
A comprehensive qualitative exploration of the difficulties and facilitators encountered by organizations in the implementation and maintenance of an Information Security Management System (ISMS)

Lukas Grenefalk & Christopher Norén Wallin

Department of Computer and Systems Sciences

Degree project 30 HE credits
Computer and Systems Sciences
Degree project at the master level
Spring term 2023
Supervisor: Stefan Axelsson
Abstract

This research aims to investigate the challenges and success factors associated with the implementation and maintenance of Information Security Management Systems (ISMS) in organizations. Despite the increasing importance of information security in today's digital age, research shows that organizations continue to struggle with effectively implementing ISMS and maintaining it up to date. The study will explore the various cultural, strategic, tactical, and operational factors that affect the performance of organizational ISMS. The research will provide insight into the challenges and factors contributing to a successful ISMS implementation and maintenance, filling a gap in the existing literature. In this study, the qualitative survey method was utilized as the research strategy, complemented by semi-structured interviews for data collection. A total of 11 interviews were held with Senior Information Security professionals who have experience in implementing and maintaining Information Security Management Systems. Thematic analysis was then employed to analyze the data from the interviews. The study identified 15 themes related to challenges and success factors within implementation and maintenance of ISMS. Four themes related to implementation challenges, four relating to implementation success factors, three to maintenance challenges and four to maintenance success factors. The themes are Misconceptions of Security, Lack of Top Management Support, Resistance to Change, ISMS Design, Communication, Internal Security Culture, Top Management Support, ISMS Design, Resource Constraints, Continuous Administration, Employee Attitudes, Relationships, Ownership, Accessibility and Compliance.

Keywords: ISMS, Information Security Management Systems, challenges, success factors, implementation, maintenance
Synopsis

Background
Information security threats have become a major concern for organizations as they have become increasingly dependent on information systems in their business operations. Cybercrime has become a lucrative business for criminals and as a result, organizations are implementing information security management systems (ISMS) to reduce the risk of security-related incidents and comply with regulatory requirements.

Problem
Despite the increasing importance of information security, organizations struggle with effective implementation of ISMS and there is a lack of understanding of a range of factors affecting its performance. The study aims to fill the gap in existing literature by exploring both the implementation and maintenance challenges and success factors of ISMS.

Research Questions

● What are the challenges of implementing an ISMS?
● What are the factors contributing to a successful implementation of an ISMS?
● What are the challenges of maintaining an ISMS?
● What are the factors contributing to a successful maintenance of an ISMS?

Method
This study used a qualitative research approach. The research strategy was qualitative surveys with semi-structured interviews as the data collection method. The qualitative surveys provided in-depth knowledge into the multiple factors influencing the success and challenges of ISMS implementation and maintenance. The interviews were one-to-one and conducted with experienced professionals with a minimum of 5 years of experience in information security management. The data was analyzed using thematic analysis.

Result
The semi-structured interviews were analyzed using thematic analysis. Results found 15 themes related to challenges and success factors during ISMS Implementation and Maintenance. Four themes related to implementation challenges, four relating to implementation success factors, three to maintenance challenges and four to maintenance success factors.

Discussion
The study found that the primary ISMS implementation challenges were Misconceptions of Security, Lack of Top Management Support, Resistance to Change and ISMS Design. The Themes related to Implementation Success Factors were Communication, Internal Security Culture, Top Management Support, and ISMS Design. Factors relating to Maintenance challenges were Resource Constraints, Continuous Administration, and Employee Attitudes. Themes relating to Maintenance Success factors were Relationships, Ownership, Accessibility, and Compliance.
Acknowledgement

We would like to thank our supervisor Stefan Axelsson for the support and guidance throughout the thesis. We would also like to express our gratitude to all respondents who participated in our interviews for this study.
# Table of Contents

1 Introduction  
1.1 Background 1  
1.2 Research problem 2  
1.3 Research question 2  
1.4 Target audience 2  

2 Extended Background  
2.1 Information Security Management 3  
2.2 ISO/IEC 27001 - Information Security Management System 3  
2.3 Previous research 4  

3 Methodology  
3.1 Research Strategy 6  
3.2 Alternative Research Strategy 6  
3.2.1 Experiment 6  
3.2.2 Phenomenology 7  
3.3 Data Collection 7  
3.4 Alternative Data Collection Method 7  
3.4.1 Questionnaire 7  
3.4.2 Focus group 8  
3.5 Application of method 8  
3.5.1 Interviews 8  
3.5.2 Sampling 9  
3.6 Data Analysis 9  
3.7 Ethical considerations 10  

4 Result  
4.1 Thematic analysis 12  
4.2 ISMS Implementation 13  
4.2.1 Implementation challenges 13  
4.2.2 Implementation success factors 16  
4.3 ISMS Maintenance 17  
4.3.1 Maintenance challenges 17  
4.3.2 Maintenance success factors 19  

5 Discussion  
5.1 Discussion of results 22  
5.2 Limitations 25  
5.3 Ethical and social aspects 26  
5.4 Validity & reliability 26  
5.5 Future research 27  

6 Conclusion 28  
References 29  
Appendix A – Consent Form 32  
Appendix B – Interview Questions 33
| Appendix C – Participants                     | 34 |
| Appendix D – Reflection Document 1           | 35 |
| Appendix E – Reflection Document 2           | 37 |
List of Tables

Table 1: Security controls .......................... 4
Table 2: Phases of Thematic analysis (Braun & Clarke, 2006) .... 10
Table 3: Thematic analysis ......................... 13
List of Abbreviations

COBIT - Control Objective for Information and Related Technology Standards
CISO - Chief Information Security Officer
DORA - Digital Operational Resilience Act
GDPR - General Data Protection Regulation
ISM - Information Security Management
ISMS - Information Security Management System
ISO - International Organization for Standardization
KPI - Key Performance Indicators
NIST - National Institute of Standards and Technology
PCI DSS - Payment Card Industry Data Security Standard
SOC2 - Service Organizational Control (2)
1 Introduction

1.1 Background

Information security threats have become a major risk to organizations as they have become increasingly dependent on information systems in their business operations (Singh et al, 2014). At the same time, cybercrime has become a lucrative business for criminals and was estimated to cost the global economy approximately 1 trillion USD in 2020 (Cremer et al, 2022). As a result, regulators are introducing new legislations such as DORA, NIS2, and GDPR which are forcing organizations to enhance their information security and protection of customer data. To address this issue, organizations implement information security management systems (ISMS) to reduce the risk of security-related incidents and to comply with customer and regulatory requirements. This in turn has resulted in dramatically increasing security expenditure in organization and is estimated to cost organizations 188,3 billion USD by 2023 (Gartner, 2022).

Previously efforts to prevent security-related threats were primarily technological (Singh et al, 2014). In current days it is well known that the majority of data breaches are a result of human elements (Stewart & Jurjens, 2017; Constantino et al, 2018; IBM, 2020; ENISA, 2022; Basset et al, 2022). Therefore, using only technological measures is not sufficient to provide a secure organization, instead, you need a balance between technological and non-technological measures (Kayworth & Whitten, 2012; Singh et al, 2014). The understanding and importance of utilizing people-centered and organizational measures to prevent information security incidents have been elevated as a result (Werlinger, 2009; Stewart & Jurjens, 2017). However, some organizations still tend to focus on the technological aspects of security, which leaves them vulnerable to non-technological information security threats (Choobineh et al, 2007, Hasim & Razali, 2019).

To help organizations efficiently manage and balance their information security efforts, international standards have been developed. The most well-known standard is the International Standard ISO/IEC 27001. The standard includes guidelines and best practices for building an information security management system (ISMS) (Stewart & Jurjens, 2017; Aleksandrova et al, 2020).

The idea is that if organizations are implementing the guidelines and controls of the standard effectively, the overall security of the organization will increase. However, the implementation and maintenance of an ISMS can become a complex and expensive process for organizations, which can result in organizations not implementing and maintaining enough security controls (De Lange et al, 2016; Velasco et al, 2018). Organizations also tend to implement too many controls due to their lack of knowledge of their effectiveness, creating additional deficiencies in their systems (Baker & Wallace, 2007). Furthermore, Zammani & Razali (2016) identified that organizations tend to fail in implementing an ISMS because they are unaware of the factors contributing to a successful implementation. This shows the complexity of balancing the number of efforts and controls put into place in organizations in order to produce an efficient information security management system.
1.2 Research problem

The objective of this research is to examine the challenges and success factors associated with the implementation of Information Security Management Systems (ISMS) in organizations. Furthermore, the study aims to explore post-implementation challenges and success factors related to maintenance and the present tense. Despite the increasing importance of information security in today's digital age, studies have shown that organizations continue to struggle with effectively implementing ISMS (Werlinger, 2009; Zammani et al, 2019). Yet, there is still a lack of understanding of the various cultural, strategic, tactical, and operational factors and their effect on performance factors of organizational ISMS (Singh et al, 2014; Topa & Karyda, 2019). Furthermore, most studies focus on the implementation phase of the ISMS but not the challenges and success factors of maintenance, leaving the topic relatively unexplored (Sharma & Dash, 2012; Singh, 2014; Zammani et al; 2019; Hasim & Razali, 2019). Also, most studies are a few years old, and their results may not fully reflect the current state of the field. Investigating not only the challenges of ISMS implementation but also providing insight into the maintenance of ISMS will thereby fill a gap in the existing literature and provide new knowledge about ISMS implementation and maintenance.

1.3 Research question

The following research questions have been formulated:

- What are the challenges of implementing an ISMS?
- What are the factors contributing to a successful implementation of an ISMS?
- What are the challenges of maintaining an ISMS?
- What are the factors contributing to a successful maintenance of an ISMS?

1.4 Target audience

As this study aims to understand the challenges and success factors of ISMS implementation and maintenance, the target audience consists mainly of security professionals and organizations. This could for example be information security consultants working with ISMS implementation, private organizations, and governmental organizations such as municipalities.
2 Extended Background

This section presents and analyzes prior research in the subject area as well as describes the concept of information security management. The aim of the research background is to deepen the understanding of the field and reinforce the problem statement and research question.

2.1 Information Security Management

Information security is, according to the National Institute of Standard and Technology (NIST, n.d.), defined as “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.” Information Security Management (ISM) is the process where you manage the work with information security. There are frameworks and standards for best practices that include sets of policies, procedures, and technologies that are designed to safeguard information assets and ensure their confidentiality, integrity, and availability. ISM is the overall process of protecting information, while an information security management system (ISMS) is a specific framework that processes and ensures that all necessary controls are in place. In other words, ISMS could be seen as the systematic approach for handling ISM.

According to Aleksandrova et al (2020), the most known standard for best practices in information security management (ISM) is the ISO 27001 standard which is described in-depth in section 2.2. Other common ISMSs are NIST 800-53, COBIT, SOC 2, and PCI DSS. While they all provide a framework and best practices for information security management, they are each targeted toward different industries, sectors, and use cases. ISO 27001 is a more widely adopted standard for ISMS, NIST 800-53 is focused on Federal agencies and contractors but can be used by other actors, COBIT provides a holistic approach to IT governance and management, SOC 2 is focused on service organizations and PCI DSS is focused on protecting sensitive credit card information (Lainhart IV et al, 2016; Grispos, 2019; Korkkinen, 2021)

2.2 ISO/IEC 27001 - Information Security Management System

ISO/IEC 27001:2022 is the latest ISO 27001-series provided by the International Organization for Standardization (ISO) and replaces the previous 2013 standard. The standard specifies “requirements for establishing, implementing, maintaining, and continually improving information security management systems within the context of the organization” (ISO, 2022, p.5). The purpose of the standard is to ensure the confidentiality, integrity, and availability of an organization’s information through implementing policies, procedures, guidelines, and technological implementations. The information security management system can be seen as the policies, procedures, and guidelines implemented, monitored, and maintained within the organization.

The ISO 27001:2022 standard can be divided into two different parts namely the mandatory requirements & required documents and the security controls. The mandatory requirements & documents are to be found in sections 4 to 10 in the standard covering areas such as understanding the organization’s context, leadership, planning, support, operation, performance evaluation, and
improvement. The security controls can be found in the Annex A in the standard and are divided into four sections namely, organizational, people, physical and technological controls. The two largest categories of security controls are the technological and organizational measures covering for example access control, password policies, firewalls, network security, legal requirements, secure configuration etcetera. The other two control groups cover the physical and people controls which include background checking, information security awareness, protecting cables, protecting office sites etcetera.

As previously mentioned, information security was previously very focused on technological measures to protect against security threats (Singh et al, 2013). However, as seen in table 1, the ISO standard balances technological and non-technical measures to ensure an effective and balanced information security management system. The implementation of the security controls should be used in the context of clause 6.1.3 Risk treatment (ISO, 2022). This means in practice that the controls are not mandatory to implement, but if choosing not to implement some control it should be justified in a Statement of Applicability in order to claim conformity with the standard. In other words, in order to comply with the standard, the required documents from sections 4 to 10 must be implemented and maintained together with the justified security controls.

<table>
<thead>
<tr>
<th>Control type</th>
<th>Number of Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational</td>
<td>37</td>
</tr>
<tr>
<td>People</td>
<td>8</td>
</tr>
<tr>
<td>Physical</td>
<td>14</td>
</tr>
<tr>
<td>Technological</td>
<td>34</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>93</strong></td>
</tr>
</tbody>
</table>

*Table 1: Security controls*

### 2.3 Previous research

There are multiple studies investigating the topic of information security management. Singh et al (2014) identified factors of organizations' information security management (ISM) and issues through a literature review. The study identified ten factors of importance when managing information security including top management support, Information security policy, information security training, information security awareness training, Information security audit, adherence to best practices, asset management, regulation compliance, incident management, and information security culture. Most of which are elements within the ISO 27001 standard. Zammani et al (2019) investigated critical success factors during ISM implementation using surveys. The study identified forty-five items and fourteen factors contributing to the successful implementation of ISM, including top management support, Information security coordination team, information security management team, resource planning etcetera (ibid). Similar results were found by Hasim & Razali (2019) through a literature review where the authors identified 12 success factors. The results are not unexpected considering the articles of Singh et al (2014) and Zammani et al (2019) were included in the review. Werlinger et al (2009) analyzed the challenges of IT security management. Results showed that the greatest challenges identified were primarily of the organizational nature e.g., lack of budget, low priority of security, access control, and top management support. Human and technological challenges were also identified including the complexity of systems, vulnerabilities, lack of training, culture, and communication.
Topa & Karyda (2019) conducted a gap analysis on the contents of ISO 27001-27005 to provide guidelines to security managers. Results showed that factors concerning security behavior like top management participation, embracing cultural context, encouraging employees to comply, cost of compliance etcetera are barely considered within the standards which could critically affect the effectiveness of the ISM (ibid). Hu et al (2012) identified that organizational culture defines security behavior, and that top management support can have a positive effect on the security culture within the organization. Lowry & Moody (2014) identified that Information Security Policy compliance is harder to reach if stakeholders believe their freedom is at stake, which may pose a challenge to organizations. Stewart & Jurgens (2017) investigated ISM and the human aspects in organizations. The findings indicate that proper adherence to security compliance can effectively prevent data breaches within an organization and that certain variables can direct employees to compliance. The variables identified were knowledge sharing, socialization, work experience, skilled leadership management, and intervention (ibid).

The findings of Sharma & Dash (2012) suggest that implementing ISO 27001 can demand a lot of time and resources and that companies should have an implementation plan early in the compliance process to enhance compliance efforts. Their study recommends identifying business objectives as a first step in implementing ISO 27001. Business objectives can be derived from the company's mission, strategic plan, and existing IT goals. The biggest challenges in implementing ISO 27001 are the time and resources that it requires, especially if companies don't have an implementation plan early in the compliance process. To overcome these challenges, Sharma & Dash (2012) suggest that internal auditors can help identify primary business objectives and implementation scope and work with IT departments to determine current compliance maturity levels and analyze the compliance process' return on investment. Using experienced staff members or external consultants can also be helpful in implementing the standard.

In summary, several studies have explored the factors and challenges involved in information security management. Key elements of successful ISM include top management support, clear policies, training programs, regular audits, adherence to best practices, asset management, and compliance with regulations. Critical success factors in ISM implementation include a dedicated security team, proper resource planning, and strong leadership. ISO 27001-27005 standards are widely used in ISM, but a gap analysis has shown that factors related to security behavior are not adequately addressed. Human factors, such as knowledge sharing and proper leadership, also play a role in successful ISM and in preventing data breaches. Finally, implementing ISO 27001 can be resource-intensive, but having a clear implementation plan and using internal or external experts can help overcome these challenges. However, previous research has a knowledge gap when it comes to understanding the success factors and challenges in maintaining the information security management system (ISMS) after implementation. There is a lack of understanding about how to keep the ISMS up to date and functioning effectively. Additionally, several studies are a few years old, and their conclusions may not accurately reflect the current state of information security in organizations, given the ever-evolving nature of the field.
3 Methodology

In this chapter the methodological choices of the study are presented and discussed together with the ethical considerations.

3.1 Research Strategy

This study employed a qualitative research approach with a focus on understanding the challenges and success factors for Information Security Management System (ISMS) implementation and maintenance. The research strategy used in this study was a survey followed by semi-structured interviews as the data collection method. Due to the need for depth rather than breadth in this study, the quantitative survey strategy was considered unsuitable for the intended objective of acquiring comprehensive insights into the implementation and maintenance of ISMS. Instead, qualitative surveys through interviews were considered most suitable. Using qualitative surveys had several benefits, including the ability to ask follow-up questions for more depth and immediate responses compared to quantitative methods. It also allowed the respondents to provide unique answers instead of being limited to a set of predetermined responses (Denscombe, 2014). The negatives of using the qualitative approach compared to the quantitative approach is that it is relatively labor intensive as it requires active participation of the researchers in the interviews (ibid). However, it was determined through a pilot study that the level of labor intensity was manageable and not a concern. In summary, the survey research strategy was able to provide sufficient depth and detail that is necessary to understand the challenges and success factors of implementing ISMS.

3.2 Alternative Research Strategy

This section examines alternative research methods that could have been applied to this study. However, as explained below these methods were deemed not suitable for this specific study.

3.2.1 Experiment

For this study, conducting an experiment could provide clear-cut results, however it is not a feasible research strategy due to ethical, practical, and legal constraints associated with this study’s research objective. Especially in practical terms since implementing ISMS might occur over a long period of time, which makes the experiment research strategy highly infeasible. In particular, experiments are supposed to replicate real-life situations where behavior or decisions would be made (Denscombe, 2014). Creating real-life situations of ISMS related work can be complicated and too time-consuming and thus not applicable considering the time restrictions of this study. However, experiment as an alternative research strategy could be feasible if it is limited to one or a few certain components of ISMS, in other words if it is connected to specific variables. An example could be developing a security awareness training program or a risk assessment tool, in other words specific components of ISMS content. The experiment could be conducted over a specific period of time, which probably would be longer than an average interview, which makes this research strategy infeasible considering the scope of time for this study.
3.2.2 Phenomenology

Another alternative research strategy that was considered is phenomenology. In this study, phenomenology could have been used to e.g., understand how information security professionals experience operating an ISMS within an organization. In this context, it could have analyzed the feelings and perceptions of their work and produced in-depth knowledge about their human experience, but less focused on the measures to overcome ISMS implementation challenges. That itself could be useful if the purpose were to understand information security workers' everyday life experience but less useful in the context of gaining an understanding of practical measures in operation. As a result, phenomenology was discarded as the research method due to its focus on understanding feelings and perceptions rather than understanding specific practical measures.

3.3 Data Collection

The most appropriate data collection method for this study was one-to-one semi-structured interviews. The method where selected based on the need to gain an in-depth understanding of ISMS implementation and maintenance. Firstly, the interviews provided in-depth knowledge and insights into people's emotions, opinions, experiences, and feelings (Denscombe, 2014). All these factors were crucial to understanding the challenges and success factors involved in implementing and maintaining an ISMS. Interviews allowed for follow-up on unclear answers compared to static questionnaires. The semi-structured format provided flexibility for the interviewer in discussing topics without a specific order. Furthermore, semi-structured interviews allowed the interviewee to speak more freely and develop ideas on the questions asked during the session which provided the depth to understand ISMS implementation and maintenance (ibid). The interviews were conducted one-to-one through Teams, meaning with one participant and the researchers. The benefit of the one-to-one interviews is that it was relatively easy to control compared to group interviews as only one person is interviewed. Furthermore, in the interviews, there was one person being interviewed which made the data easier to transcribe and the data relatively straightforward as it only came from one source (Denscombe, 2014).

3.4 Alternative Data Collection Method

Following section includes alternative data collection methods in order to demonstrate the rigor of our research, increase the reliability of the findings, and provide transparency and understanding of the research process. It illustrates the breadth of the research and the extent to which we considered different approaches for collecting data.

3.4.1 Questionnaire

One alternative data collection method that was considered was a questionnaire. A questionnaire would have allowed for the collection of quantitative data on ISMS implementation Challenges and success factors, which would have provided a broad overview of the participants' experiences, perceptions, and opinions. However, it was decided that a questionnaire would not be as appropriate as semi-structured interviews in this case, as it would not allow for the same level of depth and detail in the participants' responses and would not allow for follow-up questions or exploration of additional topics that may arise during the interviews. In general, questionnaires are better when you need breadth, as previously mentioned, but this study needs more depth than breadth, which makes questionnaires unideal (Randolph, 2008).
This research aims to examine the difficulties and facilitators of ISMS implementation, which necessitates more comprehensive responses as opposed to brief and frequent responses for high response rates typically associated with questionnaires (Denscombe, 2014).

3.4.2 Focus group

Other than questionnaires, focus groups were contemplated as an alternative data collection method. A focus group would have allowed for the collection of both quantitative and qualitative data in our study and would have made it possible for group discussion and interaction among the participants. Nonetheless, it was decided that a focus group would not be as appropriate as semi-structured interviews in this case, as it would not make possible for the same level of individualization and personalization in the participants' responses and may not be as effective in exploring the challenges and success factors of ISMS implementation in-depth. There are also other disadvantages with using focus groups such as difficulties in analyzing data as a large amount of data can be generated very quickly which can lead to increased time consumption in transcribing recordings, lack of control over proceedings, and respondents speaking at the same time (Bryman, 2012).

3.5 Application of method

This part will cover the execution of our chosen methodology for collecting data. The practical steps of how the research was conducted in terms of sampling and interviewing is discussed.

3.5.1 Interviews

As previously mentioned, semi-structured interviews were selected as the data collection method for this study. The interview questions are categorized under two topics. One topic is connected to ISMS implementation and the other one connected to maintenance of the ISMS, see Appendix B. The questions within each topic are designed to allow for free interpretation, facilitating spontaneous discussions and encouraging natural follow-up questions. The total number of predetermined questions is only 9, hence it is presumed to ask at least the same amount of follow up questions. Furthermore, the interview questions are semi-structured because they are open-ended, which allows the participants to be flexible which opens up for nuanced responses. It is also semi-structured in terms of allowing deviations from original questions if the respondent has partially answered the next question in a previous one. Lastly, the semi-structured interview method allowed for a greater participant engagement, as participants felt that they could speak freely and openly about their experiences. This approach created a comfortable interview environment which felt more natural and dynamic, compared to using a structured interview approach with a bigger frequency of predetermined questions. Therefore, applying semi-structured interviews in this context may have helped to elicit more in-depth and meaningful responses with more valuable insights that might have had no chance to occur in a stricter interview environment.

The interview questions were formulated based on the research questions and the identified gap in literature that highlighted a lack of understanding of the various cultural, strategic, tactical and operational factors and their effect on performance factors of organizational ISMS. The questions were intentionally crafted to thoroughly investigate these factors, as they are directly relevant to the research questions of this study. In order to test the interview questions a pilot study was conducted. The pilot study was conducted on an experienced security professional working with ISMS implementation and maintenance for over 20 years. The purpose of the pilot study was to test whether the selected research strategy, data collection method and interview questions would be able to provide the knowledge
required to answer the research questions. After the interview was finished the subject had time to give input into the interview questions and share their thoughts and opinions on whether the questions were feasible or not. The information provided from the pilot study was used to improve the interview questions and estimate the required time and resources required to conduct the study. Furthermore, it also confirmed that the selected research strategy and data collection method was suitable for the purpose of this study.

A total of 11 interviews were conducted until data saturation had been reached. The interviews were held and recorded via Teams in both English and Swedish and were ongoing for approximately 40-60 minutes per interview. The interview recordings were then transcribed through the transcription tool Avrio, and then exported into Word-documents for thematic analysis.

### 3.5.2 Sampling

In general, a qualitative survey involves gathering insights from a limited number of individuals within a specific population (Denscombe, 2014). In this study the selected population was senior information security professionals working with implementing and maintaining ISMS. Due to the prevalence of security professionals across various organizations, there was no single organization that could be approached to acquire knowledge required for this study. Instead, each security professional that was of interest for being interviewed had to be contacted individually. To identify potential security professionals that could be of interest for this study a purposive sampling technique was used, meaning that the interview subjects were selected on the basis of their experience and relevance (Denscombe, 2014).

The participants were primarily identified on the social media platform LinkedIn. To identify the subjects some keywords were used in the search engine on LinkedIn such as Chief Information Security Officer (CISO), Senior Information Security Officer, Senior Information Security Consultant. Potential interview subjects' profiles were then analyzed to see whether they have relevant knowledge and experience within ISMS implementation and maintenance. When multiple information security professionals had been identified the initial contact was made by sending a message on the platform presenting the researchers, information about the study, and information about the interview. If the subject was willing to participate in an interview, further information was sent including a consent-form together with the interview questions that were expected to be asked during the interview, see Appendix A. The goal was to reach a maximum of 12 participants in order to draw generalizable conclusions. A total of 21 Security professionals were contacted based on their experience, of which 11 participated in the interview. Most of the people that did not participate gave no answer at all whereas a few referred to lack of time.

### 3.6 Data Analysis

The data collected from the interviews were analyzed using thematic analysis. Thematic analysis is a technique used to identify, examine, and report on patterns, or themes, within a data set (Braun & Clarke, 2006). This is a common approach in qualitative data analysis and one strategy could be to create an index of central themes and subthemes and then insert them into a matrix where all the data can be organized (Bryman, 2012).

Themes are often built on codes that have been identified in for example transcripts, as in our case, and provide the researcher with a basis for understanding the data and making a theoretical contribution to the literature related to the ISMS implementation examination. It's important to note
that the themes are not pre-determined, and they emerge from the data as we as researchers go through the process of identifying and analyzing the codes (ibid.).

The process of thematic analysis involved transcribing the interviews, reading the transcripts, identifying codes, grouping codes into themes, and then refining the themes to produce a final set of themes that represented the data (Bryman, 2012). The process suggested by Braun & Clarke (2006) was used in this study, see table 3.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description of the process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Familiarizing yourself with your data:</td>
<td>Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.</td>
</tr>
<tr>
<td>2. Generating initial codes:</td>
<td>Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.</td>
</tr>
<tr>
<td>3. Searching for themes:</td>
<td>Collating codes into potential themes, gathering all data relevant to each potential theme.</td>
</tr>
<tr>
<td>4. Reviewing themes:</td>
<td>Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic ‘map’ of the analysis.</td>
</tr>
<tr>
<td>5. Defining and naming themes:</td>
<td>Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.</td>
</tr>
<tr>
<td>6. Producing the report:</td>
<td>The final opportunity for analysis. Selection of vivid, compelling extract examples, final selection of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.</td>
</tr>
</tbody>
</table>

Table 2: Phases of Thematic analysis (Braun & Clarke, 2006)

In other words, the thematic analysis process starts with data collection, which is the semi-structured interviews in our case, then we read through the transcripts from the interviews in order to identify relevant codes. After identifying relevant codes, we group the codes into themes and then finally interpret the themes in relation to the research questions.

Worth mentioning is that thematic analysis has historically been an underdeveloped data analysis method because there are such few clear specifications for its contents, steps, and best practice (Bryman, 2012). However, thematic analysis is being developed more and more over the years as more researchers provide detailed explanations of their way of doing it, such as Ryan and Bernard (2003) and Braun and Clarke (2006) (ibid.).

### 3.7 Ethical considerations

When conducting a study that involves people, multiple ethical considerations must be considered. According to the Ethics Review Act, certain research must go through an ethical review for the research to be allowed to be conducted. In this study, it was decided that no ethical review must be conducted by the ethical review authority as this study will not collect any data specified in the regulation (Swedish Research Council, 2017). However, even though it does not require an ethical review, ethics must still be considered throughout the research.

The Swedish research council (2002) has stated four ethical principles that were taken into consideration during the research process namely the information requirement, consent requirement, confidentiality requirement, and use requirement. To fulfil the information and consent requirement, the participants were informed of the purpose of the study and their rights as participants through a consent form that was provided before the interviews. The consent form was distributed to the participants through email, see appendix A. To ensure that the participants fully understood the purpose of the research, the research's intent was re-explained during the interview, along with information about their right to end the interview at any time and revoke their consent.
To fulfil the confidentiality requirement all information about the participants is kept confidential and stored in a secure manner. Furthermore, no information regarding the participants is included within the document to provide anonymity, instead the participants are referred to as CISO X or Senior Consultant X depending on their occupation. Finally, in order to fulfil the use requirement, the data that is being collected will only be used for research purposes and not distributed to any third party. The use of the data is therefore only limited to the scope of this study.
4 Result

This chapter presents the findings of the thematic analysis that was conducted on the data collected from the semi-structured interviews, as well as the analysis. It provides a comprehensive overview of the key themes and patterns that emerged from the data collected.

4.1 Thematic analysis

A thematic analysis has been conducted on the data obtained from the interview transcripts, which has resulted in the identification of various emergent themes which have been derived from codes. The identified themes have been further classified and linked to upper-level codes and categories, to facilitate a comprehensive understanding of the data. Upper-level code is a higher-order theme that captures broader concepts that have emerged from the collected data to facilitate the narrative of seeing key findings. It could be referred to superordinate codes or global codes that provide a clear understanding for the overarching meaning. Since the interviews were held in both Swedish and English there have been translations into English of the quotes stated under each theme that comes from the respondents. The findings have been presented in tabular form below for clarity and ease of reference. The table does not prioritize the themes based on their importance, rather, it presents them as having equal significance. Within the implementation processes two themes, namely Top Management Support and ISMS design were identified as both a challenge and a success factor and will therefore be discussed together in section 4.2.

<table>
<thead>
<tr>
<th>Categories</th>
<th>Themes</th>
<th>Upper-level codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Challenges</td>
<td>Misconceptions of Security</td>
<td>Lack of Knowledge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of Experience</td>
</tr>
<tr>
<td></td>
<td>Lack of Top Management Support</td>
<td>Organizational Barriers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resource Constraints</td>
</tr>
<tr>
<td></td>
<td>Resistance to Change</td>
<td>Top Down</td>
</tr>
<tr>
<td></td>
<td>ISMS Design</td>
<td>Accountability &amp; Responsibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Change Management</td>
</tr>
<tr>
<td>Implementation Success</td>
<td>Communication</td>
<td>Policies, Procedures &amp; Guidelines</td>
</tr>
<tr>
<td>Factors</td>
<td></td>
<td>Complex Documentations</td>
</tr>
<tr>
<td></td>
<td>Internal Security Culture</td>
<td>Insufficient Analysis</td>
</tr>
<tr>
<td></td>
<td>Top Management Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12
<table>
<thead>
<tr>
<th>Maintenance Challenges</th>
<th>Resource Constraints</th>
<th>Prioritization and Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Continuous administration</td>
<td>Communication and Advocacy</td>
</tr>
<tr>
<td></td>
<td>Employee Attitudes</td>
<td>Documentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ownership</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organizational Culture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perceptions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compliance &amp; Complacency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integration</td>
</tr>
<tr>
<td>Maintenance Success Factors</td>
<td>Relationships</td>
<td>Communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Education &amp; Awareness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organizational Understanding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visibility</td>
</tr>
<tr>
<td></td>
<td>Ownership</td>
<td>Leadership</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self-awareness</td>
</tr>
<tr>
<td></td>
<td>Accessibility</td>
<td>Incentives</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>Simplicity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reviewing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auditing</td>
</tr>
</tbody>
</table>

*Table 3: Thematic analysis*

### 4.2 ISMS Implementation

#### 4.2.1 Implementation challenges

**Misconception of Security**

Nine respondents agreed that a common challenge within the ISMS implementation phase is misconceptions of what information security and Information Security Management Systems really is. It appears that one of the main reasons for this is the general lack of knowledge and experience in practice about the subject. It has been identified that a common perception of information security is that it only is a technical issue rather than a strategic one. People within organizations assume that information security only concerns IT security departments and that they will handle all aspects of information security, but it really permeates in most departments. In other words, there is a misconception that it is solely the responsibility of the IT department, rather than involving processes throughout the whole organization. Another example regarding the experience deficiency is that consultants can be theoretical experts but lack practical knowledge when it comes to the actual implementation, which already appeared on the first interview by CISO A:
“...because it's written by people that have never done the donkey work, as I call it. The farmer's work. They've never worked in the field. They've seen fields, they know what a field should look like, but they've never actually picked up the shovel and done anything. So, if you haven't done that, you'll build something that's not implementable at all.”

Additionally, there may be difficulties in making people understand the weight and benefits of information security, and employees may not recognize its importance. Top management may not fully understand the scope and importance of what they have ordered, and there may be a lack of commitment to information security overall. There can be a desire for full commitment from a bottom-up perspective, but top management only sees increased costs that brings no revenue. CISO E highlights this as a big challenge:

“...that information security becomes a cost when working with it. We cannot show any profit. However, we can demonstrate that what we do reduces the risks that can lead to losses...”

Another misconception about the cost perspective is that management has unrealistic expectations, such as if a one-time investment in security technology will provide complete protection for the organization's information assets.

Moreover, some organizations only consider implementing an ISMS because their customers or partners require it. In these cases, the focus is on compliance with regulations or contractual obligations, rather than on the intrinsic value of a solid and long-term information security work.

**Top Management Support**

Ten of the participants responded that lack of top management support is one of the major challenges and one of the reasons why ISMS implementations are unsuccessful. Lack of Top management support in this context is often explained as: the organization not providing sufficient resources, lack of motivation from senior management, the security personnel not given mandate to make changes, lack of communication with senior management, and security being seen as an unnecessary cost.

Most respondents believed that the lack of top management support was related to misconceptions of what an ISMS is, but also lack of motivation. Often it is implemented because of requirements from customers or recommendations from auditors but with no actual intent of making the organization more secure. Senior consultant C explained that:

“The motivation of the senior management is really the main factor which then leads to the other contributing causes which are lack of resources and lack of communication within the organization. If the management does not radiate a commitment to the information security work, then the rest of the organization will not adopt it in a good way”.

This in turn often results in the organization implementing and communicating the ISMS from a bottom-up approach instead of top down, which several participants believed caused problems in terms of getting support from employees and departments within the organization, as they do not see it as something requested from the management team. Senior consultant C continuous:

“Some stakeholders will get more work. They will need to make their processes more comprehensive. They may need to learn new things. if they do not see the benefit of an ISMS. Then they won't be so motivated. Especially if they feel that it is not a priority for management. So why is it a priority for me?”

The majority of respondents also identified lack of resources and prioritization as a major consequence of lack of top management support. This was often described in a context where the security
professionals want to implement controls to certain parts of the businesses but are met with resistance due to lack of resources. CISO C explained that:

“If you can’t show your boss that this money, it doesn’t bring production increase or new features or faster streamlined production but it’s just security. Then it is difficult to get up the motivation and get priority. Especially if you don’t have a very supportive top management.”

On the other hand, having Top management support was deemed as one of the most important factors for a successful ISMS implementation. The reason for this is that the organization gets the adequate resources needed to establish a robust security framework, which in turn facilitates the smooth implementation of security measures throughout the organization, without encountering any significant opposition. CISO explains:

“Really, you need a quite powerful voice coming from the CEO just to regularly remind people this needs to be done and achieve it. Having the stakeholder know that they’re getting the executive support is key.

Four participants explicitly suggested that having the Chief Information Security Officer (CISO) within the top management or within the executive leadership will make the implementation process easier as it brings security to the agenda and makes the senior management and the board aware of information security. This in turn leads to less resistance from the management team. Senior consultant D:

“In those situations where the information security manager is part of the management team, they have the opportunity to influence. so, then you don’t get as much resistance from the management team.”

Resistance to change

Another central theme identified from codes related to rather cultural aspects and organizational factors is the resistance to change. Implementing a new ISMS requires employees to some extent change the way they work and the way they think. It is a question of change management. Nine of the respondents have highlighted that it is a significant challenge.

Employees may fear changes, both as they may see it as an increase in their duties or workload and fear of the unknown. Additionally, the respondents have lifted a perception of “you can’t teach an old dog new tricks” kind of mindset amongst the employees, which makes it difficult to get people to adopt new processes and behaviors.

“...one must be clear in saying that an information security management system is not a system support. It is a way of working in a safe way and thus takes integrating information security and technical controls into their existing work processes. But there, you must also remember that there are process owners. There are people who work in the processes, who are used to working in a certain way. There is usually quite a lot of resistance from them because they either don’t see the value in the change or it affects them that they have to change their ways of working”.

This quote from senior consultant D is about adopting new behaviors but also making people accountable and responsible, which is a significant challenge, as it may require changes in job roles, responsibilities, and expectations which then again comes back to the resistance of changing and the fear of taking on increased responsibilities.

CISO E refers to something she calls the change curve or the psychological acceptance curve as a way of seeing the challenge of employees’ resistance to change. This model highlights the emotional stages individuals go through when facing changes and transitions. Humans are by nature against a change at
first when you present it, since implementing ISMS is a change of routines. She says this is a big challenge which needs to be addressed when implementing the ISMS. You will get counter questions similar to “why should I do something different; I have always worked this way, and nothing has happened?”.

**ISMS design**

A common main challenge identified by eight participants during the ISMS implementation process was rooted in the ISMS design. But if done correctly it was seen as a contributing factor to a successful implementation. A lacking ISMS design was believed to involve insufficient analysis on the controls that are selected, meaning that the controls are not relevant, sufficient or not implementable in the organizational context. In order to have a solid design, a solid groundwork during the control selection must be done. CISO C explains:

“The first challenge is to have the skills and time to do solid groundwork in the selection of controls. There it is also about involving the right people within the business. You have to have a business connection when you do that, as I see it. You can't just sit in your corner as a security professional and think this should be implemented. You have to connect the business.”

Having badly written security policies, procedures and guidelines was another critical challenge that eight of the participants had experienced. In this context it is primarily documentation written using a language that was too security specific e.g., using security buzzwords, but also documentation that was vague and not specific in the requirements. This may lead to frustration among those responsible for implementing certain controls, as they don’t understand what should be done. CISO A explains:

“...lots of words in it, but where's the bit that says, you need to dig a hole and it has to be this deep and it has to be this wide. It's too fluffy. It's not precise enough. So that's the biggest challenge on implementation, is badly written policies and badly written standards.”

Lastly, another major factor leading to challenges were complex documentation, meaning having an overwhelming amount of documentation used within the implementation process. This in turn makes it confusing for the stakeholders to adapt the requirements from the ISMS. Therefore, to avoid challenges arising from poorly designed ISMS, the controls must align with business context and requirements, use straightforward language in documentation, and avoid excessive documentation to prevent unnecessary complexity.

### 4.2.2 Implementation success factors

**Communication**

When asking the respondents about what factors they think are crucial for the success of ISMS implementation all participants mentioned communication related factors. One of the main findings was the importance of speaking the language of employees and avoiding technical buzzwords that can be confusing and alienating. Incorporating the language of business and avoiding jargon can aid in conveying the significance of security measures to the intended audience, thus encouraging their active participation and cooperation. It is also essential to make people understand the benefits of implementing an ISMS and the potential risks to the organization's reputation and costs in case of errors.

It is also crucial to inform and make employees agree to the policies, highlighting the strategic point of view compared to the technical aspects. The benefits of being ISO certified should be communicated effectively, and existing communication channels should be utilized to reach all employees, instead of finding new ways to reach the employees:
“...but it is rare that people search for perhaps completely new channels solely because of security information or training or something like that. So you have to understand, like, your setting and then use the channels that are already there.” - Senior Consultant C

Furthermore, communicating and showing successful work for other departments can be an effective way to convince employees of the benefits of implementing an ISMS.

Getting to know employees and their work can help in tailoring the communication to their specific needs and concerns. Taking separate meetings with the most resistant people can also be an effective strategy to address their concerns and persuade them to support the implementation of an ISMS:

“...which is usually separate meetings with those people. It is a first lecture where you really just try to explain not project specific stuff but like just just the value of this and try to describe the value at all levels of the business and how people would possibly be affected.” - Senior Consultant D

Overall, effective communication is crucial for implementing an ISMS, and organizations should pay attention to the communication strategies used to ensure successful implementation.

**Internal Security Culture**

Another crucial topic that was brought up by all participants in terms of the success of ISMS implementation is the internal security culture. Several codes related to education and awareness programs that can foster a strong security culture were identified.

Education programs, delivered through repetition, are crucial for instilling a strong security culture in employees. It is also important to highlight the difference between cybersecurity and IS/ISMS and to make top management and board members understand the importance of security. Explaining the risks on an individual level and highlighting the purpose and background of the ISMS is helpful.

Using top management as an example in information security training and educating the organization about ISMS can be effective ways to promote a strong security culture:

“Then we have an annual training for all employees, including where you take an exam. And we do that by first having our management team take the test and then I tell them all what average score the results had.” - CISO F

Conducting eLearnings and internal education can be effective ways to foster a strong security culture and make employees understand the weight and importance of the ISMS. For organizations operating within regulated industries, the existing culture of working with risk and compliance can make it easier to implement an ISMS. This is particularly true for banks and governmental actors who are often ahead of non-regulated organizations in this regard:

“If you look at the Police, the Armed Forces. They have completely different motives. They must have them (ISMS) in place. The banking sector also needs it differently. A private company however that is not subject to such heavy regulation, they can see it as wanting to do the least possible for it...” - Senior Consultant A

**4.3 ISMS Maintenance**

**4.3.1 Maintenance challenges**

**Resource Constraints**
Resource constraints were identified as one of the major challenges during maintenance of the ISMS by nine of the participants. Resources are often a result of the previously identified theme “top management support”. Lack of resources during the maintenance of the ISMS often involved insufficient resources for monitoring such as no security tooling to keep track of vulnerabilities, no resources for auditing, and lack of personnel to maintain the ISMS. Most of the participants agreed that security budgets are often not sufficient in order to maintain the ISMS. CISO E explains:

“Resources are never plentiful when working with information security. You struggle and there is not enough.”

Security is in this context not prioritized and can rather be seen as a burden. Especially the middle or lower management can get frustrated as they gain additional workload with an already restricted budget. As a consequence, they find it challenging to concentrate on their primary task, creating a conflict of interest within the organization. CISO E explains:

“The least interest is when you get down to the lowest management levels and budget responsibility where you actually see costs associated with security. But they are hard pressed to keep their budget and hard pressed to carry out business development projects or keeping operational projects alive. And then security comes as an extra charge.”

Continuous administration

One of the most prominent themes identified early on was about how important it is to set up an implementable ISMS from the beginning. Seven respondents said that without a solid foundation, maintaining the ISMS would be impossible. Therefore, a central challenge is to ensure that the ISMS is designed in the right way in accordance with the organization’s specific needs and constraints.

Another key theme identified was the challenge of making the processes for updating the ISMS. The participants highlighted the importance of developing concise procedures in terms of maintenance activities to ensure that the ISMS is constantly up to date. Followed by making the processes clear, respondents mentioned the documentation as a challenge, which highlights the need for an effective document management process to enable all necessary records are maintained and easily accessible.

Understanding that the ISMS has a dynamic nature was also noted as a challenge. Three respondents said that ongoing changes in the environment around the organization are ever changing and that regulatory and technological aspects might require ongoing adjustments to maintain an effective ISMS.

“A management system is not static, it is dynamic and constantly changing in relation to the outside world, in relation to the organization. You have to work a lot with monitoring your processes and developing them.” - Senior Consultant C

Three respondents discussed about cultural security aspects such as how maintaining momentum and interest in the system can be a challenge. This highlights the need to ensure ongoing support and engagement from leadership and other stakeholders, but also balancing operational and strategic work when maintaining the ISMS. This points at the need for effective planning and prioritization to guarantee that maintenance tasks do not conflict with other organizational priorities.

Employee Attitudes

The human factors and employee attitudes related to maintaining an ISMS were a crucial aspect by six of the participants, making this the last and final major theme under maintenance challenges.

One of the main challenges identified was the obstinacy of people to follow the controls. The interviewees mentioned that employees may resist following the established controls, making it
difficult to maintain the full potential of the ISMS. Complacency was also mentioned, stating that employees may become complacent over time and fail to follow procedures, which can compromise the security of the system.

Another central aspect recognized was the issue of organizations implementing ISMS for the looks only, rather than to improve their security posture. They noted that some organizations may work with an ISMS only to appear compliant, rather than to ensure that their systems are secure.

“...information security is not huge either. Our business will not die if we do not have information security. But our customers demand it so we have to have it.” - CISO E

Some interviewees also said that some employees may view security as an extra layer, rather than an integral part of all processes. Therefore, it is a challenge to make sure that employees understand the importance of information security and its relevance to their daily work in order to integrate it to existing processes and making people see the bigger picture.

“And what you do a lot of times is you implement information security management systems alongside existing management systems because you think it will be too complex to integrate them. Then you suddenly have two parallel processes on almost everything. And it's kind of stupid. Because one of these processes will get stuck.” - Senior Consultant C

4.3.2 Maintenance success factors

Relationships

In the theme of maintenance success factors seven of the respondents pointed out that relationships with involved stakeholders is a key factor. Hosting forums and stakeholder councils was mentioned as a useful tool to discuss security matters and helping stakeholders who have questions or concerns.

“I think that an important thing is that, to the extent necessary, if there are no existing forums, that you create forums for coordination where CISO and the key stakeholders that you need to be in contact with actually have a coordination forum, a risk council or what it can now be.” - Senior Consultant C

Being visible in the organization was also noted as important, as it helps to create a sense of trust and transparency. CISO A suggested that it is important to make it clear to employees who the security people are and that they are there to help, not police.

Encouraging employees to identify their own areas of improvement was also brought up by the interviewees. Participants suggested that this can be achieved by making it easy to understand the importance of information security and providing ongoing education programs to employees.

“...giving people access statistics to show how they're performing against the KPIs, um, but also trying to encourage them to identify their own areas of improvement” - CISO D

Adapting communication to the subject matter by understanding the business and regional context and needs, as well as the organizational culture, was also seen as critical. Policies and guidelines should be adapted to the subject matter.

“...to really adapt. Listen to your colleagues, understand where you are about it. If you are in China, there will be extremely many or different threats and risks than if it is in the West.” - CISO G

Ownership

Ownership was deemed as one of the most important factors for a successful maintenance of an ISMS by six of the participants. In this context, ownership primarily refers to clearly defining responsibilities
and assigning accountability to individuals for specific actions. Assigning responsibilities and accountability will facilitate control implementation and compliance monitoring, as dedicated personnel can be followed up on for control implementation and adherence. For the maintenance to be efficient, the ownership structure needs to be defined during the implementation process. CISO C explains:

“To begin with, you have to build a structure of people, stakeholders, individuals who are responsible for the ISMS implementation. And you can then use those people to ask questions. You can send out a number of controls, vice versa, and ask them Do you have it in place? What is the status of this?”

Having a well-defined ownership structure also reduces the load on security personnel, as they may be placed in situations where they are perceived as solely responsible and accountable for all security aspects within the organization. This is according to most participants an ideal situation if wanting to have a successful maintenance of an ISMS as security personnel cannot be solely responsible nor accountable for security.

"It is important that there are dedicated responsibilities for security, that you bring it out in projects and point out which people should do what. If it doesn't exist, it's very easy for it to just stop and nothing happens, and then it becomes something where there's a security manager sitting there who has to try to run everything at the same time."

Accessibility

In order to maintain an ISMS effectively, seven of the participants deemed accessibility to be a critical factor. In this context accessibility meant primarily two things, making documentation and compliance metrics visible to the stakeholders. Firstly, ensuring the accessibility of documentation means making it easy to find, such as placing it on an intranet homepage where stakeholders are actively working. This can greatly facilitate the maintenance of the ISMS. CISO F explains:

“It must be collected together (documentation). So we have worked a lot in recent years on simplifying the management system itself so that it should be more easily accessible and that the parts that concern people should be able to find them easily on the intranet.”

Secondly, making compliance metrics accessible in this context means that the control compliance metrics (e.g. dedicated KPI: s) and vulnerabilities should be visible to the accountable and responsible people within the organization and not hiding them within certain documents or unknown systems. CISO D explains:

“It's hard to get people to go and start looking around in other systems, which they're not familiar with on a monthly basis. So what the lesson we've learned there is taking that data out of those systems, putting them into something which they're looking at on a regular basis.”

Instead, respondents emphasized the need to integrate compliance metrics and vulnerabilities into the systems where stakeholders actively work, eliminating the need to search through separate Excel documents. This could for example involve integrating security tooling within service platforms to visualize security within the platform that they are actively working within.

Compliance

The last category in the theme of maintenance success factors is related to compliance. Having internal and external audits is often beneficial for maintenance, as it provides the organization with a clear understanding of their weaknesses and what needs to be fixed. This also provides more weight to the security professional opinions, which can help to give resources to fix it.
Setting up processes for enforced monitoring and auditing of the organization's security posture was brought up by eight respondents. This involves identifying risks, monitoring identified risks, measuring if risks are being mitigated, and implementing control functions that follow up on security compliance as well as knowing who owns the risk in question. Enforced reviews of the ISMS were also recommended, with review periods set depending on the change in the organization.
5 Discussion

This chapter delves deeper into the interpretation of the findings and compare them with previous research. This section also includes limitations, ethical and societal aspects, validity and reliability as well as future research.

5.1 Discussion of results

The aim of this study was to gain an in-depth understanding of the challenges and factors contributing to a successful implementation and maintenance of an ISMS. The rationale for conducting research in this area stems from the increasing significance of information security due to heightened regulations on safeguarding personal data and information, alongside escalating dependencies on information technology within organizations (Singh et al, 2014; Aleksandrova et al, 2020). This study provided insights into various cultural, strategic, tactical and operational factors complementing previous research findings. Furthermore, the study identified multiple challenges and factors contributing to a successful implementation and maintenance of an ISMS.

The major challenges identified during ISMS implementation are grouped into the following themes: Misconceptions of security, Lack of Top Management Support, Resistance to Change and ISMS design. Top management support and the ISMS design were also recognized as significant factors contributing to success and will therefore be further discussed in later sections of this chapter. Misconceptions of Security was a common theme discussing challenges of ISMS implementation, stemming from a lack of knowledge and experience. Nine respondents perceived that a common misconception of security within the organizations is solely a technical issue handled by IT departments, rather than a strategic concern involving the entire organization. Similar beliefs have been acknowledged by Singh et al (2014) and seem to still be present within organizations. Werlinger et al (2009) suggest that the misconceptions of IT security and risk may be a consequence of lacking security awareness. Furthermore, participants experienced difficulties in making people understand the importance of information security and it is often seen as a cost rather than an investment. Unrealistic expectations about one-time investments in security technology and a focus on compliance rather than long-term value also pose challenges in ISMS implementation.

Another theme linked to challenges during the implementation process was Resistance to Change. Stakeholders within the organizations are often afraid of the outcomes of an ISMS implementation as it might increase their responsibilities and workload. This in turn often results in a negative attitude to implementing the changes required. Furthermore, stakeholders might be used to working in a certain way and are not willing to change their way of work. This in turn might result in difficulties making stakeholders adopt new behaviors and processes. Similar findings were suggested by Lowry & Moody (2014) showing that resistance to change may be greater if the stakeholder believes their freedom is at stake. Additionally, if the stakeholders have not faced consequences due to a security issue, the resistance to behavior change can be higher. Previous research also suggests that Resistance to Change may be a consequence of lacking internal security culture (Werlinger et al, 2009).

The factors contributing to a successful implementation of an ISMS were grouped into four major themes namely, Top Management Support, Internal Security Culture, ISMS Design and Communicational Factors. Top Management Support can be described as the provision of adequate resources by senior and executive leadership to facilitate security efforts within the organization,
which in turn facilitates the implementation as security does not get substandard due to resource constraints. Furthermore, top management support helps motivate the organization and pushes security from a top-down approach which decreases opposition in the organization. Including Chief Security Officers within the senior management was also considered an effective measure as it further helps to facilitate security. On the contrary, Lack of Top Management Support often results in lack of motivation, resources and prioritization and can thus be a critical challenge for organizations during ISMS implementation. Top Management Support being a crucial factor during Information Security Management is also supported by previous research (Werlinger, 2009; Singh et al, 2014; Stewart & Jurgens, 2017; Zammani et al, 2019). However, there are differences in the findings as this study goes into greater detail of how the absence or presence of support from top management is manifested within organizations.

Internal Security Culture was deemed a major theme for successful ISMS implementation. Education and awareness programs, including repetition and involvement of top management, was considered to be crucial for fostering a strong security culture. Similar results are supported by previous research, which have raised security culture, security training and communication as important factors during Information security management (Werlinger et al, 2009; Singh et al, 2014; Stewart & Jurgens 2017). Using top management as examples in information security training and conducting eLearnings can be effective, which is in line with previous research (Hu et al, 2012). Organizations in regulated industries may have an advantage in implementing ISMS due to existing risk and compliance culture, particularly in banks and governmental sectors which is supported by the findings of Topa & Karyda (2019).

ISMS design was shown to be a critical success factor as well as a challenge during ISMS implementation. In this context ISMS design means that selected controls must align with business context and requirements, the written documentation should use straightforward language and avoid buzzwords, furthermore, documentation should be minimized to prevent excessive documentation and complexity. Similar results were found by Topa & Karyda (2019), which showed that Information Security Policies should be in reasonable size and written clearly and adapted to a broader audience in order to be effective.

Effective Communication has been identified as a crucial element for the successful implementation of an ISMS, as supported by previous research conducted by Stewart and Jurgens (2017). Findings show that in order to effectively communicate about security measures, it is crucial to use language that employees understand and avoid technical jargon. Highlighting the benefits and risks in a relatable way encourages employee participation which is in line with previous research (Werlinger, 2009). Policy communication should focus on strategic perspective rather than technical details, gaining employee agreement. Understanding employees' needs and concerns through personalized communication can aid in tailoring the message. Meeting individually with resistant employees can also be effective in addressing their concerns and gaining support for ISMS implementation.

Resource Constraints during the maintenance of the ISMS was deemed as one of the major challenges. In this context it often involved lack of resources in terms of providing security tooling for monitoring vulnerabilities and patches, conducting external and internal audits, and lack of personnel that monitor and make continuous improvements to the ISMS. This often creates conflicts, especially within lower or middle management as they often operate under pressed budgets. Previous studies identified resource planning both in manpower and money as critical for Information Security Management, which is in line with the results of this study (Singh et al, 2014; Zammani et al, 2019; Topa & Karyda, 2019).
Continuous Administration is the theme that points at the importance of setting up an implementable ISMS from the beginning was highlighted as a prerequisite for a successful ongoing management of the ISMS. Making the processes for updating the ISMS clear and concise as well as having understood the dynamic nature of the system is also a prerequisite for successful ongoing adjustments.

Employee Attitudes focuses on the human factors such as the employees’ resistance to following controls, complacency, and organizations implementing ISMS for appearances rather than improving security. Furthermore, it appears that some employees may view security as an extra layer, rather than an integral part of all processes. Another challenge is to make sure that employees understand the importance of information security and its relevance to their daily work. All of this is in accordance with Topa & Karyda’s results from 2019 such as embracing cultural context and encouraging employees to comply. Also, Werlinger et al. (2009) mentions the difficulty of making people understand the significance of information security.

Relationships appeared to be one of the main success factors where maintaining relationships with stakeholders is the key. Hosting forums and stakeholder councils can help to discuss security matters and aid. It was suggested that being visible in the organization and encouraging employees to identify their own areas of improvement are critical factors. Adapting communication to the subject matter by understanding the business, regional context, organizational culture and adapting policies and guidelines were also seen as crucial, which is in line with Werlinger et al. (2009) who emphasizes the communication part as a big challenge.

Ownership, defined as assigning responsibilities and accountability to individuals for specific actions, is considered crucial for the successful maintenance of an ISMS. This allows for effective control implementation and compliance monitoring, as designated personnel can be held accountable for their tasks. Furthermore, by having a well-defined ownership structure, the burden on security personnel is reduced as they are not considered to be solely responsible for all security aspects within the organization. Assigning clear responsibilities has also been suggested as a critical success factor during Information Security Management, supporting the results of this study (Singh et al, 2014; Zammani et al, 2019; Topa & Karyda 2019).

Accessibility was a key factor for a successful maintenance of an ISMS. Accessibility in this context means that documentation and compliance metrics such as vulnerabilities and KPIs are clearly visible and communicated to the stakeholders. Similar findings were suggested by Topa & Karyda (2019) which stated that Information Security Policies should be effectively communicated and available to all stakeholders. Participants suggested having the documentation within the company’s intranet where it is clearly visible to all stakeholders and having the compliance metrics where the stakeholders are actively working. Having documentation within hidden folders or metrics within security systems or excel documents should be avoided as it minimizes the incentive for stakeholders to actively participate in the security work.

Compliance is the final maintenance success factor that includes that internal and external audits are beneficial for identifying weaknesses and providing weight to security professional opinions, which is backed up by Zamman et al (2019). It was suggested that setting up processes for enforced monitoring and auditing of the organization’s security posture is of great importance. This includes identifying, monitoring, measuring and mitigating risks, implementing control functions as well as being aware of who the risk owner is. Enforced reviews of the ISMS were also recommended for a successful maintenance work, with review periods set according to organizational changes.

In summary, multiple themes were identified during the implementation and maintenance of an ISMS. The major themes identified for the challenges of implementing an ISMS were Misconceptions of
security, Lack of Top Management Support, Resistance to Change and ISMS design. The themes identified for the factors contributing to implementing an ISMS were Top Management Support, Internal Security Culture, ISMS Design and Communicational Factors of which Top Management Support and ISMS design related to the challenges during the implementation process. The challenges of maintaining an ISMS were primarily related to Resource Constraints, Continuous Administration, Employee Attitudes and the success factors were related to Relationships, Ownership, Accessibility, and Compliance. Previous research also supported similar findings across most of the themes; however, this study provided differences in terms of depth and detail in its findings as it demonstrated how the factors are manifested within the organizations. Furthermore, the study also provided suggestions on how to prevent and overcome challenges that arise during implementation and maintenance.

5.2 Limitations

A pilot study was conducted before the data collection was initialized in order to find out if the research strategy, data collection method and interview questions were suitable and if the amount of time it consumed was feasible for the time scope of this study. The goal was to reach minimum 10 interviews but maximum 12 interviews to draw any conclusions for generalizability. One could argue that this is a rather small sample size, but the time scope of the study restricts the sample size since our transcription documents exceeded 165 pages which requires a lot of administration. Furthermore, it was deemed that data saturation had been reached as no new information or themes was being discovered. However, a larger sample size could potentially be even more representative for the broader population.

A total of 11 interviews were conducted with professionals who all had senior positions as either CISO or consultants with a broad experience from ISM related work such as implementation and maintenance. However, they all came from different backgrounds in terms of industries and size of organizations. On one hand one can believe it will give results that are inconsistent and hard to thematically analyze because the narratives are differentiated, but this was not the case. The findings of the study had many common factors and are to some extent in line with previous research, which adds objectivity and external validity to the study. New information also occurred which will contribute to future research, but also may require further research to be necessary to validate the findings.

Possible selection bias of the respondents can be eliminated, at least to the extent that it would influence and affect the findings from for example having respondents that are more willing to participate then others such as friends. A purposive sampling technique was carried out based on experience and relevance. This took place on LinkedIn when scanning people with roles such as CISO or Senior Information Security Consultant.

However, interviews are limited to companies primarily operating within the western world which may cause problems in generalizability to other populations or contexts since companies within different regions may face different challenges. This is because technology and culture may differ depending on the region which could affect the type of challenges that organizations face when implementing and maintaining an ISMS (Topa & Karyda, 2019).
5.3 Ethical and social aspects

In this study, the Ethical Principles outlined by the Swedish Research Council (2002) were employed as a guiding framework to ensure transparency and truthfulness as discussed in section 3.7. The research was conducted with a keen consideration of ethical considerations, including the selection of appropriate research methods and the meticulous description of these methods to enable replication. To further enhance the study's credibility, the quotes from respondents who spoke non-Swedish were translated into English and reproduced word-for-word.

From a societal perspective, this study should be viewed as an effort to enhance the understanding of how organizations can effectively implement and uphold security measures, and by doing so reduce the risk of information security related incidents from occurring. As previously discussed, organizations are becoming increasingly dependent on information systems which increases their attack surface and risk for incidents (Singh, 2014). While at the same time, cybercrime has become a lucrative business increasing the risk even further (Cremer et al, 2022). Having understood of how to reduce risks and how organizations should work with information security is therefore essential to create resilience on both an organizational and societal level, to prevent organizations and individuals being affected by security incidents.

5.4 Validity & reliability

We have utilized the criteria proposed by Lincoln and Guba (1985) to assess the trustworthiness of qualitative research. These criteria include credibility, transferability, dependability, and confirmability.

Credibility

To improve the credibility of this study, respondent validation, also known as member check, was utilized during the interview process (Bryman, 2012). We continuously rephrased a summarized version of the interview subject's responses to confirm the accuracy of the information given and to discard any misinterpretation of the responses. However, we were mindful of possible defensive reactions from the interviewees during respondent validation. Respondent validation helped to correct our biases during the interview by getting corrections if the interpretation of the answers were wrongful and thus improved the credibility of the results.

Transferability

Transferability, or external validity, refers to the ability to generalize findings to other contexts beyond the study's setting (Bryman, 2012). One important factor to consider when evaluating transferability is the contextual factors that may differ. In our study the respondents came from Western Europe, however, some of the respondents operated globally which means that we acknowledged a broad variety of geographical factors that may differ such as culture, legal frameworks and infrastructure. The transferability was further achieved in this study through having a diverse set of participants in the form of educational backgrounds and experience, while at the same time having a long experience of ISMS implementation and maintenance. This increases the potential for the findings to be relevant and applicable to a wider range of organizations and settings beyond the specific context of the study.

Dependability

Dependability is the equivalent of reliability (Bryman, 2012). Dependability can be challenging, particularly when it comes to replicating social situations. However, by providing a thorough
methodological description and utilizing the same techniques and interview questions with the same respondents, we were able to enhance the dependability of our study and generate similar results. In this study, the concrete nature of the subject matter also limited interpretation, with answers taken just as they appear to further support dependability.

**Confirmability**

Confirmability bears a resemblance to objectivity (Bryman, 2012). We achieved this by using audit trails which included being transparent and thoroughly describing how the data collection and sampling was conducted. Furthermore, the raw data collected in the form of recordings and transcriptions were kept, together with notes from the data reduction and analysis, creating audit trails for the findings. The potential threat of researcher bias was mitigated through our semi-structured interview format that allowed respondents to talk freely together with conducting a literature review on existing research within the area.

### 5.5 Future research

A future research agenda could potentially be to investigate different segments such as small to medium or large-sized enterprises to see if the findings differ. It could also be interesting to conduct a comparative study that explores the differences in implementation and maintenance challenges and success factors faced by companies in different regions, such as those in South America or Asia. This could potentially lead to different findings due to technological and cultural differences. Furthermore, additional research could be conducted to analyze the actual impact of each challenge and success factor within organizations. This could be conducted through a broader, and extensive data set using e.g., a quantitative method. This could potentially yield generalizable conclusions regarding the correlation and causation between each factor and the challenges and success of implementing and maintaining an ISMS.
This study analyzed challenges and success factors related to Information Security Management Systems (ISMS). More specifically, it has aimed to understand and identify the challenges and factors relating to a successful implementation and maintenance of an ISMS. The research questions were based on the needs of further research on why organizations tend to succeed and fail their implementation and maintenance of an ISMS. Extensive research was put into understanding what current research has identified and what needs to be further investigated. It was deemed that maintenance of ISMS remained relatively unexplored whereas some studies had analyzed the implementation of ISMS. The study adopted a qualitative method to answer the research question with the intent of gaining in-depth insights into various factors contributing to challenges and success factors within organizations. A total of 11 security professionals were interviewed using semi-structured interviews and were selected based on their experience within the field. The study identified 15 themes in which four related to implementation challenges, four relating to implementation success factors, three to maintenance challenges and four to maintenance success factors. The themes related to implementation challenges were Misconceptions of Security, Lack of Top Management Support, Resistance to Change and ISMS Design. The Themes related to Implementation Success Factors were Communication, Internal Security Culture, Top Management Support, and ISMS Design. Factors relating to Maintenance challenges were Resource Constraints, Continuous Administration, and Employee Attitudes. Themes relating to Maintenance Success factors were Relationships, Ownership, Accessibility, and Compliance. While previous research backed up most of the findings in this study, this research delved deeper into each factor and its expression within organizations, providing more comprehensive and detailed insights. The study also produced recommendations on how to overcome implementation and maintenance challenges derived from participants' experiences and suggestions.
References

Scientific references


Electronic references:


Appendix A – Consent Form

We are two students from the Master’s Programme in Information Security at the Department of Computer and Systems Sciences (DSV) at Stockholm University.

For contact:

Christopher Norén Wallin   Lukas Grenefalk

Email: christophernoren1@gmail.com  Lukas.grenefalk@hotmail.com

The purpose of the study is to gain insights into the challenges and success factors of Information Security Management Systems (ISMS) implementations and maintenance (post-implementation) for organizations. The study will use semi-structured interviews as a data collection method to gather participants' experiences and perspectives related to ISMS implementation and maintenance.

The interview will last approximately 45-60 minutes and will be conducted in either Swedish or English, depending on your preference. The interview will be semi-structured, meaning that the interviewer will have a set of questions prepared, but the conversation may also include follow-up questions or further elaboration on the participant's responses.

Your identity will be kept confidential and anonymous in all written and published materials. The interview will be recorded for transcription and analysis purposes only, and the recording will be deleted after the study is completed. You will have the right to withdraw and alter your contributions as well as cancel the interview at any time. You also have the right to refrain from answering specific questions and all participation is voluntary.

By participating in this study, participants are giving their informed consent to participate in this research study. Participants are encouraged to ask the interviewer any questions they may have about the study or their participation before giving their consent.

I give my consent to participate in this study under the conditions above:

Name

____________________

Signature

____________________

Date

____________________
Appendix B – Interview Questions

- **Introduction**
  Could you introduce yourself?
  - What is your background?
  - What is your current position?
  - How long have you been working with information security?

- **Challenges and Success factors of implementing ISMS:**
  What are the biggest challenges you have faced during an ISMS implementation process?
  If any, how did you address these challenges?
  What factors do you think are critical to the success of an ISMS implementation?
  How has the ISMS implementation been received within the organization(s)?
  How do you measure the success of the ISMS implementation?

- **Challenges and success factors of maintaining an ISMS:**
  What are the main challenges you have faced in maintaining the ISMS?
  If any, how did you address these challenges?
  What are the factors contributing to a successful maintenance of the ISMS?
  How do you or the organization ensure that employees continue to follow the ISMS policies, procedures and guidelines?
## Appendix C – Participants

<table>
<thead>
<tr>
<th>Participant</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO A</td>
<td>Over 20 years of experience within Information Security</td>
</tr>
<tr>
<td>CISO B</td>
<td>Over 20 years of experience within Information Security</td>
</tr>
<tr>
<td>CISO C</td>
<td>Over 20 years of experience within Information Security and IT</td>
</tr>
<tr>
<td>CISO D</td>
<td>Over 20 years of experience within Information Security and IT</td>
</tr>
<tr>
<td>CISO E</td>
<td>5 years of experience within Information Security</td>
</tr>
<tr>
<td>CISO F</td>
<td>18 years of experience within Information Security and IT</td>
</tr>
<tr>
<td>CISO G</td>
<td>6 years of experience within Information Security</td>
</tr>
<tr>
<td>Senior Security Consultant A</td>
<td>6 years of experience within Information Security, working primarily as a consultant</td>
</tr>
<tr>
<td>Senior Security Consultant B</td>
<td>5 years of experience within Information Security, working primarily as a consultant</td>
</tr>
<tr>
<td>Senior Security Consultant C</td>
<td>5 years of experience within Information Security, working primarily as a consultant</td>
</tr>
<tr>
<td>Senior Security Consultant D</td>
<td>6 years of experience within Information Security, working primarily as a consultant</td>
</tr>
</tbody>
</table>
Appendix D – Reflection Document 1

Lukas Grenefalk

● How does your study correspond to the goals of the thesis course? Why? Focus on the goals that were achieved especially well and those that were not well achieved.

Overall, I believe our study correspond to the goals of the thesis course. We have with relevant scientific methods and scientific literature completed a master’s thesis that contributes to information security related areas within computer and systems sciences. The contribution closes a gap in previous research that lacks knowledge about implementation challenges and mainly maintenance challenges of ISMS related work in organizations. Throughout the course I have learnt to improve my critical thinking and analytical skills in order to analyze and interpret our findings within the context of existing knowledge. One challenge to achieve the goal within was to extract the relevant information from the collected data, which was a lot of audio and in its turn text to go through. This took a long time to perform thematic analysis on, since a lot of information is excluded which created a fear of filtering out valuable information. Being consequent and patient with the data analysis helped us achieve the goal eventually.

● How did the planning of your study work? What could you have done better?

To be honest, the planning of our study was exemplary. Me and Christopher were very clear to ourselves that we wanted to have finished all interviews by early or mid-April, which was achieved. Next goal we had was to be almost or fully completed with the thesis by early May, which also was achieved. Since we both work part-time, we were both very meticulous with how we managed our time outside work which enabled a couple days a week with full dedication to effective thesis work. I am very grateful for having Christopher as a thesis partner. We are very like-minded in many areas which enabled effective teamwork to complete everything this thesis course required.

● How does the thesis work relate to your education? Which courses and areas have been most relevant for your thesis work?

As a student of the Master’s Programme in Information Security, I can say that information security management systems are a very central part of information security when it comes to organizations. Therefore, our chosen subject and area of research align very closely with several courses we have taken. I would especially like to point out Information Security in Organisations, Management of Global IT Resources and Legal Aspects of Information Security as the most relevant courses for our thesis work. I think the course names are quite self-explanatory with what content they teach and why they are relevant for our study.

● How valuable is the thesis for your future work and/or studies?

Everything from the previous literature within the field that we have carefully considered to the findings we have made provides a solid foundation for my future work, without any doubt. The full-time role I will start after the summer includes ISMS related tasks. Our thesis has contributed with a
great knowledge base that hopefully will facilitate the start of my information security career. Beyond the sharpened research skills and critical thinking abilities I have gotten, this thesis has enhanced my expertise in the ISMS field of study. Additionally, I believe our thesis can showcase my capabilities of planning and executing a considerable and significant project. This can be valuable both to me on a personal level as well as for future employers.

- **How satisfied are you with your thesis work and its results? Why?**

  I am very satisfied with our thesis work and the results we have produced. Mostly because we had a clearly defined gap in existing research that we wanted to close. We successfully closed the research gap with a couple of very precise research questions that every single one of them can be answered based on our collected data. Almost every interview we conducted was exemplary. Having up to one hour discussion with over 10 information security professionals was extremely informative and educative. I feel happy and satisfied and I genuinely hope our accomplishment have provided both theoretical and practical implications that can assist organizations in successfully implementing and maintaining information security management systems.
Christopher Norén Wallin

● How does your study correspond to the goals of the thesis course? Why? Focus on the goals that were achieved especially well and those that were not well achieved.

We think that the thesis met the goals of the thesis course, however, certain areas might have been improved even further. For example, we “only” conducted 11 interviews until we reached data saturation. If we conducted the study on a more global level (meaning including participants from multiple countries) we might have gained additional insights due to differences in technology and culture around the world, and thus, reach saturation at a later stage. Therefore, the scientific contribution could perhaps have been elevated and be more generalizable for the whole world. However, despite only focusing on the western world, a majority of the results aligned with other studies conducted in non-western contexts indicating that the generalizability might not have been affected.

Furthermore, the formulation of interview questions could possibly have been better, the interviews resulted in over 160 pages of transcripted material with a lot of information and topics that were left out of scope of this study. For example, we gathered data around participants' beliefs and suggestions on measuring security within organizations. Though it is an interesting topic we left it unexplored within the text as it did not answer the research question. Gaining this information was mainly due to a question we asked regarding if it is possible to measure success of security. Including the subject of measuring security success within the interview questions, even though it was interesting, wasted time in interviews which could have been used to ask questions relevant to the research questions.

Moreover, we sometimes struggled in separating the topics of ISMS maintenance and implementation, for example, it is impossible to maintain something that has not been implemented. This caused problems sometimes during the data analysis since interviewees at times started to talk about implementation within maintenance and vice versa. However, through detailed analysis of the results we managed to resolve the issue and managed to separate into different areas. Therefore, in general, though we faced problems during the thesis writing, we believe that we met the overall goals of the course.

● How did the planning of your study work? What could you have done better?

The planning went well, early on we decided that there was going to be a large focus on finishing the first three chapters as early as possible without compromising with the quality of the contents. This was largely due to recommendations from the supervisor but also through experience where it had been identified that the data collection and data analysis often takes most of the time. Therefore, we managed to be finished with the first three chapters relatively fast and could proceed with data collection early on into the course. The only major improvement that could have been done is to have put more time into the selection of the subject. First the thought was to write about social engineering attacks, but after starting the thesis writing we identified that the results would be predictable, and that the thesis would not be able to make a scientific contribution. However, we were relatively quick on
identifying a new subject which we both were very interested in.

- **How does the thesis work relate to your education? Which courses and areas have been most relevant for your thesis work?**

The topic of ISMS implementation and maintenance is very related to our master program within Information Security as it has been included as main content within both the course Information Security in Organisations “SECORG” and Cyber Security “CYBER”. The thesis can thus be seen as a study conducted to gain further understanding of this subject, to which could help to further help students understand the challenges of Information Security Management Systems. Furthermore, the course MMII and FMVEK have been really helpful to gain an understanding of the research process and how to conduct studies in higher-level education.

- **How valuable is the thesis for your future work and/or studies?**

The experience and results of the thesis have been really beneficial already, during the studies I have been working part-time with writing, implementing and maintaining an ISMS. Being able to identify challenges and success factors have been very useful not just for me but also for my colleagues and the results have, even though it is not published yet, been included in discussion on how to tackle certain challenges within the company. Thus, the experience of writing this thesis is and will be very helpful in my future work as it is something I probably will continue working with in the future.

- **How satisfied are you with your thesis work and its results? Why?**

We are very satisfied with the thesis work and results of the study. Firstly, we had a very good cooperation along the way where we both contributed equally throughout the project. Secondly, we believe that the thesis we produced is well-written as it is coherent and has a good flow throughout the text making it easy for a third-party to gain a good understanding of the topic. Lastly, the findings of the results we believe are relevant and contribute to the current scientific knowledge.