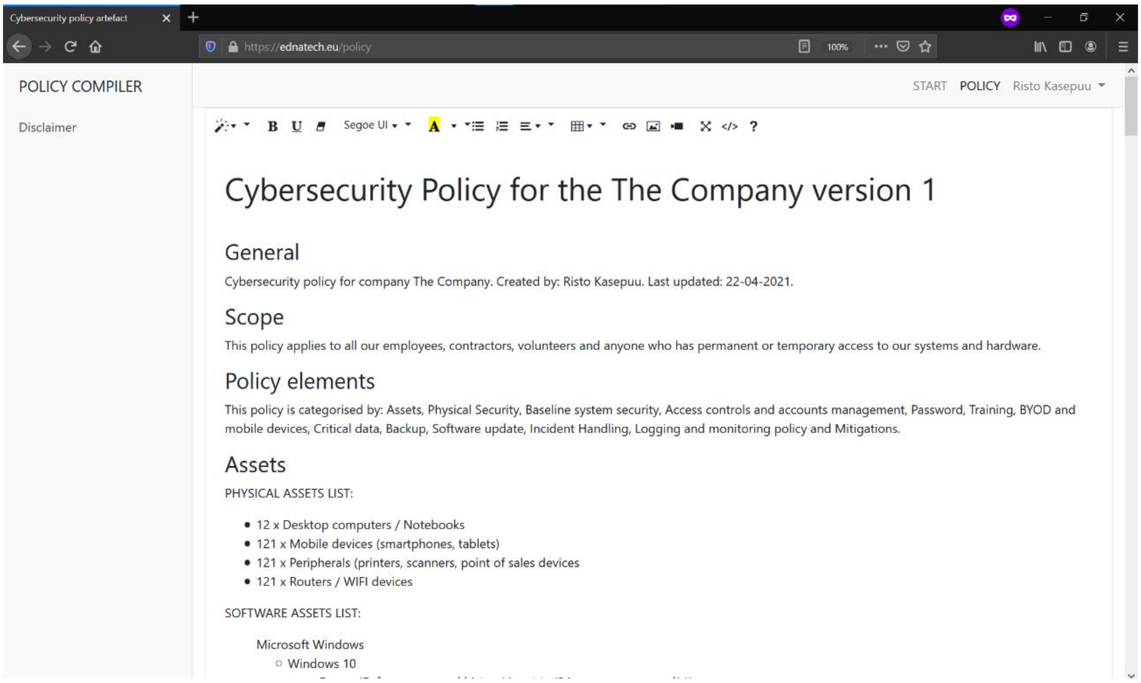
Document author name:

Risto Kasepuu

Please select devices connected to the Internet

List all the devices that are connected to the companys network.

Figure 13 – Compile policy (screenshot)



Cybersecurity Policy for the The Company version 1

General

Cybersecurity policy for company The Company. Created by: Risto Kasepuu. Last updated: 22-04-2021.

Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

This policy is categorised by: Assets, Physical Security, Baseline system security, Access controls and accounts management, Password, Training, BYOD and mobile devices, Critical data, Backup, Software update, Incident Handling, Logging and monitoring policy and Mitigations.

Assets

PHYSICAL ASSETS LIST:

- 12 x Desktop computers / Notebooks
- 121 x Mobile devices (smartphones, tablets)
- 121 x Peripherals (printers, scanners, point of sales devices
- 121 x Routers / WIFI devices

SOFTWARE ASSETS LIST:

Microsoft Windows
- Windows 10

Figure 14 – Policy viewer/editor (screenshot)

6 Evaluation

This chapter validates the requirements extracted from literature research, the survey responses, and SME interviews.

Two interviews were conducted. In the first one, the requirements from the survey responses and non-functional findings are validated.

The second interview will validate requirement findings from the first interview, literature research, and non-functional findings. The second interview also validates the proposed concept prototype policy artefact.

6.1 Findings

The goal of this chapter is to validate the prototype artefact findings.

6.1.1 Interview I

Interview I summary is attached in Appendix 5. Interview statements that contribute to the artefact validation are expressed.

IV1 - a. Artefact should be easy to use and understand.

IV1 - b. The artefact should compile a structured full policy document that is understandable for non-specialists.

IV1 – b. The time spent using the artefact should be as efficient as possible.

IV1 – c. The presented artefact user interface is validated as easy to use and understand. Survey-style questions are an excellent way to use the artefact.

IV1 – d. User account generation in the artefact is confirmed.

IV1 – e. Broader policy topic coverage requirements are validated.

IV1 – f. Policy edit feature request is new information and added to the requirements list.

IV1 – g. The web-based interface is confirmed.

IV1 – h. ENISA risk headers in a different colour are new information and added to the requirements list.

6.1.2 Interview II

IV2 – a. User interface usability is confirmed.

IV2 – b. The policy edit feature is confirmed.

IV2 – c. Policy chapters are confirmed.

IV2 – d. Assets, OS list, and additional software are confirmed.

IV2 – e. ENISA Top risks are confirmed.

IV2 – f. The web-based interface is confirmed.

IV2- g. CERT information is confirmed.

IV2 -h. A clear policy structure is confirmed.

IV2 -i. ENISA risks headers in a different colour are confirmed.

6.1.3 Requirement validation

The interviews with SMEs were used for the requirement validation. Two interviews were conducted with an SME, and the validation results are listed in Table 9.

Table 9 - Requirements validation

Constraint	**Description**	**Validated by**
1.1	Simple to compile	IV1
1.2	Prepared policy document	IV1, IV2
2.1	Structured and analytical document	IV1, IV2
2.2	Responsible person for cybersecurity	IV1
2.3	Software and hardware mapping policy	IV1, IV2
2.4	Training policy	IV1, IV2
2.5	Outside office devices policy	IV1, IV2
2.6	BYOD device policy	IV1, IV2
2.7	Software update policy	IV1, IV2
3.1	Web-based user interface	IV2
3.2	Policy edit feature	IV2
3.3	Critical data policy	IV1, IV2
3.4	Passwords policy	IV1, IV2

3.5	Incident handling policy	IV1, IV2
3.6	Physical security policy	IV1, IV2
3.7	Logging and monitoring policy	IV1, IV2
3.8	ENISA Cybersecurity risks	IV1, IV2
3.9	Backup policy	IV1, IV2
3.10	ENISA Cybersecurity risk headers in a different colour	IV2

The non-functional requirements that are included in this research are present in a table on their validation. Non-functional requirements are displayed in Table 10.

Table 10 - Non-functional requirements validation

Description	**Validated by**
Clear communicative objectives	IV1, IV2
Prepared policy document	IV1, IV2
Clear structure	IV1, IV2
Clearly defined concepts	IV1, IV2
Keep up-to-date	IV1, IV2
Stakeholders	IV1, IV2
Common sense	IV2
Up to date threat information	IV1, IV2

6.1.4 Conclusion

The findings were validated using interviews with SMEs. All the requirements were validated.

7 Summary

This chapter will discuss conclusions, limitations, and recommendations for future works.

7.1.1 Conclusions

This master's thesis followed the Design Science Research Methodology process [14].

At first, the problem and motivation were identified. Second, the objectives of a solution were defined. Third, an artefact was designed and validated using the DSRM process.

The thesis proposed a prototype concept artefact for helping compile the cybersecurity policy. Several sub-questions helped guide the research path. Each research question will be discussed individually.

SQ1: Research into most common cybercrimes threats in the EU SMEs sector.

As the literature review presented, the most common cybercrimes threats to the EU SMEs sector include: Malware, Web-based Attacks, Phishing, Web Application Attacks, SPAM, Distributed Denial of Service (DDoS), Identity Theft, Data Breach, Insider Threat, Botnets, Physical Manipulation, Damage, Theft and Loss, Information Leakage, Ransomware, Cyber Espionage, Cryptojacking.

The list is not final, but it represents the TOP 15 from the ENISA report [1]. As the literature research showed, the information security governance frameworks do not offer up-to-date solutions for cybersecurity threats and mitigations. The ENISA threat report was applied as a source of the artefact mitigation chapter.

SQ2: Research into the most common information security governance frameworks and, if possible, select appropriately for SMEs.

As the result of the analysis, it is found that the most common security governance frameworks are ISO [35], CIS [36], NIST [37], ENISA [38]. All of them (except for ENISA) provide guidelines on what chapters the cybersecurity policy document could include.

As this research revealed, the security governance frameworks themselves are building blocks that SMEs must put together to meet the business requirements. All the researched frameworks provide different components that a cybersecurity policy could include. However, none of the researched frameworks provided a complete cybersecurity document structure or detailed concept examples that can be used in a real-life situation.

The second factor that was discovered was that the oldest and most established frameworks (for example, ISO family frameworks) are intended for larger organisations. In the typical case, SMEs lack the resources or even the organisational structure to implement the policy proposed by such frameworks.

SQ3: Collect extra knowledge about the functionality of the prototype tool by using a survey.

As the research required additional knowledge for building the artefact, literature was researched and discussions with experts were held. It was decided that a survey is the preferred method for data collection.

The quantitative research method was selected, and a web survey was conducted. The survey questions were self-designed and verified by experts.

Questions are included in Appendix 1 and a list of survey findings in Appendix 7.

RQ: Can the absence of cybersecurity knowledge in the SMEs be supported by the tool to aid in developing cybersecurity policy?

As the research demonstrated, there is no software tool available for SMEs to aid in developing cybersecurity policy. The proposed prototype artefact brings the knowledge of cybersecurity policy closer to SMEs and makes cybersecurity policy further understandable and approachable.

While answering the main research question, it was confirmed in the interviews that prototype artefact supports the absence of cybersecurity knowledge that various SMEs might have. The prototype artefact provides the right starting point for compiling a cybersecurity policy.

Still, this research can form the beginning of more substantial research. The proposed prototype artefacts can be seen as a concept of the technical cybersecurity knowledge base, which is frequently updated and commonly used by stakeholders.

7.1.2 Reflections on the research process and results

The following actions were undertaken in the process of the research and problem space analysis.

The novel real-world problem was identified, connected, and translated into a research question.

- A suitable research method was selected and applied to the research question.

Once the research method was decided on, the research proper was conducted to validate the hypotheses postulated for the thesis.

- Different analyses were conducted to gather requirements for policy structure, topics, and artefact development.
- Existing information security governance frameworks were deemed insufficient as they do not provide ready-to-use cybersecurity policy documents.

- The findings of the research were then converted to the software artefact requirements.
- A novel policy structure template and model was established as a stepping stone for SMEs.

From there, the artefact was developed and validated as a meaningful and valuable option for SMEs. The following core tenets were observed:

- The artefact is easy to use and easy to understand.
- The artefact counters the lacking cybersecurity knowledge of SMEs.
- The artefact will improve SMEs cybersecurity level if the policy is implemented.
- The artefact inspires SMEs to develop cybersecurity policy and documentation.

In conclusion, the research question posed was answered—an artefact can help compensate for missing cybersecurity knowledge in SMEs.

7.1.3 Artefact

Prototype artefact is available at https://www.ednatech.eu.

7.1.4 Limitations

Each research paper contains many trade-offs and choices to respect the paper's purpose and time constraints.

The proposed policy that the prototype artefact generates is not flawless and is built on research findings from literature research and the survey. To provide additional research dept, it could have included requirement collection done via focus group interviews. However, time constraints and the COVID-19 situation were the deciding factors not to use this method.

The proposed concept prototype policy artefact offers a limited and simplified view of the cybersecurity policy compiling because of the common-sense approach that was always considered. The policy can be a highly complex document, dependent on the details of the company's business processes, and the research of this thesis can offer only a surface level approach.

As the methodology research reveals, the artefact validation could be done by a case study or group interview.

The case study was considered as an artefact validation option. However, this methodology anticipates full cooperation with an SME, detailed exposure of the business processes, secrets, and a lengthy time period. These factors did not fit the scope and timeframe.

Because of the COVID-19 situation, it was discussed having a video conference with a small number of potential participants, but the interest in this type of interview was inconclusive.

It is noted that the selected approach limits the validation credibility. Nevertheless, the belief in the prototype artefact validity and usefulness is strong because the contacts of some companies involved in the survey expressed interest in using the artefact in real-life situations.

As one of the research findings was up-to-date policy, which was confirmed in the validation interview, it was added under the limitations part and is subject to further study.

As the ENISA threats report was used to add the different cybersecurity risks, generally updated once a year, it provides updated information and mitigation compared to the information governance frameworks analysed in this paper.

However, the policy could be updated against the live threats database to provide maximum effectiveness in real-world usage situations.

7.1.5 Recommendations for the future works

As the research showed, compiling a cybersecurity policy can take many months to complete. The process does not end there; the policy must be updated continuously to fit the ever-changing cybersecurity landscape. As the concept prototype was proposed to be utilized as a backbone for policy building, it is fair to admit that this approach is simplified and unlocks only the complex policy universe's surface.

7.1.5.1 Sector-specific cybersecurity policies.

Various business sectors need a more detailed approach to cybersecurity policy. As this paper differentiated companies in this research by the size defined in the EU, it is not always the obvious choice. For example, a small fintech team with less than ten-person can require complicated cybersecurity and related policies to comply with the banks or card issuing organisations, plus different regulative norms worldwide. In the EU's case, GDPR is also always in the background.

The recommendation for future papers is to investigate different business areas and focus on the policy of a specific sector. This research direction could add value to the selected sector and provide business sector-based cybersecurity templates for companies to use and to improve cybersecurity awareness.

7.1.5.2 Automated AI-generated policies.

Another proposed research path lies within automation, integration, and AI.

Some paragraphs of the cybersecurity policy should always be up to date, without human interruption, for example, the company’s specific assets and valid cybersecurity threats. Various tools can map infrastructure assets and software down to deeper levels. The policy compiler could be integrated with this type of service to add more value by doing less editor work and reducing human errors.

Also, if there is no dedicated person appointed for network monitoring, which is quite common in SMEs, the up-to-date assets monitoring can raise alerts when a new device appears in the network. The threats policy could offer real-time threat information to policy users.

References

[1] "ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected." https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (accessed Nov. 04, 2020).

[2] C. Kent, M. Tanner, and S. Kabanda, "How South African SMEs address cyber security: The case of web server logs and intrusion detection," in *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Aug. 2016, pp. 100–105, doi: 10.1109/EmergiTech.2016.7737319.

[3] P. O. of the E. Union, "User guide to the SME definition.," Sep. 03, 2020. http://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1 (accessed Feb. 04, 2021).

[4] "SME definition," *Internal Market, Industry, Entrepreneurship and SMEs - European Commission*, Jul. 05, 2016. https://ec.europa.eu/growth/smes/sme-definition_en (accessed Jan. 03, 2021).

[5] European Network and Information Security Agency., *Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* LU: Publications Office, 2015.

[6] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Jun. 2020, pp. 1–5, doi: 10.1109/CyberSA49311.2020.9139638.

[7] "EUR-Lex - 32016R0679 - EN - EUR-Lex." https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed Feb. 04, 2021).

[8] "EUR-Lex - 32016L1148 - EN - EUR-Lex." https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed Feb. 04, 2021).

[9] "NIS Directive." https://www.enisa.europa.eu/topics/nis-directive (accessed Feb. 04, 2021).

[10] E. Rostami, F. Karlsson, and S. Gao, "Requirements for computerized tools to design information security policies," *Comput. Secur.*, vol. 99, p. 102063, Dec. 2020, doi: 10.1016/j.cose.2020.102063.

[11] "The Map of Cybersecurity Domains (version 2.0) | LinkedIn." https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/ (accessed Dec. 13, 2020).

[12] R. J. Wieringa, *Design Science Methodology for Information Systems and Software Engineering*. Springer, 2014.

[13] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[14] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[15] R. Koeze, "Designing a cyber risk assessment tool for small to medium enterprises," 2017, Accessed: Nov. 23, 2020. [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid%3A8ffae35d-0695-4eb9-b488-471bd1c9e10d.

[16] M. Stoica, M. Mircea, and B. Ghilic-Micu, "Software Development: Agile vs. Traditional," *Inform. Econ.*, vol. 17, no. 4/2013, pp. 64–76, Dec. 2013, doi: 10.12948/issn14531305/17.4.2013.06.

[17] A. Aurum and C. Wohlin, Eds., *Engineering and managing software requirements*. Berlin: Springer, 2005.

[18] K. Schwaber and M. Beedle, *Agile software development with Scrum*, vol. 1. Prentice Hall Upper Saddle River, 2002.

[19] K. Beck, *Extreme programming explained: embrace change*. addison-wesley professional, 2000.

[20] A. Cockburn, *Crystal clear: A human-powered methodology for small teams: A human-powered methodology for small teams*. Pearson Education, 2004.

[21] "Scrum Team Roles and Responsibilities | Scrum Alliance." https://www.scrumalliance.org/about-scrum/team (accessed Feb. 22, 2021).

[22] P. Abrahamsson, O. Salo, J. Ronkainen, and J. Warsta, “Agile Software Development Methods: Review and Analysis,” *ArXiv170908439 Cs*, Sep. 2017, Accessed: Feb. 22, 2021. [Online]. Available: http://arxiv.org/abs/1709.08439.

[23] I. Inayat, S. S. Salim, S. Marczak, M. Daneva, and S. Shamshirband, “A systematic literature review on agile requirements engineering practices and challenges,” *Comput. Hum. Behav.*, vol. 51, pp. 915–929, Oct. 2015, doi: 10.1016/j.chb.2014.10.046.

[24] L. Cao and B. Ramesh, “Agile Requirements Engineering Practices: An Empirical Study,” *IEEE Softw.*, vol. 25, no. 1, pp. 60–67, Jan. 2008, doi: 10.1109/MS.2008.1.

[25] M. Daneva *et al.*, “Agile requirements prioritization in large-scale outsourced system projects: An empirical study,” *J. Syst. Softw.*, vol. 86, no. 5, pp. 1333–1353, May 2013, doi: 10.1016/j.jss.2012.12.046.

[26] D. Carlson and P. Matuzic, “Practical agile requirements engineering,” 2010.

[27] K. Boness and R. Harrison, “Goal Sketching: Towards Agile Requirements Engineering,” in *International Conference on Software Engineering Advances (ICSEA 2007)*, Aug. 2007, pp. 71–71, doi: 10.1109/ICSEA.2007.36.

[28] J. Karlsson, C. Wohlin, and B. Regnell, “An evaluation of methods for prioritizing software requirements,” *Inf. Softw. Technol.*, vol. 39, no. 14, pp. 939–947, Jan. 1998, doi: 10.1016/S0950-5849(97)00053-0.

[29] Z. Bakalova, M. Daneva, A. Herrmann, and R. Wieringa, “Agile Requirements Prioritization: What Happens in Practice and What Is Described in Literature,” in *Requirements Engineering: Foundation for Software Quality*, Berlin, Heidelberg, 2011, pp. 181–195, doi: 10.1007/978-3-642-19858-8_18.

[30] V. Mahnič and T. Hovelja, “On using planning poker for estimating user stories,” *J. Syst. Softw.*, vol. 85, no. 9, pp. 2086–2095, Sep. 2012, doi: 10.1016/j.jss.2012.04.005.

[31] K. E. Wiegers, “First Things First: Prioritizing Requirements,” p. 6, 1999.

[32] N. A. Ernst, A. Borgida, I. J. Jureta, and J. Mylopoulos, “Agile requirements engineering via paraconsistent reasoning,” *Inf. Syst.*, vol. 43, pp. 100–116, Jul. 2014, doi: 10.1016/j.is.2013.05.008.

[33] A. Hevner and S. Chatterjee, *Design Research in Information Systems*. .

[34] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards." https://www.pcisecuritystandards.org/pci_security/ (accessed Jan. 14, 2021).

[35] ISO, "ISO," *ISO*. https://www.iso.org (accessed Nov. 01, 2020).

[36] "CIS," *CIS*. https://www.cisecurity.org/ (accessed Jan. 15, 2021).

[37] "National Institute of Standards and Technology," *NIST*. https://www.nist.gov/ (accessed Jan. 14, 2021).

[38] "ENISA." https://www.enisa.europa.eu (accessed Nov. 08, 2020).

[39] ISO, "ISO - ISO/IEC 27001 — Information security management," *ISO*. https://www.iso.org/isoiec-27001-information-security.html (accessed Nov. 08, 2020).

[40] "0._Explanatory_note_and_overview_on_ISO_Survey_2019_results.pdf." Accessed: Jan. 14, 2021. [Online]. Available: https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_and_overview_on_ISO_Survey_2019_results.pdf?nodeid=21413237&vernum=-2.

[41] "Committee 09. ISO Survey of certifications to management system standards - Full results." Accessed: Jan. 14, 2021. [Online]. Available: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.

[42] ISO, "ISO/IEC 27032:2012," *ISO*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/43/44375.html (accessed Nov. 09, 2020).

[43] "List of ISO 27001 mandatory documents and records." https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-2013-revision/ (accessed Feb. 10, 2021).

[44] "CIS Controls SME Companion Guide," *CIS*. https://www.cisecurity.org/white-papers/cis-controls-sme-guide/ (accessed Feb. 10, 2021).

[45] "Cybersecurity for Small Business," *Federal Trade Commission*, Oct. 05, 2018. https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (accessed Feb. 11, 2021).

[46] "About ENISA - The European Union Agency for Cybersecurity." https://www.enisa.europa.eu/about-enisa/about-enisa (accessed Feb. 13, 2021).

[47] "Cloud Security Guide for SMEs." https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes (accessed Feb. 13, 2021).

[48] S. Easterbrook, J. Singer, M.-A. Storey, and D. Damian, "Selecting Empirical Methods for Software Engineering Research," in *Guide to Advanced Empirical Software Engineering*, F. Shull, J. Singer, and D. I. K. Sjøberg, Eds. London: Springer, 2008, pp. 285–311.

[49] A. Bryman, *Social research methods*, 4th ed. Oxford ; New York: Oxford University Press, 2012.

[50] "IEEE/ISO/IEC 24765-2017 - ISO/IEC/IEEE International Standard - Systems and software engineering--Vocabulary." https://standards.ieee.org/standard/24765-2017.html (accessed Apr. 08, 2021).

[51] "NIST CSF Policy Template Guide 2020." https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf (accessed Mar. 04, 2021).

[52] "PHP: Hypertext Preprocessor." https://www.php.net/ (accessed Mar. 24, 2021).

[53] "Welcome to Python.org," *Python.org*. https://www.python.org/ (accessed Apr. 08, 2021).

[54] "Blog Tool, Publishing Platform, and CMS," *WordPress*. https://wordpress.org/ (accessed Apr. 08, 2021).

[55] "The Web framework for perfectionists with deadlines | Django." https://www.djangoproject.com/ (accessed Apr. 08, 2021).

[56] "Laravel - The PHP Framework For Web Artisans." https://laravel.com/ (accessed Mar. 24, 2021).

[57] "MySQL." https://www.mysql.com/ (accessed Apr. 09, 2021).

Appendix 1 – Survey questions

Hello!

I am Taltech Cybersecurity II years masters student, and I need your input to complete my master's thesis. This survey takes approximately 5 minutes to answer.

The aim of this master's thesis is to develop software that would help small and medium-sized enterprises to compile a set of information security (Cybersecurity) rules. The survey is anonymous, and the answers are used in a generalised form.

* If you have any questions about the survey or would like to receive a summary, please leave your email.

* If you would like to participate in a software/tool prototype validation interview, please leave your email address.

* If you have any questions, please send an email to ristok@outlook.com

Thank you!

Question	Measurement
Describe the environment requirements (organisational and technical) the prototype tool must comply.	Choice between < 10, < 50, < 250.
What is the turnover of your company?	The choice between Less or equal to 2 million €, Less or equal to 10 million €, Less or equal to 50 million €.
Has your company ever been affected or involved in a cyber security incident?	The choice between yes and no.
Have you calculated how much is your company's digital data (information) worth?	Multiple choice between Less than 5000€, 5000 - 10 000€, 10 000 - 50 000€, 50 000 - 100 000€, 100 000 - 1 000 000€, More than 1 000 000 €.
Have you ever done information security analysis in your company?	The choice between yes and no.
Do you have an appointed person who is responsible for information security in your company?	The choice between yes and no.
Have you mapped your company hardware and software?	The choice between yes and no.
Is your company outsourcing IT management services?	Multiple selections option and free text input, Yes, full responsibility (hardware, software, regulations, etc) is outsourced, Partially, only hardware management, Partially, only software management, Partially, only regulations, No, Other.
Is your company using an information security governance framework?	Multiple selections option and free text input, ISO, ISKE, CIS, NIST, ENISA, We have our own internal rules, Not using at all, Other.
Do you need a better solution for managing a company's information security regulations?	The choice between yes and no.

Would you use a tool that gives you a possibility of compiling a set of information security regulations for your company?	The choice between yes and no.
Are regular information security trainings conducted for the company's employees?	The choice between yes and no.
How much time are you willing to spend learning information security regulation tool functionality?	The choice between, 1 hours, 3 hours, 1 working day, No time at all
Please select the company's budget (including manhours) allocated to information security regulation management.	Selection between, Less than 1000€ per year, More than 10 000€ per year, More than 30 000€ per year, Prefer not to say.
Do you have procedures in place for devices that are used outside the physical office?	The choice between yes and no.
What type of devices are the users in your company mostly using?	Multiple choice option, Notebook computers, phone, tablet, Desktop computers
Do users use their own (BYOD) devices for work?	
What type of OS'es is your company using?	Multiple selections option and free text input, Microsoft Windows, MacOS, Linux, Android, iOS, Other
Are you using security products provided by the OS (example: Microsoft Defender Antivirus) provider?	The choice between yes and no.
What different types of information security devices and tools is you company using?	Multiple selections option between, Antivirus and anti-malware software, Mobile device security, Two-factor authentication, Email security, Access control, Data loss prevention, Firewall, Data encryption
Please rank "Easy to use" as a list of qualities of information security regulation tool:	Linear scale from 1 Not important to 5 Important.
Please rank "Easy to understand policy compiling" as a list of qualities of information security regulation tool:	Linear scale from 1 Not important to 5 Important.

Please rank "Offers ready to use policy" as a list of qualities of information security regulation tool:	Linear scale from 1 Not important to 5 Important.
Please rank "Compliant with information security governance frameworks (ISO, CIS, NIST, etc...)" as a list of qualities of information security regulation tool:	Linear scale from 1 Not important to 5 Important.

Appendix 2 – Literature research

Search engine	**Keyword**
Google Scholar / Scopus	(Cybersecurity OR cyber security OR security OR information security) AND
	• Cybersecurity • Small and medium enterprises • SME • Awareness • Risk • Tool • Artefact • Framework • Information security governance
	Design Science
	Agile AND
	• Software development • Methods • Requirement engineering • Prototype • Requirements modelling

Appendix 3 – Expert sessions

One of the expert interview sessions on various information security frameworks in the SME context was held with a cybersecurity expert with 10+ years of experience in the field. The concluded opinion from the professional experience was that implementing an ISO framework is a full-time coordination job for one person and that it requires cooperation between all departments supporting the effort.

In the second part of the discussion, the expert also enlisted some alternative frameworks to the ISO framework that an SME could consider implementing as a cybersecurity framework, and some of the framework implementation examples were discussed.

The third topic dealt with the potential academic study contact points with SMEs. The options discussed were an interview and a survey. It was decided to use the survey as the initial information collection method. We presented our survey questions to the expert and followed the feedback to adjust the questions for better suitability. We also agreed to use SMEs interviews to validate the artefact development and the final prototype.

Appendix 4 – Interview Guide

Part A, Introduction

- Short presentation of the topic and introduction of the research question.
- Disclaimer that the interview is anonymous and all data is used only for academic research.
- Confirmation that questions do not have to be answered if that is the preference of the interviewee.
- The interviewer asks permission to record the interview. Recorded materials will be later used for analysis.
- The interviewer states that the interviewee will receive the transcript of the interview after it is ready to review it and object if anything is deemed incorrect.

Part B, Demographic Questions

- Please describe your work responsibilities.

Part C, Company Background and Cybersecurity Questions

- How many people are working in the company?
- What is the company's annual turnover?
- Please give an overview of the IT solutions implemented at the company.
- Does the company have a person responsible for information security (cybersecurity)?
- Has the company performed any cybersecurity analysis before?
- Does the company have an existing cybersecurity policy enforced?

    - If yes, please describe the policy coverage, for example, password policy, user management policy etc.

    - If no, please describe the reason for not having a cybersecurity policy?

Part D, artefact questions

- Have you considered using software that can help you to compile a cybersecurity policy?

- If you could use this type of software, what effect would you expect?

    - Would this software help you explain and establish a baseline cybersecurity state within your company?

- What type of a user interface should this cybersecurity tool have?

- What type of questions should the artefact ask to provide value and understanding to non-IT or cybersecurity specialist.

Present the artefact.

- Please provide feedback about the artefact.

- Introduce different findings from the literature review, the survey and ask for feedback.

- Does the artefact support the missing cybersecurity knowledge that SMEs might have?

Appendix 5 – Summary of Interview I

At the beginning of the interview, the interview objective and research question are explained. It is confirmed that the interview is anonymous. All the business-related information will be kept private, and the questions can be left unanswered if that is deemed necessary by the interviewee.

The first interview was organized with a small contract programming company, with 15 employees, classified as micro-enterprises. The interview took place with the company's director, who oversees the company strategy, general management, sales management, and recruiting new people. The same person is in charge of cybersecurity. The IT solutions are not discussed due to them being part of the business secret.

The company does not have a cybersecurity policy in force because it has people with cybersecurity competencies, and one of the responsibilities for them is to assess the cybersecurity situation. The enterprise has never done a cybersecurity analysis, and they have never considered using a software solution for this purpose. If this type of tool exist it must be easy to use.

Artefact presentation. The question was asked about the policy scope. Literature research findings were introduced that are not yet implemented to the policy artefact. It was verified that the findings are helpful and should be involved in the policy. One of the remarks was about the top risks; the risks paragraphs should be in a different colour to be more visible in the document.

It was confirmed that survey style questions are easy to use and it is remarked that checklists are valuable in this business sector. The web-based interface is validated, as the artefact is demonstrated on the computer.

It was verified that the user interface of the artefact is straightforward and comfortable to understand. User account generation was confirmed to be effective as it is essential as the artefact contains business-sensitive information. It is confirmed that the policy should include a complete structured document filled with all the general information that is easy to understand.

The next part of the feedback included comments on the policy view screen, where the edit feature is requested.

The company expressed interest in using the artefact internally in some cases. However, they saw the real value in encouraging their clients to use it because of the detailed overview of the different angles of the cybersecurity policy.

The research question is confirmed; the artefact provides value and adds missing cybersecurity knowledge to the SME, to aid in developing a cybersecurity policy.

Appendix 6 – Summary of Interview II

At the beginning of the interview, the interview objective and research question are explained. It is confirmed that the interview is anonymous. All the business-related information will be kept private, and the questions can be left unanswered.

The second interview was performed with a company classified as a medium-sized enterprise representative. The company has seven employees. The interviewee is responsible for sustainable management and operational management, including coordinating IT with different IT partners. The company has implemented extensive numbers of IT solutions, and all of them are subcontracted. The interviewee is responsible for GDPR, but no specific person is appointed to be responsible for cybersecurity. The enterprise has done a cybersecurity audit before. They have not considered using software for managing cybersecurity.

Artefact presentation. It was confirmed that the tool is beneficial and could be used to compile the cybersecurity policy. It is mentioned that if this tool had existed before they ordered the cybersecurity audit, it had provided more valuable knowledge.

Each policy chapter is explained. All the policy chapters that the artefact includes are confirmed. ENISA, Top risks and the different colour headers are confirmed. Showing CERT contact information in the policy is confirmed. Clear policy structure and need for a variety of policy chapters are confirmed. Web interface that uses the survey style approach is confirmed. It is verified that the artefact helps establish baseline security and helps the user understand different attack vectors and risks.

The research question is confirmed; the artefact supports the deficiency of cybersecurity knowledge that regular SMEs might have because it provides a structured cybersecurity policy document.

Appendix 7 – Survey responses

Finding	Description
F1	58,8% of the recipients have never done an information security analysis in the company.
F2	64,7% of the participants answered that they do not have a person in the company who is responsible for cybersecurity.
F3	52,9% of the answerers had mapped their company hardware and software.
F4	64,7% of companies are not using any rules or information security governance frameworks to regulate their information security.
F5	70,6% answered, they need a better solution for managing information security regulations, and 88,2% of them would use a software tool to manage this area.
F6	Regular training was not conducted in 76,5% of the companies.
F7	Software tool should be easy to learn, as 35,3% was willing to spend one hour, 35,3% one working day and 23,5% three hours learning the tool.
F8	Over half 52,9% of the participants do not have procedures for devices used outside the office.
F9	58,8% of the companies are using notebook computers.
F10	Moreover, 64,7% of employees are using their own devices.
F11	Microsoft Windows (35,5%), Android (17,6%) were the most common operating systems used.
F12	Most of the companies (94,1%) are using OS provided security products.
F13	Software artefact must be easy to use.

F14	Simple to compile.
F15	Prepared policy document.