Degree project

A simplified ISMS

Investigating how an ISMS for a smaller organization can be implemented

Master Degree Project in Informatics

Second Cycle 15 credits

Spring term 2021

Student: Agnes Asp Sandin

Supervisor: Sten F Andler

Examiner: Marcus Nohlberg

Acknowledgements

I would like to thank Rose- Mharie Åhlfeldt for her interview participation and her generosity in interesting thoughts, feedback, and her network. I would also like to thank Joakim Kävrestad for all valuable help and finally, I would like to thank my father for his support and encouragement during the whole project.

Abstract

Over the past year, cyber threats have been growing tremendously, which has led to an essential need to strengthen the organization's security. One way of strengthening security is to implement an information security management system (ISMS). Although an ISMS will help improve the information security work within the business, organizations struggle with its implementation, and significantly smaller organizations. That results in smaller organization's information being potentially less protected.

This thesis investigates how an ISMS based on MSB can be simplified to make it suitable for a small organization to implement. This thesis aims to open for further research about how it can be simplified and if it has a value of doing it.

The study is based on a qualitative approach where semi-structured interviews with experts were conducted. This thesis concludes that it is possible to simplify an ISMS based on MSB for a small organization by removing external analysis, information classification, information classification model, continuity management for information assets, and incident management. In addition, the study provides tips on what a small organization should think about before and during implementation.

Keywords: Information security management system, ISMS, Information security, ISO/IEC 27001, Simplify, ISO/IEC 27000, MSB, Method support for systematic information security work.

Table of Contents

1 Introduction 1

2 Background 2

2.1 Information 2

2.2 Threats against information 2

2.3 Information security management system 3

2.4 ISO 27000-family 3

2.5 Method support for systematic information security work 4

3 Problem definition 5

3.1 Motivation 5

3.2 Research question 5

3.3 Target audience 6

3.4 Expected results 6

3.5 Limitation 6

3.6 Related research 6

4 Methodology 8

4.1 Research strategy 8

4.2 Interviews 8

4.2.1 Respondents 8

4.3 Thematic analysis 9

4.4 Ethical considerations 10

4.5 Trustworthiness of the research 10

5 Implementation 12

5.1 Interviews 12

5.2 Thematical analysis 12

6 Result and analysis 15

6.1 Definition of ISMS 15

6.2 Information security management systems 15

6.3 ISO-standards 17

6.4 Summary 18

6.5 Summary of analysis and results 19

7 Conclusion 20

7.1 How can an ISMS based on MSB be simplified to make it suitable for a small organization to implement? 20

7.1.1 A simplified ISMS 20

7.1.2 Tips to consider when implementing a simplified ISMS 21
7.1.3 Positive respondents tend to be more practical than theoretical. 22
8 Discussion 23
8.1 Societal aspects 23
8.2 Ethical aspects 23
8.3 Scientific aspects 23
8.4 Result discussion 24
8.5 Future work 24
References 26
Appendix 1: Interview questions 29

1 Introduction

Information is an essential part of both individuals and organizations. The “revolution” of Information and Communication Technology (ICT), also called digitization, has made the information more available than ever, with that said, also more exposed (Bhaharin, Mokhtar, Sulaiman & Yusof 2019).

According to Shameli-Sendi, Aghababaei-Barzegar & Cheriet (2016), information is a highly valued asset for organizations and must be protected correctly. To be able to protect the information correctly, organizations may require information security. Information security is a broad concept that contains different security measures that are both technical and administrative. ISO/IEC 27000 (2018) defines information security as “preservation of confidentiality, integrity, and availability of information”. To succeed with information security work, it may require a system to manage it, i.e., an Information Security Management System (ISMS). An ISMS is often based on standards; a common standard is the ISO/IEC 27000 family. This standard describes an ISMS as a “systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives” (ISO/IEC 27000, 2018, pp. 11-12).

Most of the conducted research has focused on larger organizations, although Shojaifar, Fricker & Gwerder (2018) describe that the risk for smaller organizations to be exposed is about the same. Several studies have confirmed that small organizations may not have a dedicated budget, infrastructure, skills, or competence, resulting in failing to implement systematic information security work (Bhattacharya, 2015). Cybercriminals are well aware of small organization’s shortcomings which they do not hesitate to exploit (Paulsen, 2016). This thesis will investigate how an Information security management system (ISMS), based on MSB’s method support, can be simplified for smaller organizations. A small organization is defined as an organization with less than 50 total employees (European Commission, 2020).

2 Background

This section presents relevant concepts related to the thesis. The section explains what information is, what kind of threats there are against information, what an information security management system is, what it is built on, and the method support for information security.

2.1 Information

It is difficult to imagine an organization without information. Almost every part of an organization contains information in various forms. It could be salaries, custom information, and e-mails, to mention some. Many tasks an organization performs would be impossible to solve without information and communications technology (Aleksandrova, Vasiliev & Aleksandrov, 2020).

Defining the concept of information may be challenging since it is widely used and has different meanings in different fields (Tsai, 2019). Wang and Hsieh (2014) describe information as collecting statements, opinions, facts, concepts, or ideas between the raw data and knowledge. It can be any processed data and is often obtained through communication, research, teaching, and observation. Another definition is “a message that is delivered from a sender to a receiver through a certain channel” (Bawden & Robinson,2013; Debons, 2008).

However, the definition used in this report is the definition by ISO/IEC (2018). ISO/IEC defines information as an asset that can be stored in many forms, for instance, digital form, paper forms, and knowledge of the employees. In many organizations, information is dependent on information and communications technology. This technology often assists in facilitating the creation, processing, storing, transmitting, protection, and destruction of information. Due to the high value of information in organizations, it can be highly critical (depending on what information) if it is incorrect or not there when needing it (ISO/ IEC, 2018).

2.2 Threats against information

A threat is a set of circumstances that can cause loss or harm in an organization (Pfleeger, Pfleeger & Margulies, 2015). A threat can also be described as anything that can exploit a vulnerability. A vulnerability is a weakness that can be exploited by threats, for instance, to gain unauthorized access to an asset within the organization (Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016).

There are numerous kinds of threats against information. It does not necessarily need to be a cybercriminal trying to attack the information; it could also be environmental threats like floods and earthquakes. Threats can be divided into three different kinds of threats. Deliberate threats cause harm on purpose, for instance, a cybercriminal attacking a particular target organization. On the other hand, accidental threats are someone that by accident threatened the information, for instance, clicking on a malicious link. The last threat is environmental and can, for instance, be a fire or, as mentioned before, a flood that threatens the information (Pfleeger, Pfleeger & Margulies, 2015).

All organizations face information security threats and vulnerabilities. While specific threats are consistent across organizations, some other threats may be specific to a particular industry, location, or business. To know what information an organization needs to protect against threats

and how to protect it may require an information security management system (Paulsen, 2016).

2.3 Information security management system

An information security management system (ISMS) is a systematic approach for working with and achieving information security within an organization. Implementing ISMS can protect information against threats and reduce the risks to acceptable levels (Asosheh, Hajinazari & Khodkari, 2013; Achmadi, Suryanto & Ramli, 2018). Risk in this context is the potential for loss, damage, or destruction of an information asset due to a threat exploiting a vulnerability (Shameli-Sendi, Aghababaei-Barzegar & Cheriet, 2016). Further on, an ISMS strives to maintain confidentiality, integrity, and availability (CIA) of the information. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity is the property of accuracy and completeness. Availability is the property of being accessible and usable upon demand by an authorized entity. Information (Asosheh, Hajinazari & Khodkari, 2013).

ISO/ IEC (2018) describes an ISMS as a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to accomplish business goals. It consists of policies, guidelines, procedures, and related resources and activities. An ISMS shall be based on risk assessment; it is the risk assessment that decides what security controls the assets need to reach acceptable levels of risk.

In order to succeed with information security work, it must constantly be reviewed and improved. By using the Plan-Do-Check-Act (PDCA) cycle, it can be easier obtained. It is an iterative model that constantly strives to improve processes. In ISMS, the first phase (plan) is about establishing an ISMS, the second phase (do) is about implementing and operating the ISMS, the third phase (check) is about monitor and review the ISMS, and the fourth phase (act) is about maintaining and improve the ISMS (Asosheh, Hajinazari & Khodkari, 2013).

An ISMS is often built on standards. There are various best practices in managing information security, but one of the most used standards in this field is ISO 27000- family (Asosheh, Hajinazari & Khodkari, 2013).

2.4 ISO 27000-family

One of ISMS's most used and known standards is the ISO/IEC 27000-family (Asosheh, Hajinazari & Khodkari, 2013). The 27000- family contains different standards regarding information security work. The fundamentals standards of the family are:

• ISO/IEC 27000 Information security management systems — Overview and vocabulary

This standard is an overview and terminology which are used throughout the ISMS family of standards. It also describes the other standards included in the 27000- family (ISO/IEC, 2018).

• ISO/IEC 27001 Information security management systems — Requirements

This standard describes the ISMS and is the one an organization can use for getting a certification. A certification means that an auditor reviews the ISMS work. Reviews the documentation and ensures that the documentation is also being lived and breathed in practice. Certification comes with several benefits; besides structured information security work, it may also be a competitive advantage. Furthermore, this standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving

ISMS (ISO/IEC, 2018).

• ISO/IEC 27002 Code of practice for information security controls. This standard provides guidance on the implementation of information security controls (ISO/IEC, 2018).

• ISO/IEC 27003 Information Security Management Systems – Guidance. This standard provides guidance on how an organization can achieve the requirements in 27001 (ISO/IEC, 2018).

2.5 Method support for systematic information security work

The Swedish Civil Contingencies Agency has developed method support for ISMS. This method is developed to support organizations in conducting systematic information security work. The support is built on the ISO/IEC 27000-family. While the ISO/IEC standards, to a greater extent, describe what to do, MSB's implementation guidelines describe how to do it (MSB, 2018). In addition, MSB describes how an ISMS can be designed and what parts and sub-parts it must include and offers different templates. Below is a figure of the required parts (Analyze, design, use and follow up and improve) and their sub-parts. Notice that this also needs to iterate.

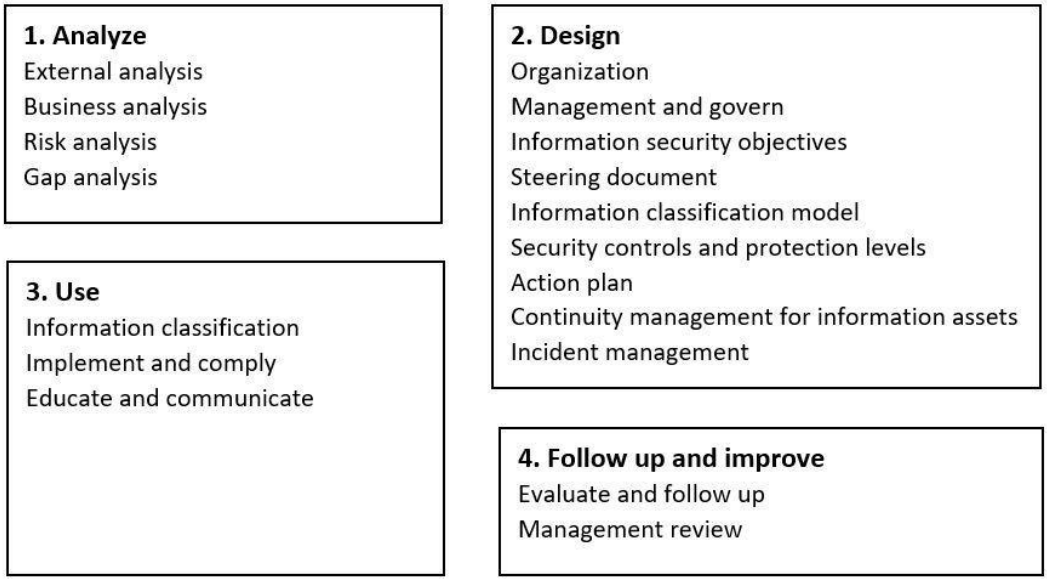

Figure 1. ISMS MSB, authors own based on MSB (MSB, 2016)

3 Problem definition

This section provides insight into the general problem area, motivation, research questions, target group, limitation, and related research.

3.1 Motivation

The averages cost of a data breach in Scandinavia 2020 is over 2.5 million dollars and is expected to increase in 2021 (IBM Security, 2020).

Several studies have confirmed that organizations have a lack of systematic information security work. A study from 2015 conducted by MSB (2016) for systematic information work for municipalities showed a significant lack of working systematically with information security. Eklund & Renner (2020) did a further study on this, and the problem still seems to remain. Municipalities do not necessarily need to be a small organization, but it indicates that this is a complex and challenging area even for larger organizations.

Unlike larger businesses with a dedicated budget, infrastructure, and skills, small organizations often lack those things, resulting in failing to implement systematic information security work (Bhattacharya, 2015). Hall, Sarkani & Mazzuchi (2011) also address this issue of small organizations struggling with implementing an ISMS due to limited resources and motivation. Therefore, small organizations become a significant target for cybercriminals because they are well aware of small organization's shortcomings regarding information security (Paulsen, 2016). Cybercriminals are also using small organizations to "practice" their skills in order to move on to the "big payoff" from attacking larger organizations (Feagin, 2015). Another motive for cybercriminals to attack smaller organizations is that they face fewer legal consequences since they stay" under the radar" because, as said before, small organizations often lack resources, for instance, resources to recognize and investigate cyberattacks (Paulsen, 2016). Even a minor denial-of-service attack or stealing of a single computer's data can sink a small organization. Although there is a strong motivation in this area, the researcher has found the studies conducted about ISMS for smaller or micro-organizations underrepresented. Shojaifar, Fricker & Gwerder (2018) also describe that the risk for smaller organizations exposed to information security threats is about the same as larger organizations. It is also interesting to see that 96% of Sweden's companies are small organizations, making this area even more important (Tillväxtverket, 2021).

Studies conducted in this area have established that companies fail to implement ISMS in larger and smaller organizations and to a greater and lesser extent. Studies have shown that it fails because there is no commitment from management, but even in studies where there is commitment, ISMS fails. This thesis wants to turn the perspective of the most founded articles and investigate whether there is something in the method support that is unnecessary, unclear, or complicated for smaller organizations and can be simplified.

3.2 Research question

The research questions this thesis aim to answer is the following:

1. How can an ISMS based on MSB be simplified to make it suitable for a small organization to implement?

Simplification means that any part/sub-part/process/activity in an ISMS can be removed or made minor than the standard requires. A small organization in this thesis is defined as an organization with less than 50 total employees (European Commission, 2020).

3.3 Target audience

The primary target audience is researchers of the same field, especially researchers who work with developing MSB or developing another implementation guide of ISMS. The second target audiences are management or future CISO's within a small organization that may read the tips regarding implementing an ISMS.

3.4 Expected results

The expected result of this thesis is that it is possible to simplify an ISMS based on MSB. In addition to this, the expected result is to find out how it can be simplified, i.e., which parts can be removed, what is complicated regarding ISMS, what is simple regarding ISMS, which parts are most important, which parts are redundant or not necessary, pitfalls, advice and a list of general security controls for a small organization.

3.5 Limitation

This thesis will be limited to MSB method support for systematic information security work and not any other ISMS tools or implementation guide. It will not examine how to simplify each sub-part of the ISMS and not either later iteration of the PDCA cycle. In addition, this thesis is limited to smaller organizations due to the lack of studies conducted, and that small organization often lack dedicated resources and competence regarding ISMS, which complicate the implementation. A small organization may also not always need or can achieve the highest security level; therefore, this thesis is limited to smaller organizations.

3.6 Related research

Many studies that have been conducted regarding ISMS in a smaller organization are case studies where a non-expert implements an ISMS in a small organization (Crafoord, 2014; Jonsson & Wehrmann, 2015; Brännlund 2019). Alternatively, the studies conducted often focus on how an ISMS can be improved by using ISO- standards or new innovative models to make it more secured (Asosheh, Hajinazari & Khodkari, 2013; Achmadi, Suryanto, & Ramli 2018). Thus, comparing this thesis with most of the studies found can be troublesome. However, there is considered one relevant article by Valdevit, Mayer & Barafort (2009) called "Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings". Valdevit, Mayer & Barafort (2009) has a similar aim and research question. However, they use another research method where they conduct research combined with an experiment in three steps where the aim is to present a complete guideline to facilitate the implementation and the certification of ISMS in SMEs (small and medium-sized enterprises). The article has relevance since it aims a simplifying for smaller organizations built on ISO/IEC 27001, which MSB is based on. However, it differs a bit from this thesis. Valdevit, Mayer & Barafort (2009) have conducted a three-year-long experiment, target SMEs (less than 250 employees), and aim for a tailored guideline that will lead to certification, which this thesis does

not intend to do. Further on is the experiment only conduct in one enterprise and is only verified by local experts. The fact that it is an article from 2009 where the work started in 2007 makes this article over 12 years old, a relatively old article in this constantly changing area (Bhaharin, Mokhtar, Sulaiman & Yusof 2019).

4 Methodology

This section will present the research strategy, collected data, respondents, thematic analysis, ethical considerations, and trustworthiness.

4.1 Research strategy

A qualitative research strategy has been applied in this thesis due to the addressed research question. To be able to answer the research question, individual in-depth interviews were considered needed. Because of the complex area, which studies in the field can support (see section 3), the best method for data collection are interviews with experts with long experience within ISMS. Together these people have over 90 years of experience in the field and are expected to answer the question better than the researcher of this study can do by using some other data collection method, for instance, questionnaires. In order to formulate good answer alternatives to questionnaires, a high level of knowledge and a great understanding of a topic are needed.

Furthermore, questionnaires scratch the surface more than interviews do and are mainly used to test hypotheses that may be useful in a later stage of the research when testing hypotheses (Conboy & Fitzgerald, 2010).

4.2 Interviews

The study has used individual in-depth interviews to answer the question, a commonly used data collection method when conducting qualitative research (Patton, 2015).

Interviews allow the interviewer to have a discussion with the respondent and take part in how they experience reality such as thoughts, positions, knowledge, experience, and stories, which often creates a more profound and greater understanding, which was considered necessary to answer the research question (Conboy & Fitzgerald, 2010). That was why interviews were planned to be conducted. Above all, it was the respondents' experience and expertise that the study wanted to take part in. A strength in conversational interviews is the ability to adapt; it is possible to follow up and investigate further depending on the respondent's answer. The study was conducted after semi-structured interviews, which means a ready-made template with interview questions to follow, but there is room for free discussion and personal follow-up questions depending on what answer the respondent gives (Alvehus 2013). The interviews were planned to take between 40 minutes and 1 hour.

4.2.1 Respondents

To find relevant respondents, expert sampling was used. The sampling technique is a purposive sampling technique where the respondent is selected based on its characteristics. As the name implies, expert sampling calls for experts in the field to be the sampling subjects. It is a positive tool to use when investigating new research areas and checking whether it would be worth conducting further studies on the topic or not (Etikan, 2016). Another approach could have been to aim for a representative sample of the target group but given the size of the target group and the time available for this work, expert sampling was selected because it was assumed to generate more data.

In this case, respondents with expert knowledge in ISMS were selected who have/ working with the 27000 series standard. According to Gobet (2005), an expert has comprehensive or authoritative knowledge in a particular area and has a minimum of ten years of experience within the field.

With the help of a researcher with long experience within ISMS, the respondents were selected. Even if these respondents do not work specifically in small organizations, they were expected to have an incredible amount of knowledge, which was considered to weigh up against someone who works in a small organization and thus be representative but instead without expert knowledge. So, these respondents are not representative of smaller organizations but were selected for good reasons because they have a lot to say about the target group. This research also investigates a new perspective regarding how MSB method support can be simplified, and therefore experts within the field considered the best way of sampling. The respondents are presented in the table below.

Respondents	**Work**	**Experience**	**Interview duration**
Alma	Associate professor of information technology. Educate and research in the field of information security.	21 years	2 hours
Beatrice	Information security consultant and participates in the development of ISO standards (27000- series) as well as holding courses in information security for SIS (Swedish Standards Institute)	8 year	1 hour
Charlie	Information security consultant	16 years	1, 5 hours
David	Mainly consulting within information security and audits for companies, educating CISO's and are also involved in the ISO standardization (27000-series), both nationally and internationally.	20 years	2,5 hours
Elias	Management consultant within information security	25 years	1 hour

Table 1. Respondents

The above names of the respondents are fictitious, "real" names were chosen instead of a letter and a number to make them easier to personify and to make it simpler to keep the respondents apart during the analysis phase.

4.3 Thematic analysis

Thematic analysis is a commonly used analysis tool in qualitative research.

Figure 2. Thematic analysis

It is used to identify, analyze, and describe themes in the collected data. This method is a flexible research tool, which can provide a rich and detailed yet complex account of data without any theoretical framework to be limited to. However, thematical analysis has been criticized due to no explicit agreement about what thematic analysis is and how to do it, which may lead to "everything goes" in a thematical analysis (Braun & Clarke 2006). Braun& Clark (2006) improve this by describing a clear six-phase of doing a thematical analysis. These six phases are: Familiarizing with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report.

Furthermore, the thematical analysis can be done in inductive and deductive. Inductive means that themes are identified during the material analysis, while deductive analysis means that themes have been determined before the analysis begins (Hayes 2000). In practice, it is rare for the researcher to have only an inductive approach because it is challenging to observe reality completely objectively without any preconceived notions and prior knowledge that the researcher possesses (Patel & Davidson, 2003).

4.4 Ethical considerations

To research with high quality, it is necessary to consider the ethical aspects. Therefore, four research requirements should be considered. These Requirements are the information requirement, the consent requirement, the confidentiality requirement, and the confidentiality requirement (Swedish Research Council, 2002).

The *information requirement* means that the researcher must inform all participants and other people involved that the research concerns the purpose of the study. The people involved must be aware that it is voluntary to participate, that they can cancel their participation, what the purpose of the study is, how it will be conducted, and where the study will be published (Swedish Research Council, 2002). In this study, all participants received information about the study, its purpose, and that it will be published in DIVA. Furthermore, it was also announced that the interviews would be recorded due to not missing anything significant and avoiding interruption. The *consent requirement* means that the participant's wishes and conditions must be respected. It may, for example, be the case that they want to suspend their participation or refrain from answering specific questions (Swedish Research Council 2002). Before each interview, all respondents received an email containing the interview questions. During the interview there was one respondent that have not read enough to answer a question and therefore asked to return, this was respected. The *confidentiality requirement* means that personal data or other information linked to those who participate in the research is protected from unauthorized persons (Swedish Research Council 2002). The respondents' names or social security numbers were not included in this study, but each respondent has a fictitious name. Furthermore, the recorded interviews are only available on the researcher's telephone, which no one other than the researcher herself has access to. The *utilization requirement* means that collected material may only be used for research purposes. It may not be used for commercial or other non-scientific purposes. The information collected was only used in this thesis and not for any other purpose (Swedish Research Council, 2002).

4.5 Trustworthiness of the research

When conducting qualitative research, it must be considered how to make the research trustworthy. To achieve trustworthiness there are usually four criteria to consider; credibility,

transferability, dependability, and confirmability (Lincoln & Guba, 1985). In this thesis three of them have been considered.

Credibility is about whether the result is believable or not. In this work, this criterion has been considered by ensuring that the data collected from the interviews have been transcribed and sent to the respondents for a review of the interviews, so nothing has been interpreted in the wrong way. Transferability is about how well the results can be applied in another context, the researcher has tried the best to deliver good and detailed descriptions so that other researchers may assess on their own whether it is transferable to their context or not. The last criterion is conformability which is about the level of confidence that the study's results are based on the participants' words and descriptions rather than the researcher's biases (Lincoln & Guba, 1985). To be aware of the researchers own thought and biases it was written down to keep more easily distinct between the researchers own thought and what the material says. Further the interviews were ending with a confirming question, this question gives the researcher a chance to reduce the risk of interpreting wrong.

5 Implementation

In this section, a presentation is given of how the survey has been carried out based on the selected methods described in chapter 4, Method.

5.1 Interviews

Before the interviews began, the researcher wrote down her bias to reduce the risk of letting biases influence the interview. However, it is difficult to achieve 100% impartiality even if one is aware of it.

The respondents were contacted via email. The first email sent out contained a presentation of the interviewer, what field the interview was planned to cover, and how long the interview was expected to take. If a confirming answer was given, a second email was sent out which contained the interview questions and information about the interview; that it will be recorded, everyone interviewed is anonymous, what the purpose is, and where it will be published. The interviews were conducted digitally, via Zoom or Teams.

First, a pilot study was conducted to get input on the questions and see which work and which did not. After this pilot study, four questions were deleted either because they added no value or overlapped with another question. The interview started by repeating the information within the emails, for instance, that the interview will be recorded and where it will be published. After that, the interview started with some general questions like the respondents working experience so that the respondent would find their feet. The interview questions were asked in the same order as they are presented in the Annex. The researcher conducted five interviews, and these took between 1 hour and 2.5 hours, depending on how many opinions and thoughts the respondent had. After each completed interview, the interview was transcribed verbatim from speech to text, except for pauses, laughter, and information unrelated to the study. The transcribed document was then sent by email to the respondents for approval to use their words and opinions in the study and ensure that the transcription matched what they said. The email that was sent also contained information about if no response is received within a week, it is considered that there are no objections to the material.

The used interview questions can be found in the appendix, where each question's purpose is also presented.

5.2 Thematical analysis

After a confirmation answer or feedback from the respondent regarding the transcribed interview, the researcher changes the feedback and then started to work with the data. The first phase was to get to know the data, reading and re-reading the whole data set, and then focus on special sections that needed more observance. When this was done, the coding process started. The first iteration of coding was done by taking each section of the data set separately, from the first to the last, in relative order. After the first iteration, it was then moved back and forwarded to see if the codes were relevant and extract more codes when the themes developed. When searching for themes, there were several possible themes like the management commitment and classifying but this was rather sub-themes. However, most of the themes were inspired by some of the interview questions. The theme” Higher possibility to succeed with ISMS in small

organizations" was the only theme not inspired by the interview questions. The approach was mainly inductive but with deduction elements since the researcher has some previous knowledge in the area. The themes were then reviewed, and the names defined and checked that it was relevant to the research question. The names of the different themes are:

- Definition of ISMS
- General parts of ISMS that organizations most often fail with
- General parts of ISMS that the organization most often succeed with
- The most important parts of an ISMS based on MSB's different parts (analyze, design, use and follow up and improve)
- Simplifying an ISMS
- ISO-standards
- Advice for a small organization that wants to implement an ISMS
- Is it possible or not possible to simplify an ISMS based on MSB?
- Higher possibility to make a good ISMS in small organizations

Data extract	**Coded for**	**Theme**
I've talked about it before, parallel universes, it will somehow fail in whole or in part because it will not work then, you have to integrated the ISMS into the organization, in the same way as you do when you budgeter, planner or whatever it is, you have to get it into what you work with in a natural way otherwise it will not work. Another variant is if you do not have the management with you, this will fail. If the management is not involved, it's over.	1. ISMS fails if it is in a parallel universe 2. Need to be integrated in the organization 3. Must have management commitment	"Advice for a small organization that wants to implement information security"

Table 2. Thematical analysis

Data extract	**Coded for**	**Theme**
A good overview of the business in a small organization, good level to then be able to work downwards. I think it is important to make the organization understand that you adapt it based on your own needs and the organization, then it will not be so gigantic. You will be able to do a good ISMS work in a smaller organization in a much more efficient way than a larger organization because you have that overview and can see the organizations whole. You will be able to do a good ISMS job in a smaller organization in a much more efficient way than a larger organization because you have, this overview and the whole.	4. Adapt to your organization's own needs. 5. Has an overview and can see the whole in a smaller organization. 6. Introduce a good ISMS in a small organization in a much more efficient way.	"Advice for a small organization that wants to implement information security" and " Higher possibility to make a good ISMS in small organizations"

Table 3. Thematical analysis

The extracted code "4. Adapt to your organization's own needs was placed in the theme" was placed in the theme "Advice for a small organization that wants to implement information security." The other codes "5. Has an overview and can see the whole in a smaller organization"

and “6. Introduce a good ISMS in a small organization in a much more efficient way” were placed in the theme” Higher possibility to make a good ISMS in small organizations.”

6 Result and analysis

This section presents the analysis and results derived from the interviews. The outcomes originate from the answers of Alma, Beatrice, Charlie, David, and Elias. The results are presented in the defined themes and the categories used during the interviews: Definition of Information security management system, Information security management systems, ISO-standards, Summary. Finally, a summary of the analysis and results is also presented. The analysis process will be described in more detail in the first section "6.1 definition of ISMS".

6.1 Definition of ISMS

All respondents answered equally and believe that there is some form of framework to be able to work with information security in a structured and continuous way and emphasized that a management system for information security is not a separate management system but part of the management system that already exists in the organization.

It may indicate that ISMS is an accepted concept among experts. This theme is presented even if it is not exactly linked to the research question but was considered necessary because if the respondents' answers had differed very much, it might have been because they define an ISMS in different ways. That was not the case but shows that there is unambiguity about the subject, which is positive. When extracting the data into this theme, mainly data originates from the two questions "What is an Information security management system for you? and "Why is an Information security management system needed?". Data were also extracted throughout the whole data set; for instance, four of the respondents mentioned during the interview that an ISMS should not be seen as a separate management system but as an integrated system in the overall management system. To distinguish which codes belonged to which respondent, to compare the answers between the respondents, each respondent had a color that represents them. Red belonged to Alma, pink belonged to Beatrice, blue belonged to Charlie, purple belonged to David, and green belonged to Elias. These colors were included throughout the analysis to be able to compare their answers quickly.

6.2 Information security management systems

General parts of ISMS that organizations most often fail with
According to the respondents, the organizations often fail with obtain a current situation, set goals, link information security work to ordinary business goals, management's commitment, classification, to start the practical work, risk analyzes, the person responsible for information security does not reach management, keep steering documents updated, documentation, and to integrate information security work in the business, i.e., almost all parts of an ISMS.

Recurring among the respondents about what organizations mostly fail at were the management's commitment, information classification, and documentation. David explains that classification is an excellent example of how things can go wrong. The classification confuses so much that it can cause the whole work to fail, and therefore want to tone it down or remove it because there is so much misunderstanding, it creates more problems than it solves. Regarding the documentation, a common mistake is too much documentation and documentation that does not correspond to reality. Charlie mentioned it as "paper-tigers," and David mentioned it as several meters as "shelf-heaters" and pointed out that ISMS is not documentation that some

organization believes.

Despite the recurring answers above, the respondents answered very differently, indicating that it is overly complex regardless of the organization's size.

General parts of ISMS that the organization most often succeed in
According to the respondents, the organizations often succeed in appointing a responsible person for the information security work, create some form of documents such as governing documents and business analysis, setting up an organization and security measures that are natural for an IT department or HR departments, such as authorization management and recruitment process. Furthermore, three respondents expressed that organizations have easier to succeed with the process leading up to the practical work, and two of the respondents had difficulty expressing any parts at all organizations succeed with.

It could indicate that the theoretical part of introducing an ISMS is more accessible for an organization to succeed in, but the question is whether the organization has succeeded when they encounter major implementation problems. In addition, there could also indicate that it is a good thing to start with security measures that are "low hanging fruit" for the organization, such as authorization management, since it is easier to succeed with measurements that are close to the already existing processes in an organization.

The most important parts of an ISMS based on MSB method support (analyze, design, use and follow up and improve)
The following result shows a sprawl among which parts are considered most important/ effective. The one thing they agreed on as the most important and effective is risk analysis. Furthermore, Alma described information classification as one of the most effective parts but mentioned that organizations have difficulty with it and mention that small organizations may even skip it. Information classification model and information classification are still stated in the above table because, during the question where she had to pick two sub-parts from every part, she considered them as most important. Furthermore, David struggle with choosing but stated that continuity is essential but may be placed in the second iteration.

It may indicate that it is obscurity regarding ISMS even among experts. The questions could also have been interpreted differently by the respondents and may have more practical or theoretical knowledge in the area. Notice that the result does not necessarily mean that the other parts are not essential but may indicate what parts may be removed or looked further on.

	Analyze	Design	Use	Follow up and improve
Alma	Business analysis, risk analysis,	Information classification model, Security controls and levels of protection	Information classification, Implement and comply	Management review
Beatrice	Gap analysis, risk analysis	Steering document, incident management	Information classification	Management review
Charlie	Business analysis, risk analysis.	Organization, management and govern	Implement and comply, educate, and communicate	Evaluate and follow up
David	Business analysis, risk analysis.	Management and govern, information security objectives	x	X
Elias	Gap analysis, risk analysis	Action plan, incident management	Educate and communicate	Management review, evaluate and follow up

Table 4. Most important parts

Simplifying an ISMS

The following text is a summary of the respondents' answers regarding the simplification of an ISMS. Among the first, get the management's support, it must be clear to what extent and how much time one is expected to spend on this. Call for a meeting with influential people in the organization and conclude the current situation and what information the organization depends on. Do a risk analysis; this does not have to be rocket science or incredibly detailed but rather a high-level discussion where the apparent risks are documented and prioritized. When this is done, there will be a list of prioritized risks. If any apparent technical protection entails a very high risk of being without, fix that first. Once it has been remedied, it is important to continue working in small steps, take the most important measures, and follow up on how it has gone before starting with new measurements. Create a steering document or a policy (for the management to show that they are behind it); it must be created based on the actual work. When the steering document has been produced, assign the responsibility for the various parts, following the line responsibility and creating a plan for the next year. An awareness program in both the short and long term must be developed for everyone in the organization as it takes a long time to change a behavior or a culture. Include training in weekly meetings or e-mails.

In addition to the summary above, several respondents mentioned that the foundation for getting the information security work on-site is to do some form of risk analysis, develop measures, start working and get it out in the organization.

6.3 ISO-standards

All respondents considered that 27001 was most important to use for a small organization. In addition, two of the respondents considered that 27002 was important and agreed that 27000 was important to fully understand 27001.

6.4 Summary

Advice for a small organization that wants to implement an ISMS

The advice collected from the interviews is presented in the table below. Several respondents stress that small organizations need to hire externally experienced people in the first phase of the implementation. It may indicate that it is more or less necessary for small organizations to hire external resources to get started with the implementation.

Alma	**Beatrice**	**Elias**
Set up the different parts in a pedagogical way, teach, bring in good consulting support, train internally, and add security routines into regular routines. Make a risk analysis and start from the risks that exist and look at the costliest risks if they occur, remedy them, and follow up.	Start with the big picture and not get caught up in too many details, such as analyzing a smaller part of the organization and finishing it before moving on to the next. Acquire skills, train someone in the business or hire skills. Notice that, although the organization hires skill, it is still the organization itself responsible for their information security work. When iterating the first time, start with the 10 most critical security measures to reduce the risk of getting too complicated.	Get external help in the first phase of developing the current situation, gap analysis, and action plan; there are the fundamentals for implementing the different security measurements. It is also essential to adapt ISMS to the organization.
Charlie	**David**	
Try to get the management's commitment by presenting what it would cost if a company did not have any security management system. Ask the questions: what information the organization is most critically dependent on, and how long the organizations can be without that information. After answering these two questions, it usually becomes quite natural what the organization needs to address and what does not necessarily need to be addressed.	Appoint a person who wants to work with this; send the employee on training or get some form of support. The support should be as low as possible, though, just to get started with the parts that the organization cannot handle. It is vital to devote time and money to this. An organization with 50 employees, one appointed employee, should spend about 40% of their working time on the ISMS during the introduction, but this amount of time can be reduced afterward. It is essential to keep in mind that a consultant should try to be as effective as possible, which means that this person should not write meaningless documents. Organizations should also do it their way and not slavishly follow templates. It is also vital to integrate the ISMS within the organization; it should not be a parallel universe.	

Table 5. Summary Advice

Is it possible or not possible to simplify an ISMS based on MSB method support?

The following results presented below are a compilation of the respondents' answers throughout the interview. In addition, the last question of the interview was a confirmation question whether they think it is possible to simplify an ISMS or not. All respondents answered following their attitude and opinions throughout the interview except for David. David did not answer an obvious yes to the question but has throughout the interview been highly critical of the classification and considered it should be removed; therefore, the answer is presented as a yes even if he answered both yes and no to the specific interview question. It could depend on

that the questions have been misunderstood, or it becomes something else when one is forced to answer yes or no instead of a question that can be discussed.

Alma	Beatrice	Charlie	David	Elias
Yes, it can definitely be simplified. Some things can be made more fleeting, while some things are good to do in more detail, but it can definitely be simplified.	I do not think the concept as such can be simplified. The method itself is there, but it can be adapted to the organization, and then it does not have to be that complicated. Maybe it would work to simplify by industry, where some parts can be reviewed.	It is absolutely possible. There is so much to do in this area; we are not done. We do not have the answers to everything yet.	Yes, it is possible to simplify by removing the information classification, but in general, the basic parts should be there, and, above all, what has to do with risk because everything in this work shall be based on risk.	Yes, in practice, it is possible to do so. Everything you do is better than do nothing at all. In a small organization, some activities may be unsuitable and thus can be skipped.

Table 6. Possible or not possible simplifying an ISMS

Higher possibility to make a good ISMS in small organizations

Interestingly, several of the respondents also mentioned that the possibility for a small organization to succeed in implementing an effective ISMS is greater than in a large organization because a small organization is less complex. Although the organization still needs to start eating the "elephant," i.e., start working in small pieces rather than try to do all things at once.

This is according to Paulsen (2016) that argues that small organizations that view cybersecurity as part of their business can build a cybersecurity culture much more quickly than most large organizations can. If small organizations embrace cybersecurity, the adaptability advantages a small organization has over large organizations could significantly change the dynamics of the cybersecurity landscape and make small organizations leaders in the field.

6.5 Summary of analysis and results

In addition to the results above, during the analysis phase, it was noticed that the respondents who had a more positive attitude to the simplification of ISMS had to a greater extent practical knowledge. Although this can not be fully ensured, it would need more in-depth questions about their work experiences and further affirmative questions if they consider themselves to have more practical or theoretical knowledge in the field, but it may indicate a connection but can not be generalized by four respondents. However, it can be seen from the information given about four of the respondents' previous work experience that at least three of the respondents have more practical knowledge while at least one respondent has more theoretical knowledge in the area. As mentioned in the introduction, the respondents who had more practical knowledge regarding ISMS were more positive and had more thoughts about which parts should be toned down, redone, or completely removed. In contrast, respondents who had more theoretical knowledge were more pessimistic about a simplification of ISMS and believes that there is no value in simplifying the tool itself, but the simplification lies in adapting the ISMS work to the organization.

7 Conclusion

This section presents the answers to the research question. The conclusions are based on the result and analysis of this thesis.

7.1 How can an ISMS based on MSB be simplified to make it suitable for a small organization to implement?

The results showed that 4 out of 5 respondents considered it possible to simplify an ISMS based on ISO standards for smaller organizations. Therefore, it is most likely possible to simplify an ISMS in one way or another. This is supported by research carried out by Valdevit, Mayer & Barafort (2009) that indicates it possible to simplify an ISMS for smaller organizations.

Based on the results and the analysis, the following conclusions have been drawn regarding how a small organization can implement a simplified version of an ISMS. The conclusion of this question contains both tips to consider when implementing a simplified ISMS and what parts can be removed during implementation.

7.1.1 A simplified ISMS

Based on the results of this thesis, a simplified version of MSB ISMS is proposed below. The interviews showed that several parts might be deleted, either because they have not been mentioned in the interviews as the highest priority during the first iteration or are contra productive. This will be described more below.

External analysis, continuity management for information assets, and incident management have been deleted because none of the respondents considered these parts as the most important to implement during the first iteration of a simplified ISMS. Although the respondents mentioned that even if incident management was not the highest priority during the first iteration and maybe not in the second iteration, it is still an essential and valuable part because it can confirm what needs to be protected against.

Except for the mentioned parts above, the classification and information classification model has been deleted because several respondents have mentioned it as counterproductive, i.e., it confuses rather than benefits and could also fail the entire ISMS implementation. That is supported by a survey conducted by MSB (2014), where the survey shows difficulties with the classification work.

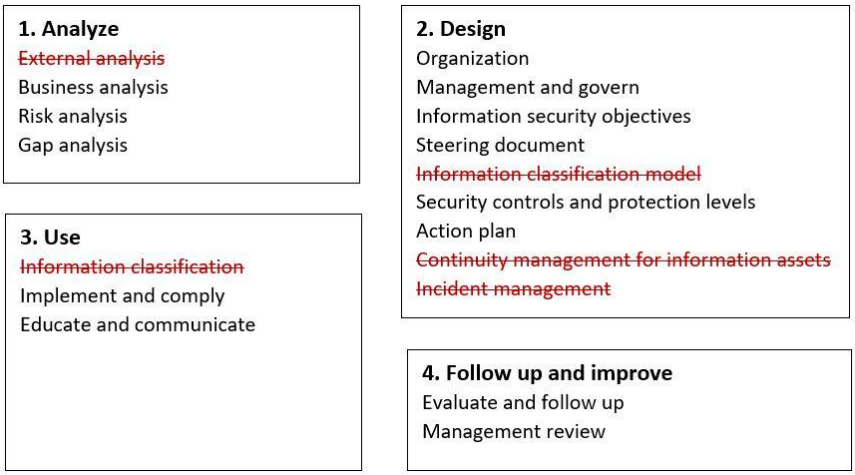

Figure 3. Simplified ISMS, authors own based on MSB (MSB, 2016)

Furthermore, the activities, i.e., the sub-parts within the different parts, can be simplified but have not been investigated in detail in this thesis more than it has been confirmed possible. Thus, the risk analysis does not necessarily have to be conducted according to a specific template that MSB provides but can initially be written down on paper in bullet form to reduce the most obvious risks.

7.1.2 Tips to consider when implementing a simplified ISMS

The following tips are a summary of the respondent's advice when implementing an ISMS.

• An ISMS is not a separate management system; it should be integrated into the management system that already exists in the organization.

• An ISMS is iterative, which means that it does not end and therefore requires perseverance.

• Except for MSB, look at ISO standard 27000 and 27001 to understand what an ISMS is; what parts and processes there are.

• Do not follow the ISO standard or the method support slavishly. Instead, use the understandable parts and the parts the organization sees the benefits of, do not do it just because it says so; an ISMS must be adapted.

• Start with the big picture and not get caught up in too many details, such as analyzing a smaller part of the organization and finishing it before moving on to the next.

• The entire work must be based on the risks since it is the risk the organization shall prevent against.

• Do not document more than necessary. Document if there is a clear purpose and a recipient to read it.

• Do not follow templates slavishly but use what works or get inspiration to create a template or use one that already exists in the organization.

• Think in terms that what is written and planned must also be implemented.

• If a technical security measure entails a high risk of being without remediating that first.

• The management must be involved; otherwise, there is no point in spending time and resources on implementing an ISMS.

• Include the employees. The conducted work must be communicated to the organization, and it should also be explained why it is done.

• Appoint a person responsible for the information security work and let this person attend courses and training. A measure of how much time this person should spend on information security work during implementation is about half of their working time.

• Routines developed should not be specific information security routines but should be routines that are part of the organization's usual routines.

• Get external help during an early stage of the implementation. Notice that a consultant should work to invoice as few hours as possible and include the organization in every step. It is not possible to completely outsource the information security work.

7.1.3 Positive respondents tend to be more practical than theoretical.

The respondents who had more practical knowledge regarding ISMS were more positive and had more thoughts about which parts can be toned down, redone, or completely removed. In contrast, respondents who are more theoretical in the field were more pessimistic about a simplification of ISMS and believe that there is no value in simplifying the tool itself, but the simplification is about adapting the ISMS to the organization. Thus, the attitude of the respondents linked to their experience may indicate a connection but need further research to determine.

8 Discussion

This section will present societal, ethical, and scientific aspects, result discussion, and future work.

8.1 Societal aspects

The cyberattacks increase, and organizations become more and more digitalized, resulting in more vulnerability when everything in an organization relies on the internet and different systems to handle their daily work.

The government has almost refused organizations to be digitalized, and therefore should also be responsible for handling its consequences more than they do (MSB, 2019). Conduct more research and provides clear and understandable guidelines for a smaller organization that also works in practice. Because if smaller organizations succeed with implementing an ISMS, there will also be a reduction in successful attacks and information loss, thus benefit society since small organizations constitute a major part of Sweden's society (Tillväxtverket, 2021).

8.2 Ethical aspects

This thesis has chosen not to interview people who work in small organizations about their experience on the subject because, despite anonymity, there is a risk that they still would not have felt safe and willing to be completely open because it can be challenging to talk about their own problems. Therefore, an ethical stance has been made by collecting data from elsewhere. Although it is a rather undramatic area and the respondents of this study have answered based on their expert knowledge, the research ethics aspects have been considered by all respondents remaining anonymous, and their words are not used for any purpose other than this thesis. In a larger context, most of the research is carried out and aimed at larger companies, which is an ethical issue when a major part of the organizations in society and thus the data in society are handled by small organizations that have difficulty complying with the standards and supports that exist because they are too extensive and complex.

8.3 Scientific aspects

The scientific contribution is that this thesis opens up for further research of how it can be simplified and if it has any value in doing it. Because, just because it can be simplified, it may not provide any value in doing so. It also shows that small organizations have different situations and conditions than large organizations and may need to be handled more as a separate group.

Valdevit, Mayer & Barafort (2009) conclude that it is possible to simplify an ISMS by downsizing the requirements of ISO/IEC 27001 to reduce the cost and complexity of an ISMS. They have conduct research combine with an experiment in three steps where the results are a finished guideline. It could be challenging to compare the results since this thesis is not a finished guideline but more similar to the first step of their conducted studies, but unfortunately, the data collected and issues found in their first step were not described in the article.

8.4 Result discussion

The study can be considered credible as there have been no consciously inaccuracies or cheats during the study, and in addition, a thematical analysis has been used as an analysis tool. The recordings were carefully listened to and then transcribed word for word by the researcher and sent to the respondents to confirm that nothing has been transcribed or interpreted wrong. In addition, the material was examined and interpreted with as objective an eye as possible so that the researcher's own opinion would not take over and influence the result. Furthermore, since it is translated to English from Swedish, it has been carefully checked that nothing is missed.

Although the things above have been considered, many things can still affect the results. The questions may have been misunderstood differently. For example, the question about which parts are the most important and gives the most effective are two different perspectives in the same question. Some respondents may think about the most effective parts, and some may have thought about what parts are most important. Afterward, that question would be turned into either two questions or remove one perspective to make it more straightforward. The result may have been negatively affected by this because respondents may have answered either one or the other, making it difficult to compare. One other question presented in the results that may affect the results is a question where the respondents were prompted to choose two parts or activities, but this can be weird because numerous activities are strongly tied together and cannot be removed or added without others.

It can also be questioned whether simplifying is the right word to use, but since this word was used throughout the study, it was not considered possible to change because the entire thesis is based on this word. Instead of simplifying, perhaps adaptation or tailored would be a more appropriate word.

The expected results were also to provide general security controls that small organizations may implement. However, it turned out that it was not possible to select general security measures for small organizations, partly because they are related to each other and partly because it was a very scattered result among the respondents.

8.5 Future work

This thesis shows that it is possible to simplify an ISMS based on MSB and broadly how to do it. However, more research is needed on how the different sub-parts, for instance, business analysis, can be simplified. It is particularly important research to conduct in order to complete a potential simplifying version of ISMS. When a simplified version is completed, it would be necessary to implement it and evaluate it if it has value.

It would be interesting to carry out further studies on how an ISMS based on MSB can be simplified by comparing opinions between experts who have worked more practically and more theoretical experts, as this could not be ensured in this study. If it turns out that there is a value of making a simplification and that most experts with practical knowledge believe it is possible to make simplifications, practical experts should be more involved as they may have more experience of doing it. Since theoretically, it can work perfectly, but in practice, it can look different; therefore, both perspectives should be more involved in developing a simplified ISMS for smaller organizations. In addition to experts, future research would also be carried out on a

more representative group such as chief information security officers (CISO) in smaller organizations to see their practical knowledge of simplifying ISMS.

Interesting research or improvement that can be done in the area is not precisely about simplifying ISMS but about adapting it to the organization. Several respondents mentioned that ISMS needs to be adapted to the organization, but what does that exactly mean? Will small organizations without any previous experience be able to determine what their adaptation should look like and successfully adapt it to their organization? Perhaps research can be carried out on how small organizations should proceed when adapting ISMS to the organization, maybe with the help of guidelines or develop different techniques that help them decide the adaption.

References

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. 2018 International Workshop on Big Data and Information Security, IWBIS 2018, 149–157. https://doi.org/10.1109/IWBIS.2018.8471700

Aleksandrova, S. V., Vasiliev, V. A., & Aleksandrov, M. N. (2020). Problems of implementing information security management systems. Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020, 78–81. https://doi.org/10.1109/ITQMIS51053.2020.9322896.

Alvehus, J (2013). Skriva uppsats med kvalitativ metod: En handbok. Stockholm: Liber

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. International Journal of Information Science and Management, 11(SPL.ISS.), 111–126.

Bawden, D., & Robinson, L. (2013). Introduction to information science. Chicago, IL:Neal-Schuman.

Bhattacharya, D. (2015). Evolution of cybersecurity issues in small businesses. RIIT 2015 - Proceedings of the 4th Annual ACM Conference on Research in Information Technology, 11. https://doi.org/10.1145/2808062.2808063

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brännlund, J. (2019). Standardisering av informationssäkerhet. Luleå tekniska universitet Institutionen för system- och rymdteknik.

Conboy, K., & Fitzgerald, B. (2010). Method and developer characteristics for effective agile method tailoring: A study of XP expert opinion. ACM Transactions on Software Engineering and Methodology (TOSEM), 20(1), 2.

Crafoord, M & Sahlin, H. (2014). Ett anpassat ledningssystem för informationssäkerhet - Hur gör en liten organisation med hög personalomsättning? Uppsala universitet: Uppsala.

Debons, A. (2008). Information science 101. Lanham, MD: Scarecrow press.

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

European Comission. (2020) User Guide to the SME Definition. https://doi.org/10.2873/677467

Feagin,R- D. (2015). The value of cybersecurity in small business. Angewandte Chemie International Edition, 6(11), 951–952. Published by ProQuest LLC (2015).

Gobet, F. (2005). Chunking Models of Expertise: Implications for Education. Applied Cognitive Psychology, 19(2), 183-204. doi:10.1002/acp.1110.

Hall, J. H., Sarkani, S. & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. Information Management & Computer Security, Vol. 19 No. 3, pp. 155-176. https://doi.org/10.1108/09685221111153546

Hayes, N. (2000). Doing psychological research : Gathering and analysing data. Buckingham:

Open University Press.

IBM Security. (2020). Cost of a Data Breach Report 2020. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

International Organization for Standardization (ISO) (2018). ISO/IEC 27000:2018(E). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Switzerland: ISO.

Jonsson, P., & Wehrmann, A. (2015). Informationssäkerhet i små och medelstora företag. Linnéuniversitetet: Kalmar.

Lincoln, Y., & Guba, E. (1985). NATURALISTIC INQUIRY. London: SAGE Publications

Myndigheten för samhällsskydd och beredskap (MSB). (2019). Comprehensive cyber security action plan 2019–2022 Sweden. Retrieved from https://rib.msb.se/filer/pdf/28898.pdf

Myndigheten för samhällsskydd och beredskap (MSB). (2016). Informationssäkerheten i Sveriges kommuner Analys och rekommendationer utifrån MSB:s kommunenkät 2015. https://rib.msb.se/filer/pdf/28222.pdf

Myndigheten för samhällsskydd och beredskap (MSB). (2018). Method support for information security management systems (ISMS). The Swedish Civil Contingencies Agency (MSB). Available at: http://www.informationsakerhet.se/metodstodet

Patel, R. & Davidsson, B. (2003). Forskningsmetodikens grunder att planera, genomföra och rapportera en undersökning. Tredje upplagan. Lund: Studentlitteratur.

Paulsen, C & Toth, P. (2016). Small Business Information Security: The Fundamentals. https://doi.org/10.6028/NIST.IR.7621r1

Pfleeger, C.P, Pfleeger, S.L. & Margulies, J. (2015). Security in computing. (5. ed.) UpperSaddle River, N.J.: Prentice Hall.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14-30. https://doi.org/10.1016/j.cose.2015.11.001

Shojaifar, A., Fricker, S. & Gwerder, M . (2018). Elicitation of SME requirements for cybersecurity solutions by studying adherence to recommendations. http://ceurws.org/Vol-2075/PT_paper_4.pdf [Accessed 2021-01-29]

Swedish Standards Institute (SIS) (2017). S-EN ISO/IEC 27001:2017. Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2013 med Cor 1:2014 and Cor 2:2015). Stockholm: SIS.

Tillvaxtverket.se (2021). Basfakta om företag. https://tillvaxtverket.se/statistik/foretagande/basfakta-om-foretag.html [accessed 2021-01-31]

Valdevit, T., Mayer, N & Barafort, B. (2009). Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings.

Vetenskapsrådet (2002). Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning. Stockholm: Vetenskapsrådet.

Webster, J., & Watson, R. T. (2002). Webster and Watson literature review. MIS Quarterly, 26(2), 11.

Whitman, M., & Mattord, H. (2016). Management of Information Security. Boston: Cengage Learning.

Appendix 1: Interview questions

General questions

- What do you work with?
- How long have you worked in the security industry?

  The purpose of these questions is to investigate how experienced the respondent is in the area, if they are more practical or theoretical and for the respondent to begin to find his/her feet.

Definition of Information security management system

- What is an Information security management system for you?
- Which parts of an Information security management system are mostly needed?
- Why is an Information security management system needed?

  The purpose of these questions is to find out what a management system for information security is. According to Niemimaa (2017), the concept can have different meanings depending on perspective. Therefore, the researcher considered it important to start by asking these questions to see what the respondent's definition is, which can be decisive for how the outcome will be for the rest of the interview.

Information security management systems

- In your experience, which parts of ISMS do organizations most often fail at? What do you think it depends on?

  The purpose of this question is to find out what is difficult by nature, or an indication of something that can / should be simplified.

- Do you have any idea how to simplify these parts?

  The purpose is to find out from the previous question whether it is difficult by nature or whether it would be possible to make a simplification.

- What parts of ISMS does the organization most often succeed in? What do you think it depends on?

  The purpose of this question is to find out what is easy in nature, or what the standard has managed to convey.

- If you can choose 2-3 parts in each step of the ISMS process (see below, analyze, design, use, follow up) which parts do you think are the most important and give the most effect for information security for a small organization? Why?

  The purpose of this question is that by choosing, the respondent is forced to think about which parts cannot be left out in an ISMS, i.e, which parts are most important. The purpose is also that the other parts that the respondent has not chosen, may be superfluous in some cases. These parts are taken from the Swedish Civil Contingencies Agency [MSB] (2018), which is a methodological support based on ISO standards.

- Do you think that it is possible / impossible to simplify these different parts? For example, in external analysis some things may be simplified /removed but the risk analysis may not be possible to reduce, and so on.

The purpose of this question is to investigate whether the respondent believes that it is possible to simplify the various parts, that the parts remain but that certain subparts in them may be simplified or removed.

The following parts are taken from MSB (2018).

Analyze
External analysis
Business analysis
Risk analysis
Gap analysis

Design
Organization
Management and govern
Information security objectives
Steering document
Information classification model
Security controls and levels of protection
Action plan
Continuity management for information assets
Incident management

Use
Information classification
Implement and comply
Educate and communicate

Follow up and improve
Evaluate and follow up
Management review

- If you were given the task of simplifying an ISMS (minimum protection), how would you set it up?

  The purpose of this question is the same as the previous question i.e. investigate whether it is possible to simplify an ISMS, but the idea is that it should open up for more discussion about, for example, which parts are most necessary.

ISO-standards

- Which ISO 27000 standard (s) do you think are most important for a small organization to use?

  The purpose of this question is to examine which standard (s) the respondent considers to be the most important to use when it comes to the introduction of an ISMS.

- If you are going to choose 15 security measures / controls to implement from the ISO standard 27001 (Appendix A, attached document) in a small organization, which ones do you choose? And why do you choose them?

The purpose of this question is that by choosing, the respondent is forced to think about which parts cannot be, that is, which safety measures are most important.

The most important success factors

- What are the most critical success factors in implementation for a small organization?

  The purpose of this question is to find out what an organization needs to be extra observant about in order to succeed with an ISMS.

- How do you get the management involved in a small organization do you think? Is it different from a larger organization?

  The purpose of this question is to find out if the respondents have any ideas / personal experience in how to best get the management involved, this is because the literature addresses the management's commitment as a critical success factor (International Organization for Standardization [ISO], 2018).

- What is the best way to communicate an ISMS for a small organization in practice?

  The purpose of this question is to find out if the respondents have any ideas / personal experience in how to best communicate an ISMS, this because the literature addresses the management's commitment as a critical success factor (SIS, 2018).

Summary

- What would your advice be for a small organization that wants to improve / implement information security work with a limited competence / budget?

  The purpose is to find out what advice the respondent would give to an organization that wants to implement an ISMS.

- Do you consider it possible or not possible to simplify an ISMS?

  The purpose of the question is to get a reinforced picture of previous questions and thus ascertain what their positions are regarding whether it is possible or not possible to simplify an ISMS.