Implementation of ISO27001 standard in startups

Róbert Fúska

Information Security, master's level (120 credits)
2022

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

Abstract

Whether it is through self-motivation, or motivation of other stakeholders, startups are starting to think about and implement information security into their infrastructures and processes. The ISO 27001 provides a comprehensive security framework and is the most used security standard in the European Union. Startups seem to struggle with the implementation process even though it seems attractive for them to implement security.

This multiple-case study investigates what are the problems startups are facing when implementing the ISO 27001 standard, and what are the potential solutions for those problems so that the experience of the implementation of the standard can be improved. This thesis identifies the problems with the implementation of the ISO 27001 based on the literature as well as the experiences and opinions of the individual cases. Unlike previous literature, this thesis successfully provides practical solutions to those problems. Moreover, the thesis provides tips on what startups should think about before and during the implementation process.

Keywords: startups, security, implementation, ISO27001, ISMS

Table of contents

List of tables

List of figures

Abbreviations

CISO - Chief Information Security Officer

DPO - Data Protection Officer

EU - European Union

GDPR - General Data Protection Regulation

ISMS - Information Security Management System

ISO - International organization for Standardization

IT - Computers and information technology

MIS - Management Information Systems

NIST - National Institute of Standards and Technology

PII – Personally Identifiable Information

PRISMA - Preferred reporting items for systematic reviews and meta-analyses

SOA - Statement of Applicability

SME - Small and Medium Enterprise

UK - United Kingdom

1. Introduction

Information security means securing information systems and data against unwanted intruders, malicious software, unwanted use, and maintaining the fitness for the purpose of information in order to minimize institutional risk (Laybats & Tredinnick, 2016). At its most fundamental level, information security is about awareness. It is about knowing what to protect and how to protect it. And it is about knowing what to do and when, because, despite best efforts, things will go wrong. (Kaila & Nyman, 2018)

The ISO 27001 is the most used standard in enterprises in the European Union (Anttila & Jussila, 2017). A big reason for that is that it presents a comprehensive security framework (Kaila & Nyman, 2018). The ISO 27001 standard helps organizations to easily respond to security requirements that are starting to be called for by their customers or other stakeholders, as well as legal requirements that have been put in place by the European Union, such as GDPR. (Lopes et al., 2019). Therefore, it is often the choice for SMEs in the European Union to get ISO 27001 compliant or certified. In order to satisfy customer requirements and laws, startups are starting to think about implementing security into their processes.

There seem to be clear advantages for startups to implement information security into their company cultures and processes. It seems that if information security is tied in with all business processes, the investments into an information security program will pay off. However there seems to be a misalignment, and startups seem to be facing issues when implementing security in their processes. Lack of resources, lack of expertise, or focus on product development are some of the difficulties that are mentioned throughout the literature (Bada & Nurse (2019); Ključnikov et al (2019)). However, there seems to be a misalignment between the attractiveness of security and the problems or excuses startups seem to be experiencing. From the experience of the author of the thesis, these problems are usually avoidable, but many other issues arise when startups are trying to implement security standards and frameworks into their organizations. It is therefore possible that the problems are not only the startups and their lack of resources, but the standards and frameworks that startups are trying to use to provide and implement security.

Therefore, the goal of this research will be to find out what are the problems startups are facing when implementing the ISO 27001 standard into their infrastructures, processes, and cultures, as well as suggest potential solutions to those problems. The thesis aims to offer clarification into what the current process of ISO 27001 implementation looks like, as well as an insight into the problems and issues startups are facing when implementing the ISO 2701 standard. Furthermore, the thesis will aim to offer solutions on how the process of implementation can be improved based on experience from individuals or companies that have already experienced the process of implementation of the ISO 27001 standard, as well as the literature. In other words, the research is trying to find out what is happening, how it is happening and will try to draw conclusions based on that reality. Furthermore, the

research aims to provide key learnings startups should take into consideration that can help them implement the ISO 27001 standard successfully.

The thesis kicks off with the motivation for performing this research, and then continues with the literature review, which provides a deep dive into what the literature knows about implementing security in startups, and why the ISO 27001 standard is an attractive choice for the startups when considering implementing information security. The literature review also presents the issues that the literature identifies in the implementation process of the ISO 27001 and offers potential solutions to those problems. The reader is then presented with an overview of the methods that were used to conduct this multiple case study. The document then follows up with a section called Data collection, where the reader is presented with the case study protocols for individual cases. Section Data analysis presents the individual case study reports, as well as the cross-case report. The thesis is then concluded with the discussion & results, where the findings from the cross-case report are summarized and the research questions of this thesis are answered.

1.1 Motivation for research

The term 'startup' has been broadly used in research that was used to form this literature review. It is therefore vital that this term is defined properly, so that only relevant research is sourced and used as a reference. It seems that a definition of what a startup is actually is quite hard to find in the accessible research papers. Cambridge Dictionary (2019) defines the word ‘startup’ as a “small business that has just been started”. But startups don’t necessarily have to be companies that have just been established, as directly contradicted by definition by another research by Salamzadeh & Hiroko (2015). Salamzadeh & Hiroko (2015) define that startup companies are companies which struggle for existence, mostly based on innovative ideas. Other articles that the research had access to and talk about startups and their issues do not mention what a definition of a startup is, or which company qualifies as a startup. In fact, research performed by Campos (2019) questions if authors are not dodging the definition of what a startup is on purpose. Their research of multiple articles over the years also didn’t result in a clear definition of what a startup is, for how long a company can be considered a startup and how many employees a startup can have. Their conclusions were that “a startup is a company, generally associated with technology, that keeps growing, creating impact on peoples’ lives” (Campos, 2019). Moreover, the terms ‘startups’ and ‘SMEs’ have been used interchangeably in all the research presented by the literature review. It can sometimes be quite unclear to find out what do the researchers mean, and which of those two terms they actually try to refer to. Based on all the facts stated, from this thesis point of view, a startup is a company with no more than 50 employees, it is less than 10 years old and has the intention to grow substantially. Furthermore, startups are seen as a subset of Small and Medium Enterprises.

“In these days, information plays an important role for an organization” (Hamdi, et.al, 2019, pp:1). Startups produce and collect vast amounts of data (Iqbal et al., 2018). But having vast amounts of data, or any data at all for that matter, is turning out to be a huge problem.

While all companies have this problem, it is true for startups in particular. While the big corporations might, the research shows that startups are either not thinking about protecting that data, or simply don’t have the resources and expertise to focus on the necessary security for this kind of data and information (Bada & Nurse, 2019). In an attempt to grow faster, they prefer to focus on developing their product and services (Ključnikov et al., 2019).

Apart from lack of resources and expertise, there are multiple other reasons for startups not considering and implementing information security, or at least secure development practices into their day-to-day business operations. One of the reasons might be that the startups might find it overwhelming and time consuming to constantly look at the new trends and news about vulnerabilities, data breaches, and other threats out there (Kaila & Nyman, 2018). Another reason might be the ignorance, unwillingness, or lack of knowledge in the top management (Anttila & Jussila, 2017).

It seems that a similar problem is already happening in a somewhat connected world to information security - the implementation of EU’s General Data Protection Regulation. GDPR really had, and still has the potential to at least lay down the basic security principles in all companies, and to protect end user’s data. But the complexity of GDPR, missing framework for implementing GDPR and not enough resources or competences have caused that there are many companies out there that are nowhere near GDPR compliant. (da Conceicao Freitas & Mira da Silva, 2018; Bada & Nurse, 2019).

SMEs and startups together are a major player in every economy. In 2018, more than 98% of all organizations in the world were startups, (Europaïsche Kommission Statistisches Amt, 2021), which accounts for about 22 million SMEs in Europe alone (Anttila & Jussila, 2017). But more than 50% of all companies worldwide have fallen victim to various kinds of IT attacks (Pfeifer, 2021). According to Pfeifer (2021), “SMEs are believed to be the weakest members of supply chains”. As specified earlier, startups are a subsection of SMEs. It is therefore safe to assume that a vast amount of private information is not secured appropriately, if secure at all. Pfeifer (2021) also says that for this reason, it is not only individuals that should be afraid. Nowadays, startups and large enterprises are interconnected by both sides trying to take advantage of the newest technologies. While this saves time and money, it also leaves large enterprises vulnerable. This is supported by research from Lloyd (2020), which summarizes that large enterprises are in fact starting to realize this threat and are starting to act on it by looking very closely on who they collaborate with.

According to Renaud (2016), the security industry reports a high increase in cybercrime activities. Many of the startups think that their small size is going to keep them off the attackers’ radar, and therefore safe from cybercrime activities. But in today’s world, the SMEs and startups must worry about security and deal with the same amount of risk as the larger enterprises do (Kurpjuhn, 2015). Startups are not going to be protected from cybercrime activities solely by their small size. As a matter of fact, research is proving that SMEs are becoming the number one target for the attackers, as the attackers realize they are potentially quite vulnerable in many areas (Kapoor et al., 2018; Bada & Nurse, 2019). Therefore, startups are in very high danger of unauthorized access to their networks and infrastructures, leading to subsequent data leaks, which could either ruin the reputation of the company, or significantly hinder the financial situation of the company. Sϕhoel et al. (2018) nicely summarize that “security flaws have killed many startups along the years”.

But it should not be fear that drives the security in the startups, even if some parties think that it can be an effective tool (Renaud, 2016). It should be their general awareness and the realization of the importance of information security for their business in general. It seems though that understanding that can still be a challenge for the majority of startups. According to Lloyd (2020), only 15% of SMEs in the UK have some kind of formal incident management process and according to Hallová et al. (2019), 61% of SMEs they researched do not even want to find out the status of their security.

The common misconception in many startups is the belief that the sole purpose of information security is to reduce the risk of an attack, and to protect their assets. And while reducing the risk of attack is one important part of implementing information security, there are many more advantages of implementing information security programs into a company's culture (Lloyd, 2020). Hamdi et al (2019) state that information is a key asset that ultimately drives company decisions. But it seems that companies haven’t yet understood the fact that implementing security into the company processes can be an enabler to achieve bigger and better things. Effective information security programs and culture can enable startups to gain trust of larger organizations easier and retain them as customers for a longer period of time. (Lloyd, 2020) As Soomro et al. (2016) suggest, “protection of data and information from potential threats should be a part of business strategy, as it can give a competitive edge in a vulnerable online business market”. Startups also have often unrealized advantages when it comes to implementing security – particularly in their size, and their motivation. As all the startups are by definition small in size, they can quickly adapt to secure development life cycles. “In fact, smaller companies implement secure development life cycles at a higher rate than larger companies, likely because they have fewer decision levels and are less prone to bureaucracy” (Sɸhoel et al., 2018: p.1).

The results from the research seem to be direct. On one hand, it is clear that while startups collect large amounts of data, they fail to protect it for various reasons such as lack of time, knowledge and/or expertise. Furthermore, the startups are very much not protected from cyber-attacks, and they are becoming a top target for attackers. On the other hand, there seem to be clear advantages for startups to implement information security into their company cultures and processes. It seems that information security can and should be tied in with all business processes, and the investments into an information security program will pay off. In fact, security can be a key factor in the future for a business to be attractive for its customers. “The competitiveness of SMEs depends on their ability to secure

management of their main asset, information, and because of this, they need to have adequate security organizational practices beyond just technological resources” (Pérez González et al., 2019: p.13). Furthermore, information security research suggests that some governments or other bodies are trying their best to push information security in SMEs and startups forward (Renaud, 2016; Bada & Nurse, 2019).

But still, there seems to be some misalignment between the literature and the real-world startups. The researchers from the research papers mentioned above have clearly pointed out why security should be attractive, even from a financial perspective, which often can be the decisive factor. But it seems not to be, and perhaps there is another problem because of which startups are not starting to take security seriously. Companies, whether large or small, have many options when they want to secure their businesses. They can either decide to follow the industry best practices, such as Center for Internet Security (CIS) or Cloud Security Alliance (CSA). There are also a number of available, popular, and industry-wide used standards, such as NIST, or ISO (Kaila & Nyman, 2018). With the number of options, it can easily get confusing for a startup without any pre-existing knowledge about information security frameworks and standards. Furthermore, the usability of frameworks or standards seems to depend on the geographic location, the needs of the enterprise, and arguably most importantly, the requirements from the customers. Can there therefore be a problem with frameworks and standards that are trying to help companies be secure?

This section has demonstrated that the startups can only benefit from any form of security being implemented. Furthermore, findings by Lopes et al. (2019) state that companies that are only in process of implementation of the ISO 27001 standard, and let alone compliant companies, are already in a great position to be compliant with the GDPR requirements. “The implementation of ISO 27001 will help organizations respond to these requirements “(Lopes et al., 2019). Therefore, the ISO 27001 can solve multiple problems at the same time, which makes it a more compelling option for the startups to implement. Furthermore, according to Kaila & Nyman (2018), the ISO 27001 presents a comprehensive security framework. All the research articles mentioned and used by this literature review talk about companies that are located in the European Union, and the potential data collection sources for this research are also geographically located in the European Union. According to Anttila & Jussila (2017), the most used standard in enterprises in the European Union is the ISO 27001. For those reasons, this thesis doesn't focus on other popular standards like NIST but focuses only on the ISO 27001 standard.

1.2 Research question

The main objective of the thesis was to find out what are the issues when startups are implementing the ISO 27001 standard into their processes and cultures and to suggest improvements to the problems.

As a result of initial literature review that was performed to gain understanding and research objectives, the following research question and sub question were formed.

- What are the problems with the current implementation process of the ISO 27001 standard in startups?
  - How can the process of implementation of the ISO 27001 standard be improved?

1.2.1 Theory behind research question

The aim of this research was to find out what are the problems with implementation of the ISO 27001 in startups and how the current processes can be improved based on experience from individuals or companies that have already experienced the process of implementation of the ISO 27001 standard. In other words, the research was trying to find out what is happening, how it is happening and will try to draw conclusions based on that reality. Therefore, the research question is related to the theory of explaining (Gregor, 2006). This research question is then sub categorized in a second subtype of theory for explaining, as this subtype refers to explanation of things in real world situations. This research will be an exploratory multiple case study from a relativist perspective, as explained in the Methodology section of the thesis, which also supports the fact that it is related to the theory of explaining.

Culot et al. (2021) summarized multiple theories that can be used for the study of ISO 27001 standard and derived two social systems. As they summarize, the social systems thinking they suggest provides a great entry point for other researchers to engage in relevant issues that are arising for managers in the technological world. This thesis falls under the first social system – "the suite of standards, formal and informal practices – including ISO/IEC 27001 – that are implemented by organizations to manage ISS and cybersecurity" (Culot et al., 2021, pp:93). This social system finds support in the congruence systems model originally formulated by Nadler & Tushman (1980). In this model, the organizational practices are seen as systems, and the model identifies the inputs and outputs of those practices. The model assumes that the inputs and outputs live in balance and define the effectiveness of a system. Furthermore, Culot et al. (2021) also highlight the principle of equifinality (Katz and Kahn, 1978), which suggest that “different configurations of various system components can lead to the same output or outcome” (Culot et al., 2021, pp:94).

Culot et al. (2021) summarize that it would be interesting to investigate the implementation of the ISO 27001 standard, and the differences between requirements and actual practices. This thesis aims to find out what are the problems with the current ISO 27001 implementation process in startups, and how can the process of implementation be improved. The thesis challenges the principle by Katz and Kahn (1978) by understanding whether the different problems in startups can lead to unified solutions, and therefore to the same outcome of improving the ISO 27001 implementation.

1.3 Research Limitations

There were a couple of limitations when conducting this research. First of all, there were not that many scientific articles and research performed on the topic of the ISO 27001 standard in startups. The research had to compromise on the methodology and include case studies and supporting research papers on this topic. Secondly, the potential cases were limited due to the fact that there are not that many startups that have been through the process of implementation of the ISO 27001.

Moreover, the number of cases that interviews have been conducted with can be considered quite low. This limitation comes as a consequence of access to relevant informants. The thesis author didn’t have access to a large number of potential informants. The thesis tried to compensate with other research conducted on the topic that would provide more data. However, while partially successful, the first limitation of lack of research around this topic really showed itself again. Additionally, even though the targeted data collection sources were individuals or organizations with experience with the ISO 27001 implementation. As the literature review argues, the project is usually run by consultants or individuals with executive power in their organizations, and therefore the thesis tried to focus on collecting information from such individuals. It was quite challenging to arrange meetings with these individuals because of their limited time availability. Lastly, even though the research argued for and benefited from shorter interviews, it would be very difficult to perform longer interviews with these individuals.

2. Literature review

2.1 Literature review process

The purpose of the literature review is to present an informative overview of the problems startups face when it comes to the implementation of the ISO 27001 standards in their infrastructures and cultures. To achieve that purpose, the review is split into multiple parts based on the systematic review process described in Moher et al. (2009). Systematic search and review process was conducted based on the concepts and methods defined by Webster and Watson (2002), Levy & Ellis (2006) and Moher et al. (2009).

Moher et al. (2009) defined the PRISMA statement to help reviewers to perform a systematic review to "identify, select, and critically appraise relevant research, and to collect and analyze data from the studies that are included in the review" (Moher et al. 2009). The PRISMA statement consists of two parts – a 27-item checklist, and a flow diagram with four phases. This diagram is particularly interesting for performing a literature review, as it defines the four phases of a systematic review, which are really helpful when identifying relevant literature.

Webster and Watson (2002) believe that literature review is concept centric. To help researchers, they have defined a Concept matrix table. This table classifies all identified relevant literature based on various concepts, and therefore gives a great overview of the collected literature for the researcher.

Levy & Ellis (2006) have successfully summarized how to complete a literature review, and what parts of the literature review cannot be missing. This literature review will be based on the methods and definitions they made in their research. Therefore, this literature review is a mixture of concepts and methods defined by all Webster and Watson (2002), Levy & Ellis (2006) and Moher et al. (2009).

To make sure the identified literature is of the highest quality, the literature identification started by taking advantage of the flow diagram described by Figure 1, which showcases the different phases of a systematic review according to Moher, et al. (2009). The first process of the systematic review is the Identification process. The Identification process began with Keyword search. To avoid unnecessary ineffectiveness throughout the process the following keywords were identified in order to find the appropriate literature.: ‘security, ISO27001, startups, ISMS, implementation’. In addition to that, it was important to specify which databases were going to be used to search for relevant literature. The search was only conducted in databases that are listed in the top 50 ranked MIS journals (Levy & Ellis, 2006). These databases were also chosen for the fact that they provide researchers with peer reviewed articles. As Levy & Ellis (2006) define, “the use of the peer-review process is essential”, as it gives the researcher confidence about the published work. Furthermore, the researchers strived to only choose relevant articles that were published on the same list of the top 50 ranked MIS journals (Levy & Ellis, 2006), but there are some exceptions of this rule due to the limitations of this research, such as lack of access to certain journals on the

list, or the lack of research conducted around the topic in general. One exception to the database choice was made in order to simplify and streamline the literature identification. Google Scholar was added to the allowed database list. The reason for adding Google Scholar was that it is simply a collection of all the relevant databases in one place, which very much streamlined the entire process. Though caution had to be taken, as only links to the approved databases with relevant literature could be used. The keyword search was just the beginning of the identification process, as it started to be ineffective very soon, when a lot of non-applicable literature started to appear during the search.

In order to achieve better search results and identify relevant literature, the search shifted the method to backward search. This included reviewing the references of the already identified relevant literature that resulted from the keyword search. Backward search was a particularly useful method for my research, as it was able to produce a lot of valuable and highly relevant literature.

To complete the identification process and to maximize the number of relevant identified literature, a forward searching process was also performed. This included the search of articles that cited the already found relevant literature, and the authors that have published the identified relevant literature.

The second part of the systematic review by Moher et al. (2009) is Screening. As a part of this phase, a number of literature articles were excluded. This was done based on the title and the abstract of the research and evaluation of the relevance of the literature towards this thesis.

During the Eligibility process, the identified literature was also constantly tested for applicability to this study. It was sometimes challenging to decide which piece of literature is the correct one to include as a part of the literature review. If a research paper was only remotely relevant, it was never used as the foundation literature, but more as a support for an argument. The researcher can, with high degree of confidence, say that I strived to not take any material out of context and tried to stay as ethical with the use of references as possible.

The thesis then ended up with a definitive number of articles relevant to the research, but it was tough to remember what the articles say in detail. Therefore, a decision was taken to structure the literature review based on concepts of the identified literature, as Webster & Watson (2002) showcase in their example of a concept matrix. Based on this, the research was able to create the matrix of relevant literature, highlighting the main concepts each research paper is talking about. The link to a full-size matrix can be found in Appendix A.

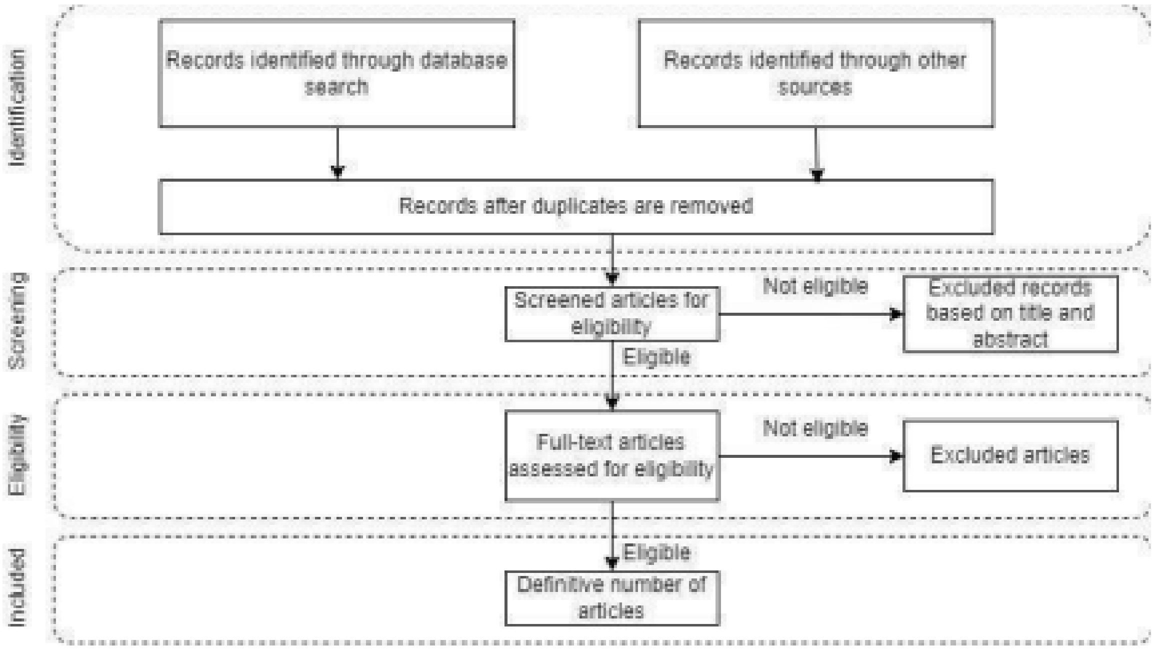
Identification
Records identified through database search
Records identified through other sources
Records after duplicates are removed
Screening
Screened articles for eligibility
Not eligible
Excluded records based on title and abstract
Eligible
Eligibility
Full-text articles assessed for eligibility
Not eligible
Excluded articles
Included
Eligible
Definitive number of articles

Figure 1 - Phases of systematic review, adopted from Moher, et al. (2009)

2.2 Reflection on used methodologies in research

Most of the relevant research from this literature review was using qualitative data collection methods. Exceptions to this rule are some articles containing quantitative data. The research methods used in the qualitative data collection were mostly case study, qualitative interviews, structured expert evaluation method and action research. It is sufficient to say that the qualitative research methods seem to be preferred. Ključnikov et al. (2019) mention in their research that by using quantitative methods in their research about the factors of success in information security management in startups, they would face a risk of getting unreliable data from inexperienced respondents.

2.3 About ISO 27001

One of the key characteristics of the ISO 27001 standard is that it attempts to cover all types of organizations, disregarding the type, size, or location of the organization (Candiwan, 2014). As Hamdi et al. (2019) summarize, the ISO 27001 is “a process management and assessment standard that provides specifications for an Information Security Management System (ISMS)". It presents a comprehensive security framework (Kaila & Nyman, 2018), and it consists of two main parts. The first part contains the requirements for the creation, implementation, maintenance, and improvements of an Information Security Management System (ISMS) of a company. The second part, also called Annex A, defines the control objectives and security controls. The Annex A consists of 11 security domains, and provides information on 114 controls across 14 categories, and other measures that can be relevant to the information security. These controls can vary from policies, procedures, practices, software controls or organizational structures. (Lami, 2013)

The motivation for the implementation of the ISO 27001 standard can vary throughout different organizations (Hamdi et al.,2019). Organizations have two options implementing the ISO 27001 standard. These options, along with the motivation, ultimately specify the goal and the scope of the project. They can be compliant with the standard, or they can go one step above that and get ISO 27001 certified. As mentioned above, the ISO 27001 standard specifies a number of clauses that are mandatory to comply with if an organization implementing the standard wants to be either compliant or certified with the standard (Hamdi et al., 2019). But given the sheer size of the standard and scope of the implementation project, the levels of compliance can vary. While multiple research papers, such as the one from Susanto et al. (2012) demonstrated multiple ways of identifying the compliance levels of an organization in depth, Nasser (2017) defines 3 overall levels of compliance:

- Compliant level – when the organization is fully compliant with the ISO 27001 standard;
- Partially compliant level – The organization has taken steps towards being compliant, but additional work is required;
- Non-compliant level – The organization hasn't taken any steps towards the ISO 27001 requirements.

There is one more level above these, which is the certification. Getting certification, however, costs additional resources. As mentioned previously in the literature review, startups are lacking resources to implement information security into their organizations. It is therefore safe to assume that unless a startup has a clear business requirement to be ISO 27001 certified and spend the additional resources to get that certification, the startups will only strive for compliance with the standard. Therefore, in the context of this research, the implementation of ISO 27001 standard in startups is the process with a goal of being ISO 27001 compliant.

2.3.1 Implementation of ISO 27001

The implementation of the ISO 27001, and the development of the Information Security Management System requires a number of measures to be taken. Available literature fails to directly identify who is the person responsible for running the implementation process. The standard also doesn't specify the exact resources (Chopra & Chaudhary, 2020). Kosutic (2016) specifies that in small organizations, it is usually the Chief Information Security Officer (CISO), and/or an external consultant. Chopra & Chaudhary (2020) define the CISO as the person responsible for preparing the information security policies and procedures and is considered the head of security. According to (Monzelo & Nunes, 2019), the person that is designated CISO has an executive role within the organization.

According to Hamdi et al. (2019), the plan-do-check-act cycle is usually used when structuring the ISMS processes. The stages of the plan-do-check-act cycle are:

- Plan – Design the ISMS
- Do – Implement and operate the ISMS
- Check – Monitor and review the ISMS

- Act – Maintain and enhance the ISMS

As Lami (2013) summarizes, the standard defines 10 key steps to be taken when organizations aim to be compliant with the standard. These steps result in creating documentation which is the backbone of the ISMS, as required by the ISO 27001. The steps are:

- Getting management support
- Definition of the ISMS scope
- Definition of a security policy
- Risk assessment
- Risk management
- Selection of controls
- Statement of applicability (SOA)
- Policies / procedures
- Internal audit
- Continuous improvement

To understand and draw what steps companies need to go through to implement the ISO 27001 standard, we can compare the plan-do-check-act process with the 10 key steps summarized by Lami (2013). When looking at the plan-do-check-act process summarized by Hamdi et al. (2019), the implementation of the ISO 27001 happens only in the first two stages. As the purpose of the last two steps is to monitor, maintain and improve something that has already been implemented, they have nothing to do with the implementation process.

When comparing the last two stages to the 10 key steps by Lami (2013), the thesis argues that only the first 8 steps are truly the implementation process. It is safe to assume that during the internal audit, no implementation of the ISO 27001 happens, as the Cambridge Dictionary (2019) defines audit as “an official examination of the accounts of a business”. During continuous improvement, it is possible for some implementations of technical controls to happen, but Cambridge Dictionary (2019) defines improvement as “an occasion when something gets better or when you make it better”. Therefore, something must first be implemented before it can get better. To summarize, due to the arguments stated just above, the implementation of the ISO 27001 standard consists of the following steps:

- Getting management support
- Definition of the ISMS scope

- Definition of a security policy
- Risk assessment
- Risk management
- Selection of controls
- Statement of applicability (SOA)
- Policies / procedures

Lami (2013) only provided partial explanations on what is understood under each step. However, to work with this model further, it is important to understand what is meant under each implementation step. Braga (2018) explained the steps in more detail in his presentation. His perspective helps to understand the meaning of each step. While some of the steps are very self-explanatory, it is beneficial to have them stated to avoid future confusion.

- Getting management support – Refers to obtaining appropriate support from the top management of an organization
- Definition of the ISMS scope – Refers to the decision about which parts of an organization is the ISMS going to be implemented on
- Definition of a security policy – Refers to defining the ‘top level’ information security policy, which is one of the most important documents within the ISMS. According to the ISO 27001 (EN ISO/IEC, 2017), this policy should include the organization's objectives with information security.
- Risk assessment – Refers to choosing an appropriate methodology for the risk assessment
- Risk management – Refers to performing the risk assessment, and deciding on the risk treatment strategies
- Selection of controls – Refers to specifying the actual controls to be applied based on the risk treatment strategies
- Statement of applicability (SOA) – Refers to preparing the SOA. SOA specifies the set of controls that are applicable to the organization.
- Policies / procedures – Refers to preparing writing the policies and procedures for the organization

To clarify what are the mandatory documents that need to be created during the implementation, Candiwan (2014) summarized the mandatory documents that an organization needs to have in place and implemented in order to be compliant with the ISO 27001 standard, with the respective clauses.

It might be confusing for the reader, and in fact for the startups as well that documents such as Internal audit program or Results of internal audits are included in the implementation process, even though the internal audit and the continuous improvement were considered not to be a part of the implementation process. However, the creation of these documents is a part of the implementation process because the documents serve as a preparation or a guide for the fact that internal audit is supposed to happen. The documents should also state how the internal audit is going to look like, so that there is little uncertainty when the time comes to perform the internal audit.

	Document	**ISO 27001 clause(s)**
1	Scope of the ISMS	4.3
2	Information security policy and objectives	5.2 & 6.2
3	Risk assessment and risk treatment methodology	6.1.2
4	Statement of Applicability	6.1.3 d
5	Risk treatment plan	6.1.3 e & 6.2
6	Risk assessment report	8.2
7	Definition of security roles and responsibilities	A. 7.1.2 & A.13.2.4
8	Inventory of assets	A.8.1.1
9	Acceptable use of assets	A.8.1.3
	Access control policy	A.9.1.1
11	Operating procedures for IT management	A.12.1.1
	Secure system engineering principles	A.14.2.5
	Supplier security policy	A.15.1.1
14	Incident management procedure	A.16.1.5
15	Business continuity procedures	A.17.1.2
	16 Statutory, regulatory, and contractual requir A	
17	Records of training, skills, experience, and qualifications	7.2
18	Monitoring and measurement results	9.1
19	Internal audit program	9.2
20	Results of internal audits	9.2
21	Results of the management review	9.3
22	Results of corrective actions	10.1
23	Logs of user activities, exceptions, and security events	A.12.4.1 & A.12.4.3

Table 1 - Mandatory requirements for ISO 27001, adopted from Candiwan (2014)

2.4 Problems with the implementation process

Hamdi et al. (2019) specifies that if organizations want to implement the ISO 27001 standard, they are required to produce a specific set of documents that are mandatory to have according to the standard. However, the available research suggests that the ISO 27001 standard isn't really designed with the startups in mind. "Although such standards present comprehensive security frameworks, they can be prohibitively cumbersome to a startup or a startup looking to take their first steps towards implementing information security practices" (Kaila & Nyman, 2018: p.34). On top of that, Gaitero et al. (2021) refer to the fact that the controls in Annex A may not be appropriate for a lot of SMEs, and therefore startups as well. They argue that "for a company to become ISO compliant the implementation of many controls is required, some of which may not be appropriate for the characteristics of most SMEs", and thus also startups (Gateiro et al., 2021: p.1). Furthermore, as Anttila & Jussila (2017) point out, they have been closely analyzing the ISO

27001:2013 standard from an organizational point of view in their research. Their findings are rather interesting and support the issue. They claim that "established information security management methodology is not available for these business environments. The international standards are mainly based on the situation of the well-established organizations, which usually are large organizations. The standards could be useful for small organizations, if they had been drawn up in accordance with their circumstances" (Anttila & Jussila, 2017: p.2). Anttila & Jussila (2017) conclude that some education, knowledge, or preexisting experience is required in order to implement the ISO 27001 in a startup, as the standard has many problem areas that can be difficult to identify for an inexperienced person with the standard, or in the field of information security.

There has been an attempt to create a framework which could help startups get ISO 27001 compliant within 7 weeks. This research was performed by Gaitero et al. (2021). While the framework was proven to work on a couple of Spanish startups, an intervention, or some amount of consulting help from an experienced security person was required, and therefore the startups were still forced to spend resources, which as this review has demonstrated before, they lack. The author of the thesis is of the opinion that the research by Gateiro et al. (2021), and other research papers in this thesis still force startups to spend resources they clearly do not have.

Other patterns were noticed as well. The available research doesn't actually provide any help to startups, other than summarizing the standard and the weaknesses of the standard, or they just use slightly different words compared to the ISO 27001 itself. Moreover, the use of the language is too complex for a person out of the information security industry. But while research aimed directly at startups or SMEs hasn't been particularly helpful, lessons can be learnt from comparisons between bigger enterprises trying to implement the ISO 27001 standard in their organizations. Study performed by Candiwan (2014) shows the gap analysis in Enterprises and SMEs in Indonesia. They define 5 maturity levels based on which they judge the quality of the implemented ISMS, where 0 is the lowest and 5 is the highest maturity level. This study concluded that large enterprises have better ISMS implemented compared to the SMEs. On average, the enterprises were on maturity level 3, whereas SMEs were on maturity level 2 only. Hamdi et al. (2019) conducted a similar gap analysis, in which they examined various types of organizations from Enterprises, SMEs, Educational institutes and non-profit organizations. They concluded that Enterprises in their gap analysis are closest to maturity level 5 with their compliance are educational institutions and enterprises.

Available research shows that most of the big corporations seem to be roughly following the 8-step implementation process outlined by Lami (2013) earlier in this chapter. This leads to patterns that are starting to appear throughout the various research papers about ISO 27001 implementation in companies of various sizes. In research performed by AbuSaad et al. (2011), which focused on implementation problems of the ISO 27001 standard in companies of various sizes in Saudi Arabia, they summarized that majority of the organizations seemed to agree that identifying the organization's assets was one of the major obstacles during the implementation phase, along with a lack of experience in the team (AbuSaad et al., 2011). Lami (2013) supports this and also points out that misidentification of assets is a common pitfall.

Most companies in the gathered research also struggled with employees being resistant to change, employees and implementers of the standard understanding of the standard itself and the involvement, or lack of it, of the top management. This is supported by research published by Vuppala et al. (2011), in which they found that the most important factor of successful ISO 27001 implementation is the management support. Research by AlMayahi & Mansoor (2012) found out that while other parts of the organizations might be striving for maximum compliance, the management was not compliant with the written policies and procedures in more than 60% of the cases. Among many other common pitfalls of the ISMS, Lami (2013) has also identified the lack of senior management support. Other research is also stressing the important role of employees in the ISMS. Lami (2013) states that employees implementing the ISO 27001 do mostly have technical background, and often only put emphasis on the technical aspects. In reality, employees of the company are often the weakest link in the security chain. “The essence of success/failure for an ISMS project mostly depends on the behavior of people involved, rather than buying/placing high-tech equipment” (Lami, 2013). Kosutic (2010) states that employees must embrace the new security controls which will come into effect with the implementation of ISO 27001. As mentioned earlier in this paper, the available literature is of the opinion that the ISO 27001 can and most likely will affect the company culture, change workflows, and affect the day to-day operations and habits. If the employees do not understand that they must embrace the security policies and procedures, the implementation of ISMS will fail. Furthermore, people often fail to understand the fact that such a project is not only affecting the IT department, but the entire company, or the entire scope of the ISO 27001 implementation. Vuppala et al. (2011) points out that drastic changes to processes before the implementation of the ISO 27001 will unnecessarily infuriate users. The scope is another problem of the ISMS implementation. It is important to decide what the scope of the ISMS is before the project even begins, or in other words which parts of the organization is one trying to secure. The size of the project greatly varies based on this decision. This common problem is also outlined in the research by Lami (2013) and supported by Vuppala et al.

(2011). Vupalla et al. (2011) summarize that “it is not necessary to implement it across the entire organization in one shot”. They also point out that the scope of the standard is adjustable, and it might be beneficial to start small, and then expand to other parts of the organizations, especially with a small number of resources.

Other factors that should be considered when implementing the ISO 27001 into organizations are the security controls and the complexity of policies and procedures. Susanto et al., (2012) summarizes that controls tend to be disorganized, and difficult to understand, and difficult to implement for organizations. AlMayahi & Mansoor (2012)

observed that ineffective security policies do result in non-compliance very quickly, while Lami (2013) sums up that ineffective security policies, procedures and instructions will lead to failure of the ISMS.

On top of all of the issues connected with the implementation of the ISO 27001, Lami (2013) comprehensively summarized a list of common mistakes throughout the process of the implementation of the ISMS. The list below presents issues that have not yet been identified by any other literature, and therefore not talked about in this literature review:

- Lack of project planning
- Lack of delegation of security roles within the organization
- Misalignment or lack of mandatory documentation for the ISO 27001 - Problems with writing and implementing business continuity plans

2.4.1 Summary of implementation problems

Table 2 below summarizes the issues with the implementation process that were discovered, discussed, and highlighted by the literature review. The explanations of the individual steps by Braga (2018) was used to logically assign the issues to the eight implementation steps derived from Lami (2013).

Implementation step	**Issue**	**Reference**
Getting management support	● The involvement, or lack of it, of the top management	• Vuppala et al. (2011); • AlMayahi & Mansoor • (2012); Lami (2013)
Definition of the ISMS scope	● Not necessary to implement it across the entire organization in one shot; ● Project affecting the entire organization; ● Education, knowledge, or pre existing experience is required in order to implement the ISO 27001 in a startup;	• Kosutic (2010); • AlMayahi & Mansoor (2012); • Vuppala et al. (2011); • Anttila & Jussila (2017); • Kosutic (2010); • Gaitero et al. (2021); • Lami (2013)

	● Lack of project planning	
Definition of a security policy	● Lack of delegation of security roles within the organization	● Lami (2013); ● Anttila & Jussila (2017)
Risk assessment	● Identifying the organization's assets;	● AbuSaad et al., (2011); ● Lami (2013)
Risk management	n/a	n/a
Selection of controls	● Emphasis only put emphasis on the technical controls; ● Employees must embrace the new security controls	● Lami (2013); ● Kosutic (2010)
Statement of applicability (SOA)	● The language and way the standard is written; ● Standard not designed with startups in mind; ● Maturity levels of ISMS	● Anttila & Jussila (2017); ● Kaila & Nyman, (2018); ● Candiwan (2014); ● Hamdi et al. (2019), ● Gaitero et al. (2021)
Policies / procedures	● Complexness of policies and procedures; ● Problems with writing and implementing business continuity plans; ● Misalignment or lack of mandatory documentation for the ISO 27001	● AlMayahi & Mansoor (2012); ● Susanto et al., (2012); ● Lami (2013)

Table 2 - Summary of implementation problems identified by the literature review compared to the 8-step implementation process derived from Lami (2013)

2.5 Solutions to implementation problems

2.5.1 Research papers

It seems that there are not many solutions to the implementation problems identified by the literature. Even when the scope of the research was increased to include articles on the topic that are not from the top 50 ranked MIS journals specified by Levy & Ellis (2006), only two available research papers were discovered. Asosheh et al. (2013) propose a methodology for addressing the risk assessment and risk management issues identified by the literature review. The suggestions provide practical support for organizations to identify assets in their organization, directly addressing the issues identified in the Risk assessment step of the implementation process. The other steps are unfortunately just very generic suggestions to obtain management support, define the ISMS scope and security policy, but do not go into any detail as to how companies are supposed to practically address these

issues. More useful part of the report is a methodology that can be used to perform qualitative risk assessment. However, lack of or wrong methodology have not been identified as an issue so far.

Punhani et al. (2012) performed a case study showcasing an implementation process of the ISO 27001 standard. While the case study fails to specify what kind of company the case was, the research manages to provide high level guidance on the fact that the ISO 27001 doesn’t have to be implemented on the entire organization. Their case study also defines the security organization and explains what roles have been defined and stating their responsibilities, however, fails to state any other roles that could potentially be possible to identify. Nevertheless, the document provides an overview of the methodology used when identifying assets and selecting controls for the threats and vulnerabilities. Other identified issues from the implementation process fail to be addressed.

2.5.2 Other publications

While both of these research articles address some of the implementation issues, mostly by providing methodology, issues outside risk assessment and risk management remain unanswered. Moreover, this practical support did not seem to be addressed directly at startups. To obtain more data on the possible solutions to the implementation problems, the author of the thesis considers it relevant to make another exception to the literature review methodology specified in the beginning of this chapter. While research articles seem to fail to provide answers, the companies on the market might already be offering solutions to those problems. Therefore, the literature review also considers blog articles and other publications to be a relevant and valuable resource that could help the thesis with answers to the research questions.

ISACA, an international association focused on IT governance published a practical guideline for implementing an ISMS. This guideline addresses some of the issues that were identified by the literature review. First and foremost, they take a fresh look at getting management support. So far, the literature review identified top management as only the management of the entire organization. However, ISACA (2016) clarifies that according to them, top management can also be understood as local managers or department managers. This could be a helpful understanding for the startups, as they could delegate the responsibilities of top management to the lower managers, if the structure allows it. Moreover, ISACA (2016) directly lists the responsibilities and primary duties of the top management. These could help to understand what is meant by the involvement of the top management, and what are the exact actions the management is expected to perform in order to support the standard. Some of the responsibilities include requiring other managers to serve as role models, making resources available for the ISMS, visible involvement in the process of ISMS or integration of the requirements set by the ISMS into business processes.

When it comes to the problems with setting the scope, Kosutic (n.d.) – an author that was previously mentioned in the identification of problems with the ISMS implementation –

mentions in his blog article that startups should probably focus on implementing the ISO 27001 in the entire organization. While ISACA (2016) states that the scope defines the amount of work that is going to be required throughout the implementation process, Kosutic (n.d.) argues that a smaller scope does not mean easier implementation. That is because the parts of the organization that one leaves out might cause the biggest problems in the future. Furthermore, both Kosutic (n.d) and Kantor (2021) stress that the ISMS should be treated as a project, as it is a complex undertaking. If startups understand that the ISMS should be treated as a project which involves a lot of people, some of the problems with project management will be solved.

ISACA (2016) also addresses the delegation of security roles. While they don't exactly specify how the roles should be delegated, they clarify that conflicts of interest should be avoided. They state that a company should establish at least a Chief Information Security Officer (CISO), and a Data Protection Officer. They directly address the issue of small companies not having enough individuals for all the security roles and therefore specify that the CISO and the DPO can in fact be delegated to one person.

Selection of controls and the highlighted issues are something that even such articles like blogs or other publications fail to address. While Kosutic (n.d.) also highlights that the problems with selection of controls exist, he or other publications fail to provide suggestions for a solution. Similarly, while risk assessment and risk management issues were addressed by Asosheh et al. (2013) and Punhani et al. (2012) earlier in this section, the identified issues connected to the Statement of Applicability haven't been addressed.

It has been identified by the literature review that the ISO 27001 is not designed with startups in mind. However, the purpose of the Statement of Applicability, according to the ISO 27001 (EN ISO/IEC, 2017) is to determine which controls are necessary to implement. Kosutic (n.d.) supports this by saying that the SOA lists all the controls that are applicable to the organization. There therefore seems to be a gap between the problem and the solution. These two areas therefore seem to be in a need for further research to provide an adequate answer.

Finally, the complexities of policies and procedures and problems with writing various plans does not seem to be addressed by the publications. This thesis is already a great help for startups to identify which documents are a mandatory part of the ISO 27001 standard by listing them in Table 1. ISACA (2016) sets out rules and success factors for the ISO 27001 documentation, however it doesn't directly address the identified issues. There seem to be companies out there on the market that are able to provide startups with templates for various documents that are required, however this is where the issue with availability of resources to acquire such documents from these platforms comes up.

Research in the form of a master thesis project was performed by Sandin (2021). Their thesis performed a qualitative research with the aim of finding out if it is possible to simplify the implementation of ISMS for small organizations. Sandin (2021) conducted 5 interviews with 5 professionals with experience with the ISO 27001 implementation process. Semi structured interviews were conducted with experts on the topic. The respondents chosen for the data collection were individuals with experience with the ISO 27001 implementation, which would classify them for the requirement of data collection points that this thesis has. The semi-structured interviews that were conducted were longer interviews, with the average duration of over 1 hour.

Their thesis identified very similar problems in the implementation of the ISO 27001 to this thesis, and summarized advice for small organizations that want to implement the ISO 27001. The interviews suggest that the small businesses hire a consultant for guiding the startups through the implementation process. This advice is however considered irrelevant, as this literature review clearly stated that in startups, there might not be enough resources to hire such help. Their thesis however gives valuable advice on how to acquire management support. One of the interviewees summarized that the top management should be presented with the cost of what it would cost to not implement security in the future. Furthermore, they summarize that the project should have a designated owner, and the work should be split into smaller steps. They specify that the project should be designed to target the ‘low hanging fruit’ first.

Table 3 below summarized the potential solutions identified by this literature review respective to the issues and implementation steps, as well as reference to the authors that the solutions were proposed by.

Implementation step	**Issue**	**Potential solution**	**Reference to the solution**
Getting management support	• The involvement, or lack of it, of the top management	• Clarify management responsibilities and duties; • Include department managers • Present cost of no security	• ISACA (2016) • Sandin (2021)

Definition of the ISMS scope	• Not necessary to implement it across the entire organization in one shot; • Project affecting the entire organization; • Education, knowledge, or pre existing experience is required in order to implement the ISO 27001 in a startup; • Lack of project planning	• Treat ISMS implementation as a project. • The scope in startups should be the entire organization • The project must have an owner • Work split into smaller phases / steps	• Kosutic (n.d.) • ISACA (2016) • Kantor (2021) • Sandin (2021)
Definition of a security policy	• Lack of delegation of security roles within the organization	• Avoid conflicts of interest; • Combine multiple security roles to one individual in startups	• ISACA (2016)
Risk assessment	• Identifying the organization's assets;	• Methodology	• Asosheh et al. (2013), Punhani et al. (2012)
Risk management	• Missing prioritization of tasks and milestones;	• Methodology	• Asosheh et al. (2013) Punhani et al. (2012)
Selection of controls	• Emphasis only put emphasis on the technical controls;	• Implement easy treatments first	• Sandin (2021)

	• Employees must embrace the new security controls		
Statement of applicability (SOA)	• The language and way the standard is written; • Standard not designed with startups in mind; • Maturity levels of ISMS	n/a	n/a
Policies / procedures	• Complexness of policies and procedures; • Problems with writing and implementing business continuity plans; • Misalignment or lack of mandatory documentation for the ISO 27001	n/a	n/a

Table 3 - Proposed solutions to identified Iso 27001 implementation issues

2.6 Research gap & Problem Statement

It is safe to assume that the problems of startups regarding lack of resources and experience will not easily go away. When startups identify the need for being secure, either through a stakeholder requirement or through their own realization, they often won't have any other option but to start implementing security on their own.

The literature review clearly highlights how the implementation process of the ISO 27001 looks like, and what is the theory behind implementing the ISO 27001. Based on those findings, the literature review was able to identify key problems throughout the implementation process of the ISO 27001. The research identifies a lot of problems with the implementation process and answers the main research question. Moreover, some solutions for the issues related to the implementation of the ISO 27001 were presented.

These solutions resulted from a combination of relevant research answering the problems and other publications such as blogs, or thesis. These publications were considered relevant as they identified the problems that the research was able to identify and proposed many solutions to those problems. It can be questioned whether all of the problems with the implementation process have been identified by the relevant literature, or whether there are other problems which the literature failed to identify. Therefore, it can be considered unclear whether these solutions are actually valid for startups, and whether there are any more problems and solutions that startups could take advantage of.

For those reasons, Startups that have further research are required to identify whether the problems highlighted by the literature review match the problems of startups, and whether startups with experience mention more problems with the implementation process. Furthermore, it would be interesting to find out if startups themselves have an idea about potential solutions that would come from their experience of working with the ISO 27001 standard. Because startups and big enterprises are interconnected, the literature review indirectly identifies that until a solution is not found, the world's data is in a potential danger of being exposed or leaked through the startups that do not have security measures in place. Such research could greatly benefit startups as they would not only be able to learn from the mistakes that have already been made. This could also replace the requirement or the issue with lack of experience. This research could offer startups valuable learnings when they start trying to implement the ISO 27001 standard on their own.

In the next chapters of this thesis, the thesis tries to find out if the problems in the implementation phase of the ISO 27001 highlighted in the literature review translate to startups, or if there are additional problems that the literature failed to identify. Furthermore, the thesis attempts to answer the research questions by introducing suggestions to those problems. This is done by examining the current implementation process in startups and learn from their mistakes, as well as highlighting any additional key steps that might arise and could help startups ease the implementation of the ISO 27001.

3. Methodology

3.1 Research approach

Research is the process of gathering, analyzing, and interpreting information or data in order to answer questions and gain understanding (Leedy and Ormrod, 2020).

Different authors have summed up different methodologies to guide researchers throughout the process of research. The two most common research methods are the qualitative and the quantitative research method. When choosing the relevant research method for a project, one must know the positives and negatives of each methodology in order to choose the correct method that should guide them to successfully answer the research question.

As Leedy and Ormrod (2020) say, qualitative research typically focuses on phenomena that are happening in the real world and tries to study the many dimensions of an issue. In contrast with quantitative research, the researcher using qualitative research is very much inside the investigated phenomena, makes observations of elements and to explain these elements. (Williams, 2007).

Yin (2018) presents the difference between the five social science research methods using three conditions – the form of a research question, the control a researcher has over behavioral events and the degree of focus on contemporary events. Based on this criteria, a researcher should be able to define which research method is relevant for their research. This matrix of choosing qualitative research strategies defined by Yin (2018) is shown in Table 4 below.

Research method	***Form of research question***	***Has / requires control over behavioral events?***	***Focuses on contemporary events?***
Case Study	How, Why?	No	Yes
Experiment	How, Why?	No	Yes
Survey	Who, What, Where, How many, How much?	No	Yes
Archival analysis	Who, What, Where, How many, How much?	No	Yes/No
History	How, Why?	No	No

Table 4 - Qualitative research strategies, adopted from Yin (2018)

When comparing the case study with other research approaches, case studies are preferred when 'how' and 'why' research questions are being asked. Furthermore, case studies are preferred when there is little to no control over events that the researcher is trying to study, and when the research focuses on events that are happening in real life. As Yin (2018) summarizes, case study is an empirical method that is used to investigate and understand real-world cases. In other words, it is used to study contemporary events and relies on direct observations of such events (Yin 2018). Case studies are also “especially suitable for learning more about a little known or poorly” (Leedy and Ormrod, 2020). Most of the relevant research from the literature review was also using one of the 5 research strategies presented by Table 4. Ključnikov, et al. (2019) mention in their research that by using quantitative methods in their research about the factors of success in information security management in SMEs, they would face a risk of getting unreliable data from inexperienced respondents. Leedy and Ormrod (2020) also summarize that qualitative research can help with uncovering key problems or obstacles in different cases.

Even though the main research question doesn’t ask ‘how’ or ‘why’, this research is trying to investigate real-world cases, and is trying to learn about a little known or poorly understood phenomena. Therefore, considering the discussion and the facts above, the research questions and the goal of this research, the researcher believes that the most appropriate method to use to conduct this research is the case study.

Case Study

Case studies can be conducted in multiple different ways. Case studies can cope with situations where there is one, but also multiple sources of evidence. Yin (2018) classifies case studies in 3 different categories – explanatory, descriptive and exploratory. While there are distinct differences between these categories, the boundary is not always sharp. Each category has its own characteristics, but there are overlaps between them. Yin (2018) defines that the exploratory research is used to develop hypotheses and propositions for further enquiry, while the explanatory case study focuses on operational processes over time. The descriptive case study focuses on real world situations and how people and/or groups address these situations. Knowing the facts, the exploratory case study seems to be a great fit for what this research is trying to achieve and seems to be the correct method to achieve the goals of the proposed research.

The proposed approach to the thesis was of a relativist one. As summarized by Yin (2018), a relativist tries to capture the viewpoints of all participants or cases in the case study and focuses on how their different inputs benefit the topic of the study. This approach is beneficial and preferred due to the nature of the ISO 27001 standard. As described in the literature review, the ISO 27001 standard is a universal framework that can be interpreted and understood in many different ways based on the needs of an organization.

Prior to data collection, a researcher must decide whether the research studies one case or multiple cases. Even though as Yin (2018) describes, multiple case studies can be quite resource expensive and require time and a lot of effort, they can be quite beneficial for the result of the research paper as single-case studies are vulnerable to criticism about the uniqueness or access to the correct information with just a single data collection point. The researcher performing this research has access to multiple cases and potential informants.

Therefore, to make the most of the research and to deliver the goal of the research as best as possible, this exploratory case study uses a holistic multiple case study design. An

additional advantage of such an approach is that the research can make the most of a replication approach. A replication approach ensures that each case is the subject of a whole case study, in which evidence is gathered and conclusions for the study are made.

Further on, each conclusion is considered to be the information needed to be replicated by other individual case studies (Yin, 2018).

3.2 Research process

Generally, the research process is made of the 6 steps as shown in the figure below (Cooper &Schindler, 2013):

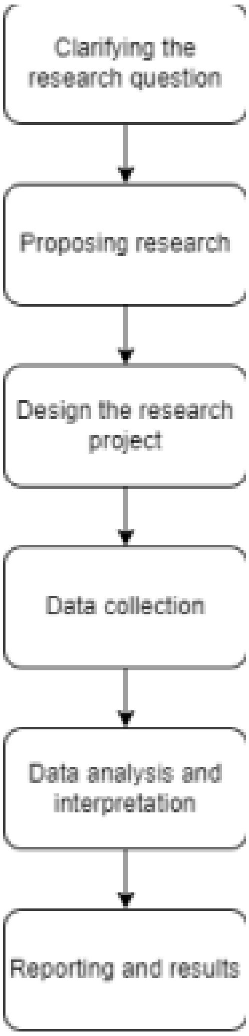
Clarifying the research question
Proposing research
Design the research project
Data collection
Data analysis and interpretation
Reporting and results

Figure 2 - Research process, adopted from Cooper & Schindler (2013)

Figure 2 above shows the overall research process used to form this thesis. The events and the results of individual steps of the research process are summarized in the list below:

- In the first step, an initial literature review was performed to find out if startups truly are having problems implementing security and ISO 27001 standards in their companies. Subsequently, a full literature review was conducted. This step focused on identifying problems and finding initial patterns in the literature. As a result of

this step, the chapter named 'Literature review', as well as the research question and the two sub questions were developed.

- During the second step, an initial proposal for the design of this research was proposed. This included the initial proposal for the methodology used in this research, as well as planning for data collection and data analysis. The chapter 'Literature review' was adjusted and refined to make sure all relevant literature is considered.

- In the third step, the research design is selected. This step resulted in the creation of a chapter named ‘Methodology’, in which the research method was selected and the details of it were described.
- In the fourth step, the data is collected by using the methods selected in this section. The data collection forms a chapter named ‘Data collection’ and follows the research process of multiple case study design outlined in Figure 3 below. Therefore, this section consists of multiple individual case study protocols.
- In the fifth step, the data is analyzed and interpreted. The data is analyzed by using the methods outlined in this chapter. Individual case study reports, as well as a cross-case report are forming the chapter ‘Data analysis’.
- The final step forms the chapter ‘Discussion & results’, in which the conclusions are formed based on the collected data, and the research questions are answered.

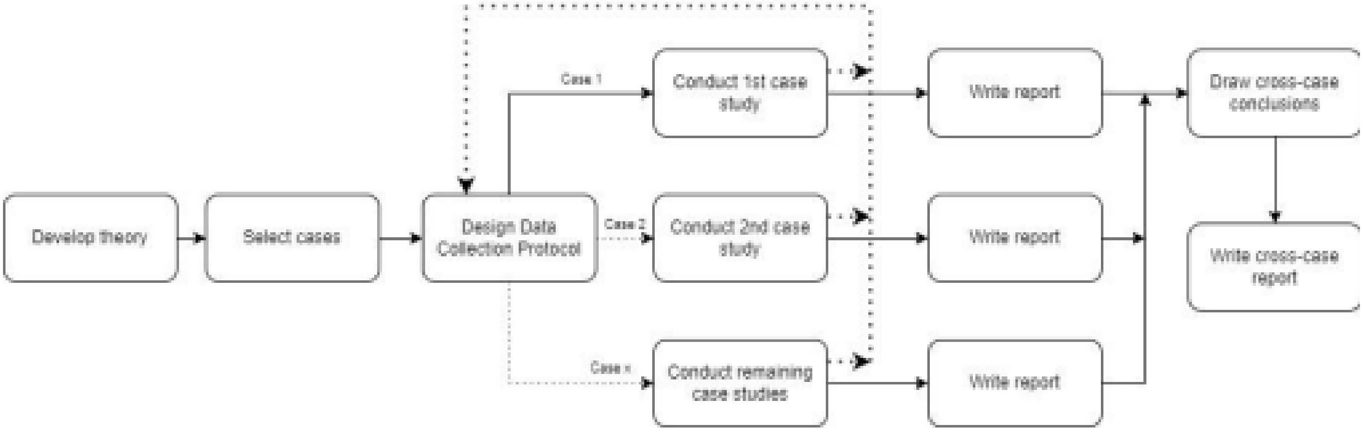

Figure 3 - Holistic multiple case study process, adopted from Yin (2018)

Figure - Holistic multiple cas

While the research process by Cooper & Schindler (2013) ensures that the thesis has a clear outline of the steps it should follow in order to fulfill its goal, more detail to steps 4 and 5 of the research process should be provided. The figure below originates from a multiple-case study procedure outlined by Yin (2018. It highlights the steps that should be completed while performing a multiple case study research in more detail, especially focusing on data collection and data analysis, which are steps 4 and 5 of the research process by Cooper & Schindler (2013).

3.3 Data collection methods

To minimize any potential criticism over data collection, it is important to answer the following questions (Leedy & Ormrod, 2020):

- What data is needed for this research?
- What is the source of the data?
- What is the means of obtaining such data?
- Are there any criteria for the admissibility of data?
- How will the data be interpreted?

Though the answers to these questions cannot be explained in short, they give a clear overview of the methodology used for data collection. Therefore, the rest of this section is a discussion of each question, while providing a clear overview of the data collection methods during this research.

As this research aims to follow a qualitative multiple case study design outlined in the previous chapter, qualitative data have been collected. According to Yin (2018), there are six sources of evidence in case studies – documentation, archival records, interviews, direct observations, participant observation, physical artifacts. All of these techniques can be useful for collecting data, but the degree of usefulness can vary based on the goal that the research is trying to achieve and the source of the data.

The data collection sources in this research were individuals and organizations. To fulfill the goal of this research, the thesis tries to understand what the bottleneck in the implementation of the ISO 27001 standard in startups is. Therefore, cases targeted for data collection are startups that have experience with the process of implementation of the ISO 27001 standard in their organization, or individuals with experience with the implementation of the ISO 27001 standard in startups. As the literature review specifies, the person that is running the implementation process is usually a person with an executive power in the organization, or an external consultant. Therefore, the thesis targeted individuals that also fulfill this requirement.

When collecting data, it is vital to distinguish between the various types of cases in this thesis. If the case is an individual, data from an organization should also be gathered to form a conclusion. However, the same applies in a reversed scenario. If the case is an organization, the data from individuals is also necessary. This is to ensure that this research indeed remains a case study, rather than some other method of qualitative research (Yin, 2018). The Table 5 below, adopted from Yin (2018), should give a clear overview about the relationship between the data collection source and the design of the research with different units of analysis, and what data does the research need to collect in order to stay relevant.

Data collection source / Design	**From an individual**	**From an organization**	**Unit of analysis (case study)**

About an individual	Individual behavior Individual attitudes	Employee records, interviews with supervisors & other employees	Individual
About an organization	How organization works, why organization works.	Personnel policies, organization outcomes	Organization

Table 5 - Data required to be collected from data collection sources based on the unit of analysis, adopted from Yin (2018)

Given the strengths and weaknesses of the sources of evidence shown in Table 4, interviews were the method of choice for the data collection. Interviews are a very valuable part of case studies, as they can suggest explanations of key events. (Yin, 2018). Case study interviews are often not tightly prescribed but tend to feel more informal (Leedy & Ormrod, 2020).

To deliver on the goal of the research, the interviews strived to find out information about the actual experiences of the startups or the individuals with the unit of analysis, which is the ISO 27001 implementation. The interviews attempted to uncover how the implementation process is understood by the startups and individuals, whether these, similar, or other steps have been followed and how. Furthermore, the interviews tried to collect data on the experiences and opinions of the individuals and the startups from the implementation process of the ISO 27001 standard. Lastly, the interviews aimed to collect data about improvements that the individuals and the startups think could be made to the process to make it easier for startups to implement.

Given the limitations of availability of the participants that this thesis has, the interviews conducted in this research are shorter case study interviews. While according to Yin (2018), the advantage of a prolonged case study interview is that a participant is often able to provide the research with more insight into the matter, and potentially access to other informants that could answer the research's inquiries better, time is a factor. Shorter case study interviews do leave less time for research to gather information, but as Yin (2018) says, these interviews tend to follow the case study protocol closely and the interviewees still remain open-minded. At this point, it is also important to consider the available resources this research has both for the data collection, but also for the data analysis part.

All the interviews have been recorded with the participant's consent. Recordings of the interviews provide more accurate data retention and an easier way of reflecting on an interview during the data analysis process.

Documentation may also be used as a source of evidence. Yin (2018) specifies that other formal studies related to the studied case can be used as a source of evidence. Therefore, to offset the limitation set by the number of available startups for an interview, the thesis has in the literature review already tried to expand the data collection sources to other formal studies that have been performed and have collected data about cases. The data sources in the documentation should however still conform to the same criteria as set by this thesis. Such documentation might reveal important insight about the research topic. This though might be difficult, as Table 6 suggests.

Source of evidence	**Strengths**	**Weaknesses**
Interviews	Targeted, insightful	Bias due to poorly constructed questions
Direct observation	Covers actions in real time, contextual	Resource consuming, narrow coverage, reflexivity
Documentation	Stable, exact, broad, not created as a result of case study	Low retrievability, access, biased selectivity
Archival records	Stable, exact, broad retrieva	biased selectivity
Participant observation	Covers actions in real time, contextual, insightful	Resource consuming, narrow coverage, reflexivity, bias
Physical artifacts	Insightful	Selectivity, availability

Table 6 - Six sources of evidence with their strengths and weaknesses, adopted from Yin (2018)

3.3.1 Case study protocol

To be as prepared as possible for the data collection during interviews, especially in a multiple-case study such as this one, a case study protocol is required (Yin, 2018). The protocol serves the purpose of guiding the researcher to stay on topic and ask the correct questions and react to various situations in a manner that is beneficial for the research. This protocol has been be constructed for each case and consists of 4 parts. Each part of the protocol is focused on different areas of the data collection procedure. (Yin, 2018)

Part 1 – an overview of the case study

- Background information about the case study
- Rationale for selecting the case
- The propositions or hypotheses being examined

Part 2 – data collection procedures

- Identification of sources of data
- Prior to conducting interviews, candidate screening shall be performed, using one phased approach. This approach ensured that the screening shall be short, and

effective, and should not take vast amounts of resources (Yin, 2018).

- Data collection schedule

- Desired location for data collection
- Data format

Part 3 – protocol questions

- These are the specific questions researcher must keep in mind while collecting data; - Yin (2018) defined different levels of questions, shown in Table 7. In part 3 of the case study protocol, only questions on level 2 should be asked. It is important to distinguish and keep this balance, as the researcher also aims to ask questions at level 1 during other parts of the interview, to make the participant feel good, and keep him in the open position rather than in a defensive one (Yin, 2018). The questions on level 2 are questions about each case which represent the researcher's line of enquiry. This partially defines the criteria for admissibility of data. The data analysis section further discusses what data has been be used, and what are the criteria for admissibility of data.
- When forming the interview questions, it is important to have in mind the goal of this research.

Level of questions	**Description**
Level 1	Questions asked to specific interviewees.
Level 2	Questions about each case representing researchers' line of inquiry.
Level 3	Questions asked about pattern findings across multiple cases.
Level 4	Questions calling on information beyond case study evidence (other literature).
Level 5	Questions beyond the scope of the study

Table 7 - 5 levels of questions (Yin, 2018)

Part 4 – Outline of the case study report

- Format of the case study report should be considered to avoid misalignment later on in the process about the format and the quality of data.

3.4 Data Analysis

"Qualitative data analysis is an iterative process, and thus a good qualitative researcher is apt to go back and forth a bit among the strategies" (Leedy & Ormrod, 2020)

Data analysis can be tricky, as there are no computer tools that perform a finished analysis, as is the case with quantitative research (Yin, 2018). In qualitative designs, data collection, data analysis and data interpretation are considered three separate steps, but in most designs, they are closely coupled (Leedy & Ormrod, 2020). Additionally, Leedy & Ormrod, (2020) also state that it is important to begin thinking about data analysis early in the data collection method. This was demonstrated in the previous section when talking about part 4 of the case study protocol. It is therefore advantageous to have a good strategy to perform data analysis early in the process.

Leedy & Ormrod (2020) propose data analysis based on Creswell (2013) data analysis spiral. As shown in Figure 4, this spiral is constructed of four steps which help the data to be processed from raw until the result, which is the final report. The first step in the data spiral is to organize the data and break them down into smaller units. Second step is to read carefully through the data to gain an overall understanding of the data. Third step consists of categorizing the data into multiple themes. Lastly, in the fourth step, the data should be summarized for readers to read, which often includes propositions or hypotheses that describe the relationships between the individual themes. Leedy & Ormrod (2020) specify that the final interpretations of data can be done in a variety of forms, such as tables, figures, and other compact ways of data presentation.

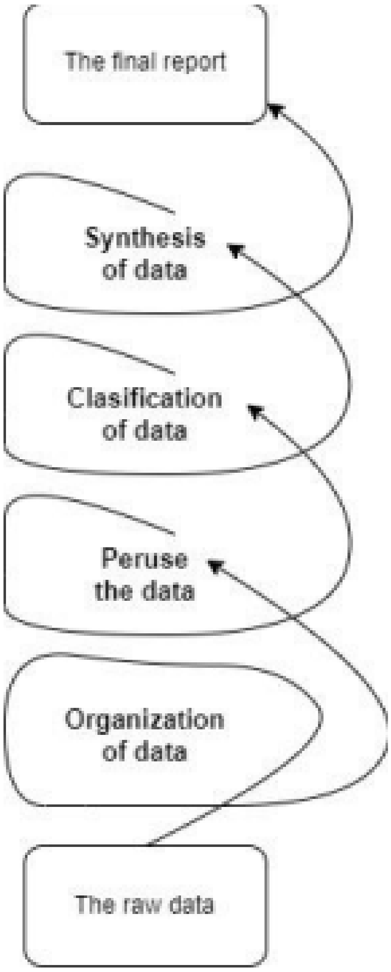

Figure 4 - Creswell (2013) data analysis spiral, adopted from Leedy & Ormrod (2020)

Yin (2018) also defined five analytic techniques that can be used to analyze collected data in a case study. Pattern matching is one of the five analytic techniques. To support the data analysis spiral defined by Creswell (2013), this technique has been used. In an explanatory case study, this technique is highly relevant, as it can help relate the patterns to questions. Pattern matching directly slots in the third step of the data analysis spiral but does not have to be limited to it. Pattern matching was used to find patterns and analyze the data both between the individual cases, but also between the cases and the literature review. Furthermore, it was also used to help draw conclusions in step 4 of the research process.

As mentioned in the data collection section of this thesis, the interviews tried to find out information about the actual experiences of the startups or the individuals with the ISO 27001 implementation. The data analysis methods mentioned just above helped the research to achieve the goal by analyzing the data in depth and comparing the data with how the literature review sees the process of implementation of the ISO 27001. Furthermore, it allowed the thesis to find patterns in the data and suggest changes and improvements to the implementation process of the ISO 27001, as well as offered learnings about the implementation.

4. Data collection

This section presents the reader with three case study protocols based on the case study protocol by Yin (2018) shown earlier in the thesis. Since this thesis aimed to collect data on the experiences and opinions of the individuals and the startups from the implementation process of the ISO 27001 standard, and data about improvements that the individuals and the startups think could be made to the process to make it easier for startups to implement, case study protocols served as a guidance in each conducted interview to gather as much relevant data as possible.

This section presents all the cases shortly. However, full case study protocols for all cases containing the detailed description of all cases, all the details about the case studies, as well as the interview questions can be found in Appendix B.

4.1 Overview of cases

The data collection consisted of conducting 4 interviews with 4 individual cases:

- Case A is an individual with vast experience and understanding of the implementation of security in startups.
- Case B is a startup working in the media, marketing and analytics industry in Copenhagen, Denmark. Due to various issues, this startup has been in the process of implementation of the ISO 27001 for a couple of years now.
- Case C is a Software-as-a-Service startup in Copenhagen, Denmark with around 40 employees working on site in their Copenhagen office and remote developers working in Bulgaria. Case C has successfully implemented the ISO 27001 standard a little over a year ago.
- Case D is a tech startup involved in the property management industry. They offer their customers, which are property professionals, a Software-as-a-Service solution for interacting with their residents. Case D has been going through the implementation process for some time now with the goal of being ISO 27001 certified. However, the implementation process was put on hold.

The thesis promised to not mention names of the interviewees, or the companies. However, to improve the readability of the document, the data collection and the individual reports refer to the individuals with pseudonyms listed in Table 32.

Case	**Interviewee pseudonym**	**Company pseudonym**
Case A	Isabella	n/a
Case B	William	Company B
Case C	James	Company C
Case D	Emma	Company D

Table 8 - Pseudonyms of cases

5. Data Analysis

This section first presents the case study reports for each case individually. Later on, the cross-case report is presented. The case study reports are constructed based on the process defined by the data analysis spiral by Creswell (2013). Each case study report first breaks the gathered data in smaller units. This is done by listing the main takeaways from the interviews, which are then summarized in a form of keywords.

After the organization phase of the Creswell (2013) spiral is finished, the perusal phase begins. The thesis can then gain a clear understanding of the data and start writing down some patterns that start to appear within each case study. The cross-case report is therefore the beginning of the third phase of the Creswell (2013) spiral by classification of the data. The cross-case report attempts to find similarities between the case studies by using the pattern matching process. To complete the cross-case report and gain a full understanding of the data, differences between each case are listed as well.

5.1 Case A report

First and foremost, Isabella agreed for the interview to be recorded. The interview with Isabella happened on time as agreed and was full of fantastic insights to the topic of implementation of the ISO 27001 standard in startups. Isabella demonstrated that they understand and have the knowledge of many implementations of the standard in multiple environments and highlighted a couple of potential shortcomings when it comes to startups implementing security either on their own, or with help from a consultant or other external party. These highlights are talked about in detail in this case report, and the findings from this report are taken further on to the cross-case report.

Understanding of the implementation

The interview started with an introduction to the topic of the thesis and what steps Isabella understands fall under the implementation part of the ISO 27001 standard. After a short discussion, it was agreed with Isabella that the implementation phase starts right after the project kickoff phase is finished and the scope of the ISO 27001 implementation is being decided on. For them, the project is finished, and the company is compliant as the policies and procedures are written. This directly reflects the first and last step of the implementation process presented in the literature review.

Management not interested

Isabella underlined that management support is vital for a project like this, but it can be quite challenging to receive it throughout the implementation of the ISO 27001 standard. Isabella thinks that the ISO 27001 itself explains well that the management support is required. They highlighted that it can be difficult for management to support such a project in general, as they don't necessarily see the benefits of having the ISO 27001 implemented. Isabella directly compared this to the perception of insurance, as it is something you should have, but you can theoretically live without it.

In her experience, it is usually a single person from the management team that is the project owner, and the other members of the management team are not so interested in how the project runs. She highlighted that this can be a huge pitfall of the project and suggested that the entire management team is in fact a part of the implementation process. Quantitative metrics such as number of breaches happening, weak password, fines that could be imposed if a breach happens, more awareness about security should be raised to the management team from the beginning of the implementation process and why the organization needs the ISO 27001 standard in general. Moreover, if there is a customer demand, Isabella thinks that that is the easiest way of getting management support to the project, as they can see quantitative metrics such as revenue as a reason to run the project at all.

Enforcing regulations

Regulations is another keyword that was mentioned by Isabella quite often. They mentioned that if there are regulations that are enforced, it can help companies to understand the need of projects like implementation of the ISO 27001 standard better. That could in turn help with management support, which greatly improves the chances of the project being a success in an organization.

It's a project

Isabella underlines that it is vital that startups treat this as a project. They clarify that the startups must have the resources allocated to run the project. Moreover, the employees should be informed that such a project is being run in the company and understand what the project requires and what people need to do in order for this project to be successfully delivered.

After the recording was finished, the case also highlighted that it is in their opinion vital to have a method that you use to run the implementation project. They said that if the companies do not have a method, it is very likely that the project will result in a failure.

Have ownership of the project

Isabella mentions that startups usually don’t have a person really having the ownership of the ISO 27001 implementation project, which can lead to the consequence of putting the project aside and not having the time to run it. The risk management side of the project suffers in that regard, as the risks that have been identified do not get enough attention, and the company is in a threat of failing the project. This can also have a profound effect on the treatments that are selected to mitigate the security issues. If there is no owner of the issues, the controls might never be implemented.

The problem of the standard

In Isabella's opinion, while the ISO 27001 standard is nice because it is really brief, it is also one of its weak points. They think that because the standard is brief and abstract, it leaves a lot of room and a gap from description to reality. That is why startups usually contact her, because she fills in that gap.

They also say that if there was a version of the standard that would zoom in on a smaller segment, or on a special type of company, it would be more relevant and less abstract for startups, which would definitely help the startups a lot.

2 sources of motivation

Isabella mentions that a lot of companies do not have prior knowledge, and they only know about the ISO 27001 standard because their customers are requesting some tangible proof of security. This is why they start the implementation process and can later struggle if no external help is provided. The biggest reason why they usually cannot run the implementation process alone is the fact that they don’t know where to go, and what steps to take next. Isabella thinks that startups, with a little bit of knowledge and interest in security could actually successfully run the implementation project alone, but the lack of support on what steps should be taken next is missing.

Isabella supports that fact by stating that in their experience, there were startups that did have some prior knowledge of the ISO 27001 and they either knew what to do, but only to a certain degree, or they got stuck somewhere and needed guidance with what steps should be taken next. She highlighted that startups tend to over complicate the project, and that usually one of the reasons they are called in to a project like this. She mentions that it is important for startups to have a methodology, which they often lack, and she brings that knowledge in.

Lack of support by the standard

Isabella says that people understand why the risk assessment is a part of the ISO 27001 implementation, but they have trouble figuring out what are the actual assets they have in an organization and the dependencies of those assets on one another. It was clear for Isabella that the ISO 27001 standard doesn't provide enough support for this problem, and it could be easily solved by providing startups with explanations of what an asset is and how it can be coupled with other assets in an organization.

Culture change

Isabella disclosed that there is usually a big gap between the people that are running the implementation of the ISO 27001 standard and are interested in the project, and the rest of the organization. In their experience, it happens very often that employees refuse to accept the change in the way they work and more importantly the change in culture which the implementation of the ISO 27001 standard inherently brings into the organization. She thinks that in general, it is very hard for people to change behavior.

When asked if she thinks this is something that is a part of the training stage, which in the understanding of the thesis comes after the implementation, Isabella said that it is possible,

but change management should be taken into consideration when the scope is being set. She says that this is something that is not highlighted in the ISO 27001 standard itself, and the people running the project usually don't realize how big of a cultural change the implementation of the ISO 27001 standard can bring into the organization.

She also thinks that including more people in the implementation phase could help with the culture change that the ISO 27001 standard brings, but the availability of those people might vary. When asked about how many people are usually involved in the implementation process, the answer wasn't quite straightforward. They generalized that it is usually the project owner and one person per each department.

A potential solution for this problem, according to Isabella, is to implement the ISO 27001 into the organization with the goal of implementing as many technical controls as possible. While this reduces the number of things employees have to remember to do when later on working according to the new security standards set by the ISO 27001, it doesn't solve the problem of culture change in an organization.

Quality of implementation

When asked about the quality of implementation of the ISO 27001 standard, Isabella thinks that once the company is done with the implementation process, the quality of the outcome is usually good, because once the ISO 27001 standard is understood, it is written well enough that the quality of the product resulting from the implementation phase is good. Another reason is that the startups understand that if the ISO 27001 compliance is requested by their customers, they must deliver a project outcome that will be satisfactory for them, otherwise they would have to re-do the project, or at least parts of the implementation again.

Policies / procedures

Whenever Isabella is working with a company on writing policies and procedures, she comes with a set of templates that she uses for all companies she is working with. She says that this is something that could definitely be standardized, because while there are some changes to the templates in wording, and some specifics when it comes to the content of the policies, it would be very advantageous to have such templates available for all startups that want to go through the implementation of the ISO 27001 standard.

Policies / Procedures - Help of systems & platforms

When asked if a system or a platform would exist which would guide the startups through the implementation process, her opinion is that it would obviously be a great help and could solve most of the problems, it doesn't solve the biggest issue startups have that they just don't have enough time. She suggests that an employee should still be dedicated to this project, if not full time than at least 20 hours a week. That would solve the problems of time, which would ultimately allow the startups to focus on other things.

Table 9 below provides the overview of keywords identified by the case with reference to the implementation steps.

Implementation step	Keyword
Getting management support	Management not interested, Enforcing regulations
Definition of the ISMS scope	It's a project, Have ownership of the project
Definition of a security policy	The problem of the standard, 2 sources of motivation
Risk assessment	Lack of support by the standard
Risk management	Lack of support by the standard
Selection of controls	Culture change
Statement of applicability (SOA)	Quality of implementation
Policies / procedures	Policies / procedures, Help of systems & platforms

Table 9 - The overview of keywords in relation to the implementation steps identified by case A

5.2 Case B report

First and foremost, William agreed for the interview to be recorded. The interview with William went very well, the interviewee was very open to discuss questions directly regarding the status of the ISO 27001 implementation in their startup and was very honest throughout the whole interview about how the implementation process went, and what went wrong. This interview was highly valuable for the thesis, as the thesis can look into the details and paths of a company that took significantly longer to go through the implementation process and learn based on those mistakes.

Currently, the company considers itself ISO 27001 compliant, but William admitted that they still have some work to do with regards to the documentation that the ISO 27001 standard requires.

Understanding of the implementation

For William, the implementation phase of the ISO 27001 is finished when all the processes and procedures are in place so that the company can follow those. Therefore, the implementation phase for company B ends with the implementation of policies and procedures.

Management learnings

Throughout the interview, management was discussed quite often, as all topics seemed to circulate back to that topic. William mentioned multiple times in their interview that the implementation project of the ISO 27001 was handled internally, started by their former CTO, and an employee. Halfway through the project, both the CTO and the employee had left the company. When the CTO left the company, the project was handed over to the

management team, particularly the CEO. However, it was unclear how this handover happened and whether it was sufficient. The management team failed to pick up on the project. William mentions that this was for multiple reasons, such as lack of skill, lack of knowledge, and lack of time.

He thinks that in order for the management to be behind and fully support a project like this, they need to understand that while it requires a lot of resources, it also comes with a lot of benefits on the other side. He mentioned that they did struggle with it, but over time the management realized that implementing the ISO 27001, or security in general, is something that will bring benefits in the future.

Ownership of the project

As mentioned above, once the former CTO had left the company, the project stopped, or at least struggled to move forward. William thinks that to lead the implementation process, one needs to have at least a bit of a technical understanding, which the CEO lacked at the time. After a little bit of time, the project was bouncing around between multiple departments, while not progressing because as William specifies, no one from the company really took an ownership of the project. William thinks this was in fact one of their biggest problems while running the project. There were only one or two people involved in running the project, and once they had left, there was nobody to pick up the project and move on with it. He expressed the opinion that multiple people have to be involved in a project like this in order for the project to be successfully delivered and implemented.

William also mentioned that for them as a startup, it was really difficult to hire someone to run the project for them, but it was also really difficult to find the person that could run the project within their employees.

Roles and responsibilities are unclear

It was mentioned that what is making the implementation process very difficult is the fact that the ISO 27001 doesn't provide enough guidance for the startups, especially in the phase of forming the security organization and making sure that everyone understands what their role and responsibility within the ISO 27001 is.

Motivation

Company B did not start the implementation project of ISO 27001 standard because it was a requirement by the customers, but because they realized the importance of security early in the company's existence and wanted to get ahead of the curve. Their goal was to ensure a high level of security throughout all of the company's departments and different jobs.

Missing guidance

As mentioned previously, the implementation process of the ISO 27001 standard was handled internally in this startup. William expressed a belief that if they had some sort of support system or a platform that would be affordable and would guide them through the implementation process of the ISO 27001, it would make a massive difference to the outcome and the duration of the project. In addition, they again feel that providing template documents would benefit the project quite extensively.

They also mentioned that the company is missing a support structure for after the implementation of the ISO 27001, which would actually be set up during the implementation. William feels that the implementation process doesn't look forward in the future, which can lead to them forgetting about actions or tasks that need to be performed in order to stay secure and ISO 27001 compliant.

Given that this startup had access to a platform that to the knowledge of the interviewer did have some of the functions that were requested and mentioned just above, a question was raised about that. The answer from the interviewee was that yes, while the platform does sell a solution with some functionality, they also send a consultant to come in and take a look at the organization, which in his opinion wasn't helpful for company B. The reason for this was that the consultant and the platform were really distant in the way they were working from what the organization required. While they promised to deliver on the stuff that was mentioned just above, they failed in doing so.

Risk treatments not the limiting factor

William specified that the company was in no way limited by the risk treatment plan and the treatments that the plan suggested should be done. The only problem was with actually enforcing those treatments into the organization, because some of the treatments were human based, and he mentions that it can be difficult to implement and monitor these treatments.

Technical skills of employees matters

William thinks that when employees have a better technical understanding, for example the people working in development, or even people working in sales but with interest in information technologies, it is easier for them to understand the implications of not being compliant. This company, according to William, had a lot of people historically that were not very technical. It was apparently much harder to get these people to understand the importance of security and the implications that working in an unsecure way might have. William added that they think this applies not only to the ISO 27001 standard, but any other guidelines in regard to the security that a company might have. They highlighted that they think this is a problem especially in companies that work with cutting edge technology.

The company tried to solve this problem with more fine-grained education for the non technical users, but inherently once the problem was identified, the company adjusted their hiring process. Currently, William mentioned that company B has very few non-technical staff, and those few employees are guided, supported, and almost forced to work securely because of the environment around them.

Company B has also identified the need for technical controls. William mentioned that whenever they identify that an individual doesn't have the necessary security practices that are required by the company, they simply cut their access or implement some measurements that force the employees to work securely.

ISO 27001 is too general

William mentions that while the ISO 27001 standard is written in a very nonspecific way, and there are parts of the ISO 27001 which do not apply to tech startups these days, it would be very hard to construct something too specific. Instead, they suggest splitting the ISO 27001 standard into smaller batches, and each batch would focus on a different area of the business. He provides an example of having an area that focuses specifically on cloud related security infrastructure, another area that focuses on disaster planning, etc. He thinks that with a structure like that, they could also better delegate the responsibilities for the security measures within the company.

Another thing that was mentioned that makes the implementation process very difficult is that the ISO 27001 doesn't provide enough guidance for the startups, especially in the phases of forming the risk assessment, or forming the security organization and making sure that everyone understands what their role and responsibility within the ISO 27001 is.

The implementation doesn't consider the future

William expressed that even though there are problems with the implementation process that were mentioned previously during the interview, they find the problem of the implementation phase not looking into the future highly annoying. He says that it is great that the ISO 27001 implementation process produces a lot of policies and procedures for the organization to be secure, but it is then hard for the organization to prove to their customers that they really are. He says that there is no standard way of providing other stakeholders the security measures that are applied and came out of the implementation process in an easy to provide and understand way. He mentions that each customer or potential customer has their own way of assessing security in other companies, and it becomes a lot of unnecessary work.

Creation of policies / procedures

William mentioned that finding out what the technical measures are and enforcing them afterwards was not the biggest challenge for the organization. He mentions that the biggest challenge they had was with the business-related part of the ISO 27001, for example the disaster recovery plan. He says that it was difficult to come up with a good disaster recovery plan, when they do not know how to enforce this plan on the organization when a disaster actually happens. William thinks that it would be beneficial for them to receive a blueprint or a template with these business-related documents, because they feel that for startups these documents actually do look pretty similar.

Table 10 below provides the overview of keywords identified by the case with reference to the implementation steps.

Implementation step	**Keywords**
Getting management support	Management learnings
Definition of the ISMS scope	Ownership of the project, Responsibilities are not clear
Definition of a security policy	Motivation
Risk assessment	Missing guidance
Risk management	Missing guidance
Selection of controls	Risk treatments not the limiting factor, Technical skills of employees matters
Statement of applicability (SOA)	ISO 27001 is too general, The implementation doesn’t consider the future
Policies / procedures	Missing guidance, Creation of policies / procedures

Table 10 - The overview of keywords in relation to the implementation steps identified by case B

5.3 Case C report

James agreed for the interview to be recorded. The interview with James happened with a slight delay, after which the interviewee actually stayed for a little longer than initially agreed. This was great, as rushing an interview could result in lack of data that could have been otherwise gathered and the thesis could benefit from. James provided a view into a successful implementation process from the management perspective and how management sees and understands the standard and the implementation process.

Understanding of the implementation

When trying to set the scene of what implementation actually is, it was very interesting to find out that for James, the implementation of the ISO 27001 standard never ends. We were able to agree that the implementation part starts with setting the scope for the implementation of the ISO 27001 standard into the organization, but James was convinced that from their perspective, the implementation doesn’t stop with finding out what the treatments are, but actually implementing the treatments. Their understanding was that since there can be new threats and therefore treatments of vulnerabilities at least every year, implementing the mitigation techniques in the organization are in fact part of the implementation process as well.

Fines are not enforced

James admitted that they have struggled with support of the other members of management. When asked why that is, James simply pointed out the fact that ISO 27001 comes at a high cost, but there is currently no way of showing to the management team that not having any security implemented can come at even higher costs. A follow up question was raised - why the management doesn’t understand this when they are presented with a risk that could potentially ruin their business? The answer to that question was that they are not afraid of such fines, because such fines are not currently being enforced. Even though there are a couple of examples of companies receiving fines for leaking data, they do not believe that it could happen to them at all, or that they would receive a fine. Therefore, they do not understand why they should put resources into a project like the implementation of the ISO 27001 standard when there is no clear benefit for the business. They suggest that more quantitative data such as how much PII data is laying around the business and calculating what fines would result from that might help the issue. But it was clearly stressed that unless fines are actually being enforced and applied on companies in the real world, the management teams will not want to put resources into the project themselves. The situation might change when the company has a clear need to have a standard like the ISO 27001 implemented.

The roles are not described

The ISO 27001 standard defines that there should be a security organization created but it doesn’t define what the individual roles are supposed to do, and what their responsibilities are in detail. While James as CISO says that he didn’t have a problem understanding what the responsibilities are, partly because their interest in security and partly because it somewhat came naturally, it could be beneficial for other people that are implementing the ISO 27001 standard to understand what it is they are supposed to do in the future, and what responsibilities come with the new role.

No external help required

James thinks that the implementation of ISO 27001 doesn’t require any outside help, startups barely have the resources to perform what they describe as a huge amount of work during normal operations. But he argues that while it is obviously beneficial for startups to have an external consultant with experience to come in and help the startup to run the project, if enough natural interest in the topic sits within the company already, then it is not required. He summarizes that if the startup doesn't have the money to pay for something like an external consultant, it is entirely possible to do it without external help.

Split into multiple phases

The implementation in this company was run as a project, with an external consultant. James thinks that the project was successfully implemented because it was split into multiple parts or phases. and people were able to understand the changes to the organization more easily

Motivation

According to James, there can be two reasons why startups or companies in general might want to implement the ISO 27001 into their organizations. It can be because they want to, or because they are forced to by pressure from outside stakeholders. James thinks that if startups implement ISO 27001 because they want to, they are not going to do a thorough job because they do not have the pressure from the outside. But if a pressure from outside stakeholders is introduced, and ISO 27001 is implemented to boost sales with security, the amount of work increases because the ISO 27001 implementation needs to deliver the results that the management and the outside stakeholders are expecting.

Tools / platforms do not support the security policies

The tools that are used and that are company critical for the organization do not, in James' opinion, support the security requirements that the company C has. That incurs a lot more resources required to build other workarounds, since these systems cannot be easily replaced by other systems. This creates a problem because as stated many times before, the resources in a startup come at a very high cost to the organization.

In James' experience, the platforms either need to enforce the policies and procedures so that the employees go around the security requirements, or there need to be other tools in place such as storage or email scanners that actually quantify how much sensitive or PII data is which employee storing unnecessarily if a company wants to really implement the ISO 27001 standard fully.

Culture change

When asked about how the employees took on the culture change that came with the implementation of ISO 27001, James was very unenthusiastic. He mentions that it is close to impossible to change people's behavior if the standard doesn't directly impact them. He states that their sales department simply could not and still do not understand why they need to work with this new set of rules, when they thought they are not impacted by any controls. While the opposite is true, and the sales department does deal with a great amount of PII data and need to explain to their customers how security and data is being handled in this organization, they thought it is irrelevant to them because what they are talking about doesn't actually affect them directly. They simply cannot understand the security restrictions that are put on them which obviously can and do slow down the work they are doing.

On the other hand, when it comes to more technical people that understand or have passion in security, there was no culture change problem. Company C outsources their development in the south of Europe, and therefore the development team is not sitting with the rest of the organization in Copenhagen. But while this is true, the lead of development has a great interest in security and therefore there was no problem with implementing security or making decisions based on security in development.

Enforcing technical controls

Company C has considered themselves ISO 27001 compliant for more than a year now. However, James points out that some requirements of this ISO standard are a burden to go through. An example they provided is the requirements of management meetings, even though management is almost seen as regular employees in terms of how they need to follow the security policies and procedures the ISO standards sets. He says that if there is work done and if security is properly introduced into all processes, which they agreed currently is not, only then it can be much more of a pleasure than a burden since that is the way company operates.

When asked if the scope could have been just the company software as a service platform, or just the Copenhagen office, he specified that if they wanted to be serious about the implementation of ISO 27001, they needed to implement it in the whole organization. He clarified that it would be much easier to implement the ISO 27001 just on the software-as-a service platform. But if they would have done that, they would never be able to be fully compliant with the ISO 27001.

It is important to know what to do next

James points out that for startups, it is important to understand what to do next. He mentioned that they know about a couple of companies that wanted to use an online platform, which aims to help companies to become ISO 27001 compliant. While the startups, including this one, did not buy their policy templates solution which gives them templates of policies they can use to write them faster, company C bought their calendar tool, which automatically spawns events into the calendars of the employees involved in the project. That way they do not forget about anything, and they know exactly what to do next with the ISO implementation, but also after that.

Treatments not limited by cost

James specifies that while the ISO was misused to replace some platforms that otherwise would be removed, money or resources was not considered when treatment strategies were being chosen.

Implementation doesn't consider the future

James specified that even though the implementation part was great, and in their opinion is not very difficult to be compliant, it fails to think about the future. What they meant by that future is that while the implementation phase produced policies and procedures, it still doesn't save the company from standardized questionnaires by their customers, which often make no sense. He would like to see this considered in the implementation phase, so that their customers can more easily identify what security measures are in place, and then ask questions if they have any.

Documents were not a problem

James also mentioned indirectly that because they were running the project with the consultant that had an understanding of what the mandatory documents are in the ISO 27001, he trusted that they are going to have all of them by the end of the project. Moreover, this also ensured that the consultant was able to guide the company into what the mandatory documents need to look like.

Table 11 below provides the overview of keywords identified by the case with reference to the implementation steps.

Implementation step	Keywords
Getting management support	Fines are not enforced
Definition of the ISMS scope	The roles are not described; No external help required, Split into multiple phases
Definition of a security policy	Motivation, Documents were not a problem
Risk assessment	Tools / platforms do not support the security policies, It is important to know what to do next
Risk management	Tools / platforms do not support the security policies, It is important to know what to do next
Selection of controls	Tools / platforms do not support the security policies, Culture change, Enforcing technical controls, Treatments not limited by cost
Statement of applicability (SOA)	Implementation doesn't consider the future
Policies / procedures	Documents were not a problem

Table 11 - The overview of keywords in relation to the implementation steps identified by case C

5.4 Case D report

Understanding of the implementation

Given that Emma, the COO of this company has a background in legal matters and some experience with the ISO 27001 implementation from previous job experiences, they had a pretty good understanding of what is meant under the implementation of the ISO 27001 and what steps does the implementation stage contain. She understood the implementation phase exactly as this thesis. Therefore, it was very easy to get the same understanding around the topic of ISO 27001 implementation.

Management support easier

Because the project is run by the COO, it seems that the company doesn't seem to have any problems with management support of the project. Emma mentions that because she is the co-founder, and she has experience and background with legal matters, the other members of the management team trust them and support the project. She also mentioned that sometimes, the other members of the management question the need for security in the company, as the implementation takes a lot of resources. However, the COO reiterated that because they do have a strong experience and decision-making position in the company, they can easily answer the questions or push them back.

Include the whole organization

Emma points out that for them, it is more important to include the entire organization in the project rather than rushing through the implementation without the employee sign off and awareness. The project could have continued without the involvement of the development team, however, she pointed out that they want to get the input and have the acknowledgement of the project within the development team as well. Company D believes that is the only way of having security actually implemented in all of their processes.

Emma also pointed out that the company totally understands why the ISO 27001, or security in general needs to be implemented. She doesn't seem to have any opposing people within the organization that would be strongly against having security implemented in their processes.

Hiring a consultant

The COO believes that while with their knowledge they would be able to complete the project on their own, they are planning to hire an external consultant in the future. She thinks they will need the consultant for wrapping up the project and actually making sure that they have done everything that was required by the ISO 27001 standard. This makes sense given that their goal is to become ISO 27001 certified.

Roles and responsibilities necessary

When asked about the definition of roles and responsibilities, Emma mentions that they currently do not have people designated for various security roles. However, it seems that Emma doesn't have a problem understanding what the individual roles are. Emma is the one currently running the project, however as mentioned above she is trying to include the entire organization in the process so that everybody understands what is going on. She points out that in the future, she will have to delegate the security roles. She thinks that while she is trying to include the entire organization, company D will still need to educate the individuals that will be assigned to certain security roles.

Motivation

There seem to be multiple motivations for implementing the ISO 27001 standard into company D. First of all, because of their background, the COO of the company highlights that it is in her and therefore the company's DNA to implement security in their organization. Moreover, she thinks that having the ISO 27001 implemented can help them with selling their product better, even if it is not the main selling point for their product.

Methodology made it easier

When asked if they struggled with how to perform the risk assessment process, Emma mentioned that they have received a methodology template from a consultant in the beginning of the project. She says that they have followed the methodology that they received and because of that she hasn't struggled with this part of the project.

Development prioritized

The thesis was keen to understand why the ISO 27001 implementation project was put on hold. Emma pointed out that even though they have gotten through the risk assessment process fairly easily, they cannot proceed as the company prefers to focus all their resources on development. It is the feedback from the development team that is missing from the risk assessment, and the COO is waiting for that. Therefore, the project cannot proceed.

Humans make mistakes

In Emma's opinion, it is helpful to implement as many technical controls as possible to the organization. They argue that there is always a threat of human error. However, she also says that they count with this reality and understand it. She explains that the company doesn't believe they will have a way of policing everything that is going on in the organization, and therefore mistakes are to be expected.

Given that the company is not in the stage of selection of controls, Emma was not able to identify how the controls are going to be selected and what the criteria for such selection will be. At this point, Emma thinks that there are necessary controls to be implemented that they will have to cover the costs for no matter what. But she also mentioned that they will strive to find the balance between the cost of the control and the benefit of it.

Experience is helpful

Emma specifies that given their background, the ISO 27001 was not too difficult to understand, however they see room for improvement. However, she says that she completely understands if people struggle with understanding what the standard requires from companies, especially if they lack the experience with risk assessments and with the process of getting to compliance.

She suggests that the implementation could be made easier by having a clearly defined process of what needs to be done. She seemed to be missing the steps that should be performed next, and therefore would appreciate having more guidance in this matter.

Templates save time

Emma mentioned that they have received help from a consultant before the project began. The consultant provided the company with templates for policies and procedures. Emma mentions that because the format and some of the policies and procedures are the same for almost all startups, this was a huge help and a timesaver. She says that they can just use the templates, or easily plug their own data to those templates, to write the policies and procedures.

Table 12 below provides the overview of keywords identified by the case D with reference to the implementation steps.

Implementation step	Keywords
Getting management support	Management support easier
Definition of the ISMS scope	Include the whole organization, Hiring a consultant
Definition of a security policy	Roles and responsibilities necessary, Motivation
Risk assessment	Methodology made it easier
Risk management	Development prioritized
Selection of controls	Humans make mistakes
Statement of applicability (SOA)	Experience is helpful
Policies / procedures	Templates save time

Table 12 - The overview of keywords in relation to the implementation steps identified by case D

5.5 Cross-case report

The cross-case report follows the methodology of the data analysis by applying the third step of the Creswell (2013) spiral onto the data. The third step is to categorize data into multiple themes and find patterns between the data from individual cases in each category, or across the categories as well.

The cross-case report begins with the overview of the overall understanding of the implementation process. The collected data has then been categorized into 7 categories. Given the understanding of the implementation process by the cases and the fact that all keywords from the risk assessment category also logically belong and were assigned to the risk management category, these two categories are joined together. Apart from that, the categories mirror the 8 steps implementation process highlighted in the literature review. A summary section at the end of the cross-case report presents the issues and potential solutions identified by all the cases.

Keywords from the individual case studies are assigned to their respective categories based on the classifications in tables g, j, k, & l. Since some of the details can overlap between multiple implementation phases, it is entirely possible for one keyword to belong into multiple categories. This way, the thesis can clearly categorize the existing problems to the implementation process highlighted by the literature, and search for patterns between the multiple cases. Another advantage is that later on, the thesis will be able to see if the implementation problems from the literature review reflect the problems in the studied cases and offer potential solutions to the issues based on suggestions of the cases as well as the literature review.

5.5.1 Understanding the implementation process

It seems that the understanding of what the implementation phase of the ISO 27001 can vary. Initially, most of the cases had a different understanding of what are the steps that the implementation process actually contains. Case A and case B agreed that from their point of view, the implementation phase goes through the 8 phases, which the literature review identified from Lami (2013). Case D also seemed to understand the implementation process the same way. However, case C's understanding is that while the implementation phase can have multiple steps such as the ones highlighted by the literature review, it in fact never ends. They see the implementation of technical controls as a part of the implementation phase. Given that the ISO 27001 is constructed based on periodical reviews in the form of internal or external audit and constant improvements to the security of an organization, there might always be new technical controls to implement.

5.5.2 Category 1 - Getting Management support

Keyword	**Keywords from case**
Management not interested, Enforcing regulations	Case A
Management learnings	Case B
Fines are not enforced	Case C
Management support easier	Case D

Table 13 - Keywords included in category 1

The ISO 27001 standard calls for the support from the top management, which is often not received. All cases were questioned in terms of their experience with management support, the lack or the abundance of it, and how they think this could be improved.

Cases A, B and C concluded that management support was lacking during the implementation of the ISO 27001 standard. This is however a bit surprising. For cases B, C and D, the implementation project was started by one of the members of the management team. Case A mentioned that a person from the management team is usually the person with the initial idea for implementation of the ISO 27001. Only case D seemed to not have a problem with the management support. But it looks like there is a clear gap between the person that kicks off the project and the rest of the management team.

It became clear from all of the interviews that even though the implementation project often starts in the management team, it is most of the time only the single individual from the management team that is interested in the project. Other members of the management team often have the knowledge that such a project is going on in the company but fail to directly support it. The interview tried to examine why that is the situation by asking follow up questions on the subject. It seems that initially, one of the first issues might be the aforementioned cost of the project. The ISO 27001 is a project that requires a lot of resources to deliver successfully, and some individuals from the management team would often prefer to invest the resources somewhere else. Case D supports this by stating that they need to often use their strong position within the management team to defend against such arguments. Another reason is that the management of startups doesn't understand the need for ISO 27001, even if there is a clear need from customers of the startups.

Cases A, B and C mention that regulations are something that could force startups and their management teams to want to be secure. In their opinion, regulations, and laws such as GDPR are not truly enforced. They say that if such regulations regarding security and privacy are truly enforced and checked upon, the need for security will surely gain much better traction with the management team. They could then clearly quantitatively visualize what losses they are up against if a disaster should happen. Case C was one of the cases which seemed to highlight this a lot by stating that until the regulations and fines are actually enforced in the real world on smaller companies such as startups, the management teams in startups are going to ignore the threat. They argue for that statement by saying that currently, the likelihood of the threat in the form of a fine happening is simply too low.

5.5.3 Category 2 - Definition of the ISMS scope

Keyword	**Keywords from case**
It's a project, Have ownership of the project	Case A
Ownership of the project, Responsibilities are not clear	Case B
The roles are not described; No external help required, Split into multiple phases	Case C
Include the whole organization, Hiring a consultant	Case D

Table 14 - Keywords included in category 2

There are multiple things to be considered when the scope of the implementation is being decided upon. Setting the scope of the implementation is a key decision that affects the entire project. Once a startup decides what the scope of the implementation is, startups should start treating the ISO 27001 implementation as a serious project with allocated resources and a method that will be used to manage the project. Case C and D support having a clear methodology when running such a project. Case C points out that even if the ISO 27001 implementation is a resource hungry project, they had made the decision in the beginning of the project to split it into multiple phases. This approach made sure that there are clear goals with each phase, and the organization understands what changes are going to happen in each phase.

Furthermore, it is clear from the interviews that startups should make it clear who has the ownership of the project. The interviewees also suggested that in startups it would be beneficial if multiple people had the ownership of a big project like this due to the fast

circulation of people. Case B is a prime example of this. Moreover, improving the involvement of more employees in the implementation process was discussed, especially with case D, but it seems that in the majority of cases, neither the employees nor the management team get progress updates from the project lead. While this possibly comes down to the project management skills of the people that are running the project, the author sees this as a possible massive benefit to not only this project, but any project within the organization.

All cases argue that if the above is in place, it is entirely possible for startups to implement the ISO 27001 standard into their organizations on their own. At the same time, they point out that it is not that easy to have all this knowledge without a consultant in advance. Therefore, while it is possible, it seems that they are still missing guidance on what the next steps should be. In the experience of all cases, it is usually the next steps and the direction within the project that the startups struggle with. As case A, case C and case D sum up, if the project is run internally, startups most often do not know what steps should be taken next.

During the interviews, each case has been presented with the question regarding the quality of the output of the implementation phase. The thinking behind this question was that some startups might consider saving resources on the implementation phase by quickly running through the implementation phase with only mapping out the current situation and pretending that everything around their business is compliant and secure. Another reason for this question was that the startups only include a certain part of the organization in the ISO 27001 compliance project. This would greatly save on the resources that are needed to run the project, and it could be easier and faster to deliver a compliance status. All the cases agreed that whatever the motivation for the ISO 27001 is (which is discussed in the following category), there are two problems as to why implementing the ISO 27001 poorly would not be beneficial. Firstly, the interviewees argue that it would be almost impossible to do given how the standard is built up. Secondly, it would be a huge waste of money and time for startups. Case C mentioned that if they wanted to run the project with satisfying results, it was never a question to only include part of the organization. According to all cases, there would be no benefit of delivering an ISO 27001 compliance that could be considered a weak, rushed, or less of a quality product by the stakeholders. It is of course possible for some implementations of the ISO 27001 to be of a lower quality compared to some others, but there always are stakeholders, whether internal or external, that are looking at the quality of the outcome of a project. The internal stakeholders always want a return on their investment, and external stakeholders are comparing the status of security to their own standards. That is also the reason why case D plans to hire a consultant after the company will have been through all the implementation steps. They seemed to be looking for validation so that the outcome of the project is satisfactory. As mentioned multiple times, the ISO 27001 implementation is a resource extensive project to run in a startup, the expectations of such stakeholders always run high.

5.5.4 Category 3 - Definition of a security policy

Keyword	**Keywords from case**
The problem of the standard, 2 sources of motivation	Case A
Motivation	Case B
Motivation, Documents were not a problem	Case C
Roles and responsibilities necessary, Motivation	Case D

Table 15 - Keywords included in category 3

Among other things, the top-level policy required by ISO 27001 standard also requires companies to set up a security organization. The security organization should highlight key responsibilities and designate individuals to these security responsibilities. However, a pattern can be observed here. First of all, it is in the opinion of the interviewees that the standard doesn't describe what the responsibilities should be, or they at least didn't understand it from the standard. Case C points out that while they struggled with this problem only briefly, it would be beneficial if this was more clearly stated. Case B and case D on the other hand mentioned that to this day they do not have a clear security organization set up. This could indicate that it is another reason why the implementation of the standard is taking so long, as it is these two companies that seem to struggle with the implementation of the ISO 27001. People need to have ownership and understanding of their roles to security, otherwise it seems that the required tasks will not be fulfilled.

Another important thing for a company to consider when creating the top-level policy is the motivation for the project. As mentioned previously, there are two scenarios under which startups might consider being compliant with the ISO 27001 standard and therefore start the implementation process at all. It is either a requirement from the customers, or the understanding of the management that this is something that can create a competitive advantage, just as the literature review of this thesis showed. Together, the cases that were interviewed have experiences of both situations. Case A highlighted that most of the time it is the requirement of the customers that brings them to any implementation process in startups, Case C was also forced to the implementation of ISO 27001 because of the requirement of their customers. Case B and D, however, started the implementation process on their own, simply because they understood that security and compliance is something that they want implemented in their organizations. They also understood that compliance with this standard might bring them additional customers, resulting in bigger revenue. Both cases B and C confirmed after the recordings that they in fact were able to acquire customers more easily thanks to being compliant with the standard. The pattern

might then look set. Both case A and case C experienced implementations that were motivated by the customer requirements, with no significant delays to the projects reported. Case B and D on the other hand did not have the pressure from external stakeholders and the implementation has not been finished yet, even in a couple of years.

5.5.5 Category 4 - Risk assessment & Risk management

Keyword	**Keywords from case**
Lack of support by the standard	Case A
Missing guidance	Case B
Tools / platforms do not support the security policies, It is important to know what to do next	Case C
Methodology made it easier, Development prioritized	Case D

Table 16 Keywords included in category 4

Risk assessment and management are crucial steps to get right during the ISO 27001 compliance process. That is because these two steps are pivotal in setting the direction of the controls and policies that are going to be applied as treatments into the organization. This is further discussed in the following categories.

When it comes to the risk assessment, Case A argues that startups often have trouble identifying what their assets are, and how those assets affect one another. In their opinion, the standard fails to provide any guidance on this matter. Case B argues that they needed to invest in an online platform that was supposed to help them identify their key assets. Case D supports this by saying that they only understood how assets are identified because of the methodology that was provided to them and their prior experience. They also mention that in order to identify all assets, the entire organization needs to be included in the process, which they currently cannot do and seems to be the limiting factor.

Case C also argues that while they were able to identify the assets in the organization, the risk management is made difficult as the key systems and online platforms that this company uses to complete their day-to-day operations do not support the implementation of the required controls. They struggled with finding and choosing realistic treatment strategies during the risk management process that could actually be implemented to their systems and would reduce the risk levels of threats and vulnerabilities.

5.5.6 Category 5 - Selection of controls

Keyword	Keywords from case
Culture change	Case A
Risk treatments not the limiting factor, Technical skills of employees matters	Case B
Tools / platforms do not support the security policies, Culture change, Enforcing technical controls, Treatments not limited by cost	Case C
Humans make mistakes, Development prioritized	Case D

Table 17 - Keywords included in category 5

Another thing startups struggle with seems to be the implementation of controls introduced by the risk treatment plan. While the companies don't seem to struggle with the number of resources needed for implementation, they seem to struggle with the actual hands-on deployment of the controls into the organization and IT infrastructure. Case A and B suggested that one way to tackle the problem of people not wanting or forgetting to follow the security rules is the implementation of technical controls wherever possible. However, case B highlights that they had a tough time enforcing mainly human base treatments, which cannot be implemented and enforced by a system or a platform. Case D supports this by saying that they fully expect people to make mistakes, especially in places where it is not possible to enforce technical controls.

Case C also argues that the key platforms and tools the startup needs to use for their operation do not support the security requirements that the ISO 27001 implementation process required them to implement, as mentioned in the previous categories. They say that policies and procedures need to be enforced wherever possible so that the employees don't have to think about security, but instead would be working in an online environment that is secure by design. They mentioned that this problem introduces high costs, as they often struggle with finding workarounds to implement the necessary security controls. One might argue that if a platform doesn't support the security features, the company should avoid using it at all. However, case C mentioned it is the key platforms that the business relies on in order to perform their day-to-day operations, like the services provided by Google or Microsoft, that suffer from this problem. Therefore, in their case it was simply not possible to avoid the risk and use a platform.

Throughout all of the interviews, culture change was a huge talking point. Employees play a key role in the compliance with any standard. As Thomas Reid famously said, “the chain is only as strong as its weakest link” (Reid, 1786). Employees must understand and follow the policies and procedures that the standard introduces to the company in order for the company to remain secure. As case A states, culture change and change management is not something that the ISO 27001 standard itself considers, and startups then often don’t realize the changes that are about to be introduced. The implementation process is usually run by one or two individuals, out of which at least one is or should be within the organization. And according to case A and C, this is exactly where the problem arises. Case A states that generally, only one person per department is involved, and that involvement happens only throughout the risk assessment step of the implementation of the standard. They argue that change management is something that should be considered throughout the implementation process, especially if the project is implemented in a short amount of time. They express that this could be helped if more people from the organization were involved in the implementation process, but argue that the availability of those may vary, and therefore were not really sure if that would in fact solve the problem. Case D supports this by saying that without the involvement of the entire organization, the project cannot continue.

Moreover, case B adds an insight about people’s skills to the topic. Case B points out that company B has a big history of hiring and employing people that are not interested in technology, even though according to them the company itself develops and sells a very advanced technological product. They say that this had a massive impact on the implementation process of the standard, as it was much harder to get people that did not understand technology onboard with the fact that they now need to consider security, and work according to rules that are defined by the standard. Case C also mentions a very similar phenomenon, and adds an example with their sales department, which doesn’t seem to be able to understand why they need to work according to some security rules defined by the standard even if they don’t think they actually work with anything that requires security rules. On the other hand, all cases B, C and D highlighted that with their development teams, it was much easier to explain, understand and implement the security controls that are required by the standard. It was stated that because these employees have a greater understanding of technologies, they can also understand what the implications are if an incident would happen.

5.5.7 Category 6 - Statement of applicability

Keyword	**Keywords from case**
Quality of implementation	Case A
ISO 27001 is too general, The implementation doesn’t consider the future	Case B
Implementation doesn’t consider the future	Case C
Experience is helpful	Case D

Table 18 - Keywords included in category 6

It can be quite easy to blame the standard and say that if the implementation phase of the ISO 27001 is too difficult, it is not the startups that are doing something wrong but rather the ISO 27001 standard is unclear. But this doesn't have to necessarily be true, as the cases have pointed out. Case A, B agreed that the standard is too broad, leaves room for interpretation and many of its parts do not apply to tech startups these days. Case D also agreed with this, however they mentioned that given their experience they had no troubles understanding why the standard is like it is and what it requires. To tackle this experience gap, case A brought up an idea to divide the standard into smaller segments that would focus either on different set types of companies, a solution they identified as really helpful. Case B also proposed that the ISO 27001 should be split into more sections, and companies could pick which section they want to be compliant with. In the thesis' view, this alone would not solve the problems that the literature review points out. As case C and D underline, the ISO 27001 is in their opinion not very difficult to be compliant with. In the author's opinion, the Statement of Applicability is there to serve just the purpose of companies being able to pick which parts of the standard do they need to comply with, and which parts of the standard do not apply to them. Furthermore, writing a standard for each type of company would not only be very time consuming, but keeping such a number of standards up to date would, in the view of the author of the thesis, be an impossible job for the International Organization for Standardization. It seems that the problem lies somewhere else. Case B and C mentioned that each customer tends to have their own set of supplier security verification, and this is where most of the problems after the implementation phase seem to appear.

Even though this problem doesn't directly affect the implementation phase, it affects the life of the company after the standard has been implemented. Even though that is out of the scope of this thesis, it is good that it has been identified. The language used by the cases and the overall feel from the interviews when this issue was discussed shows that if there was something that could be done in the implementation phase that would unify the creation of the supplier security criteria, it would reduce the resources that are required to maintain the ISO 27001 in a company. As summed up by case C, it could become a much more pleasant standard to deal with in the future.

5.5.8 Category 7 - Policies / procedures

Keyword	**Keywords from case**
Policies / procedures, Help of systems & platforms	Case A
Missing guidance, Creation of policies / procedures	Case B
Documents were not a problem	Case C
Templates save time	Case D

Table 19 - Keywords included in category 7

All the cases mentioned that they struggled, or in the situation of case D expect to struggle with the creation of all mandatory and also non mandatory documents that need to be created for ISO 27001 compliance in the implementation phase. Case B suggested that they wanted to benefit from the online platform, which promises to offer templates of such documents. Case B complained that while some of the templates which were provided through the platform were useful, the business-related documents such as the disaster recovery plan were not. They think that with certain types of documents, especially the ones that the company is not able to enforce through technical controls, all startups are in a very similar position. Case A stated that they have templates for startups ready, and they use the same templates for all startups. It was the interviewers understanding that case C also used a consultant which provided these documents for the company. They seemed to be quite happy with that procedure. Case D suggested that their expectations to struggle lowered significantly once they were provided with templates for how the policies and procedures are supposed to look like.

All cases expressed that these documents could therefore be standardized and provided as ready to go templates that the companies do not have to touch. Case A stated a similar opinion, however they added that while the majority of the documents could be standardized, startups gain a better ownership of the documents when they at least slightly edit them to match the company language and culture.

But it seems that while online platforms haven't been helpful, and all of the startups haven’t mentioned an alternative that would be capable of satisfying the needs of the startups in the implementation process, not all love is lost for online solutions. All 4 cases reacted positively when a different hypothetical online solution was mentioned that would provide the key steps that are to be taken when going through the implementation project. On top of that, if a solution would exist where the documents are standardized, yet still editable, all the cases agreed that this would be something they would be potentially willing to put their money into. Case A however points out that even if such a platform existed, there should still be a person dedicated to this project internally with the amount of time that is required to run this project allocated, looping back to the importance of having an ownership of the project.

5.5.9 Summary

The cross-case report highlighted the experiences and opinions of all cases. By using pattern matching, it was possible to categorize the data into 7 categories. The categories were formed based on the implementation process derived from Lami (2013). To easily summarize what the takeaways from each category are, Table 20 summarizes the key issues that were presented by the cross-case report. Table 21 on the other hand presents the potential solutions that the cases suggest. As the keywords were already assigned to their respective categories based on the explanations of each implementation step by Braga (2018), the thesis was able to easily assign each issue to the category it was discussed in.

Implementation step	Issue
Getting management support	Lack of involvement of top management, Regulations not enforced, Lack of pressure from stakeholders
Definition of the ISMS scope	No ownership of the project, Lack of methodology, Missing guidance
Definition of a security policy	Unclear responsibilities
Risk assessment	Asset identification
Risk management	Systems don’t support security standards
Selection of controls	Deployment of controls (both technical and human), Lack of change management, Lack of employee involvement, Technical skill of people
Statement of applicability (SOA)	Supplier security audit not standardized,
Policies / procedures	Missing guidance on format of documents

Table 20 - Issues throughout the implementation process according to the case studies

Implementation step	Potential solution
Getting management support	Enforce regulations by giving out fine, Present potential losses
Definition of the ISMS scope	Include the entire organization, Split the project to smaller phases, Communicate & include the entire organization, Map out the steps to know what to do
Definition of a security policy	Clear definition of security roles
Risk assessment	Get & use methodology for asset identification
Risk management	Platforms must start to support security
Selection of controls	Consider change management, Implement as many technical controls as possible, Hire people with better technical understanding
Statement of applicability (SOA)	Standardize the supplier security evaluation process
Policies / procedures	Open-source templates

Table 21 - Potential solutions of the implementation issues according to the cases

6. Results

Table 22 below compares the issues that were identified by the literature review and the issues that were identified by the case studies.

Implementation step	**Issues identified by literature review**	**Issues identified by the cases**
Getting management support	• Lack of involvement of top management	• Lack of involvement of top management • Regulations not enforced • Lack of pressure from stakeholders
Definition of the ISMS scope	• Not necessary to implement it across the entire organization in one shot; • Project affecting the entire organization; • Education, knowledge, or pre existing experience is required in order to implement the ISO 27001 in a startup; • Lack of project planning	• No ownership of the project • Lack of methodology • Missing guidance
Definition of a security policy	• Lack of delegation of security roles within the organization	• Unclear responsibilities
Risk assessment	• Identifying the organization's assets;	• Asset identification
Risk management	• n/a	• Systems don’t support security standards

Selection of controls	• Emphasis only put emphasis on the technical controls; • Employees must embrace the new security controls	• Deployment of controls (both technical and human) • Lack of change management • Lack of employee involvement • Technical skill of people
Statement of applicability (SOA)	• The language and way the standard is written; • Standard not designed with startups in mind; • Maturity levels of ISMS	• Supplier security audit not standardized,
Policies / procedures	• Complexness of policies and procedures; • Problems with writing and implementing business continuity plans; • Misalignment or lack of mandatory documentation for the ISO 27001	• Missing guidance on format of documents

Table 22 - Comparison of the ISO 27001 implementation issues identified by the literature and the interviewed cases

The Table 23 below showcases the potential solutions to the implementation problems that this thesis has identified. However, it is important to better explain the context of what startups need to do to avoid the implementation issues. This also helped with answering the two research sub questions.

Implementation step	**Potential solutions identified by literature review**	**Potential solutions identified by the cases**
Getting management support	• Clarify management responsibilities and duties; • Include department managers • Present cost of no security	• Enforce regulations by giving out fines • Present potential losses

Definition of the ISMS scope	• Treat ISMS implementation as a project. • The scope in startups should be the entire organization • The project must have an owner • Work split into smaller phases / steps	• Split the project to smaller phases • Communicate & include the entire organization • Map out the steps to know what to do
Definition of a security policy	• Avoid conflicts of interest; • Combine multiple security roles to one individual in startups	• Clear definition of security roles
Risk assessment	• Methodology	• Get & use methodology for asset identification
Risk management	• Methodology	• Platforms must start to support security
Selection of controls	• Implement easy treatments first	• Consider change management • Implement as many technical controls as possible • Hire people with better technical understanding
Statement of applicability (SOA)	n/a	• Standardize the supplier security evaluation process
Policies / procedures	n/a	• Open-source templates

Table 23 - Comparison of the potential solutions to the ISO 27001 implementation issues identified by the literature and the interviewed cases

6.1 Summary of problems and solutions

Almost all issues highlighted by the literature review match the issues highlighted by the case studies, however there are some exceptions. It is therefore important to discuss each phase and highlight the differences. This section discusses each phase and compare the implementation issues highlighted by literature and the case studies. Furthermore, the potential practical solutions to the implementation issues are be discussed. 6.1.1Getting

management support

Both the literature and the cases identified that the lack of involvement of the top management is the major problem in this implementation phase and a threat for the entire project. The cases however added other problems, which are the facts that the regulations are not enforced, and that there is a lack of pressure from stakeholders, which can influence the success of the implementation project.

The solution to this problem doesn't seem to be simple, but both the literature and the cases have come up with interesting suggestions that would, in the opinion of the author of the thesis, definitely help the cause. The literature states that it should be clearly communicated, and possibly even written down what are the expectations from the

management team. The literature also points out that department managers can be included as the members of the management, as they can support the implementation of ISO 27001 within their departments. However, while bigger startups might have such structure and can take advantage of this advice, smaller startups still rely on the top management. Another solution that the literature and some of the cases agree on is the presentation of potential losses. Case A also argues that quantitative metrics, such as what is the number of breaches happening due to a weak security and how that could financially influence the startup might help massively But given that there are very little data to predict what the losses actually would be, case C heavily argues that this would not work.

To tackle that completely, the interviewees call for enforcement of regulations and fines. It makes sense that once the regulations are enforced and there are financial losses to be worried about, the management teams of startups will support and be involved in the implementation of ISO 27001 standard more willingly. That would also resolve the problem of lack of pressure from stakeholders.

Implementation issue	Solution
• Lack of involvement of top management • Regulations not enforced	• Clarify management responsibilities and duties • Present cost of no security • Enforce regulations by giving out fines • Present potential losses (cost of no security)

Table 24 - Summary of problems and solutions in implementation phase 1

6.1.2 Definition of the ISMS scope

As explained in the literature review, this phase is about setting the scope for the implementation. While that is important, the thesis has identified that it is also about project management. The literature explains that bigger scope doesn't necessarily have to mean more work. While the literature argues that it is not necessary to implement the ISO 27001 across the entire organization, it is directly contradicting itself by stating that this project does affect the entire organization. It was identified that the project affects the entire organization, in one way or another, and that seems to be something that startups fail to understand in this phase. All cases also demonstrated that in startups, it is only beneficial to implement the standard across the entire organization, otherwise they would struggle with actually being compliant. What the cases pointed out was the fact that it is beneficial to split the project into multiple phases. The cases have also identified that there is a clear lack of ownership throughout the project. Project planning is an issue that the literature has identified, with cases identifying lack of methodology. However, the cases have identified that they are missing guidance in terms of what steps should be taken next in the project. Therefore, it seems that both literature and cases seem to refer to project

management problems, that include ownership of the project and project planning, and the project execution.

Having a project lead / owner and treating the ISO 27001 implementation as a project are suggestions identified by both the literature and the cases. Moreover, splitting the project into multiple steps seems to be a solution that everyone agrees to as well. Having milestones throughout the project can give the project the feeling of success when each milestone is reached. It is possible to set the milestones according to the 8 implementation steps by Lami (2013), as this thesis did. It would then be much easier for startups to map out what should happen in each phase of the project. The author of the thesis is of the opinion that methodologies such as scrum would improve the implementation of the ISO 27001 from this perspective greatly. The advice of running the ISO 27001 implementation as a project by case A can really go a long way.

Furthermore, it has been identified that communication is key, and the implementation process should strive to involve as many people as possible. The involvement of all employees doesn’t have to be direct, but if a communication about the progress of the project to the entire company is present, it has the potential of easing the impact of the culture change that the standard brings with itself.

Implementation issue	**Solution**
• Project management ○ No ownership of the project ○ Lack of project planning ○ Unclear project goals / milestones	• Treat ISMS implementation as a project • Communicate & include the entire organization • Designate a project owner • Split into smaller steps (milestones)

Table 25 - Summary of problems and solutions in implementation phase 2

6.1.3 Definition of a security policy

Both the literature and the case studies agreed that there is a problem with understanding the roles and responsibilities that are introduced with the implementation of the ISO 27001 across the organizations.

Therefore, it is clear that the only identified issue in this category is the missing delegation and low understanding of the roles and responsibilities within the organization.

Cases and the literature agree that the security roles which are required by the ISO 27001 standard are unclear. It seems that startups do not understand what security roles should be defined within an organization, and what exactly are the responsibilities of those roles. As case C pointed out, they learned by doing and that is why they didn't consider it such a big problem, but a lot of time could potentially be saved if they had understood beforehand.

It doesn't seem that the roles and responsibilities can be standardized. Each organization seems to have different needs when it comes to delegating security roles. Therefore, unless

the ISO 27001 standard, or future research does a better job in explaining the security roles, there doesn't seem to be a better solution for explaining them and the responsibilities of security to the individuals. The literature however highlights that it might be beneficial in startups to combine multiple roles to one person, however a conflict of interest must be avoided. That is true especially during the security audit that comes after the implementation process. Moreover, to tackle the problem of motivation, the cases seem to suggest that the goal of the implementation of the ISO 27001 stated in the top-level security policy should align very well with the values and the direction of the organization. This is again something that the project lead with the management team needs to set out.

Implementation issue	**Solution**
• No delegation or roles and responsibilities • Low understanding of the roles and responsibilities	• Clear definition of security roles by the standard

Table 26 - Summary of problems and solutions in implementation phase 3

6.1.4 Risk assessment

Both the cases and the literature are in an agreement that startups struggle with the identification of assets throughout the risk assessment process.

The issues in this implementation step seem to be quite clear. The startups fail to identify the assets they have in their organization, and how are those assets coupled with each other. This is a big security problem, as missing assets with crucial vulnerabilities could be detrimental to startups, if the vulnerability is exploited.

It seems that when it comes to the identification of assets, it is in fact the knowledge that is missing in startups. However, the literature and available publications do a great job in explaining the various ways of performing risk assessment to great details. Research performed by Asosheh et al. (2013) or other research articles mentioned in the Literature review section of this thesis should help startups with finding the proper methodology. This knowledge is easily accessible for startups to use. Moreover, as it was understood from the interviews, employees or the management teams seem to be very familiar with the idea of performing a risk assessment, and therefore once a methodology is identified and understood, startups should face much less trouble.

Implementation issue	**Solution**
• Identification of assets	• Get & use methodology for asset identification

Table 27 - Summary of problems and solutions in implementation phase 4

6.1.5 Risk management

Because all cases were able to manage by obtaining the methodology from consultants, or from online platforms, methodology was not identified as an issue in this category.

However, it might be beneficial for any startups that do not have the opportunity to obtain methodology from a consultant to consider looking for methodology in literature. The literature provides great methodology to companies to use, however the cases still struggled to find it.

The cases have clearly stated that they are struggling with figuring out what strategies should they apply to lower the likelihood or the impact of a vulnerability. They argue that this is because their key online tools do not support the security implementations, they would expect them to, and have to then find workarounds for those issues which can get expensive. The cases were more worried about what treatment strategies are to be selected when trying to manage the risks, as the systems they are using in their organizations are not supporting the potential treatments they wanted to apply.

The literature also seems to think that methodology will also fix the problem with selecting the controls. It can be difficult for an inexperienced individual to understand the different options one has when managing the risks and choosing the risk treatment strategies. However, an answer closely tied to the next section came from the interviews. They are of the opinion that the online platforms that startups use for their daily operations need to do a better job in supporting security controls. Once they do, it was mentioned that it would be much easier for startups to implement and be compliant with the ISO 27001 standard. Both of these issues are closely coupled with the next implementation step, the selection of controls.

Implementation issue	**Solution**
• Systems don’t support security	• Get & use methodology • Platforms must start to support security

Table 28 - Summary of problems and solutions in implementation phase 5

6.1.6 Selection of controls

The literature and the cases agree on what the problem is, however, the cases shine a bit more light onto the problem than the literature does. The problem with this phase of the implementation seems to be that there is lack of change management and employee involvement in this project in startups.

It seems that companies and startups as well are not considering the changes that the introduction of the ISO 27001 standard is going to have on the way they work, and on the overall culture of the company. As the interviews pointed out, there have been many complaints from the employees that did not understand why they have to change their comfortable way of working to something that is less comfortable and takes more time. Furthermore, it has been pointed out that the employees that are hands-on with the implementation project don't often involve other employees, which creates a gap in the organization that is not being filled. It would be interesting to observe case D in the future and find out how much better the involvement of all employees from the beginning helps the project. While this is something that the project owner and the management should handle better, the issue also seems to be connected with the technical skill of employees. It has been reported that less skilled employees have more trouble understanding and changing their way of working compared to the more 'tech savvy' people in the startups.

It was mentioned earlier that communication is one of the ways that can be used to manage the change that the ISO 27001 standard brings. However, the literature also suggests that the startups should identify and implement the easy treatments first, which will already set a tone for the security in the organization, but it will start slowly so people can start getting used to the changes. The cases seem to also suggest that as many technical controls as possible should be enforced, so that people do not have to think about the way they are working. Furthermore, the pattern that once a hiring process changed to only employ candidates that have a better understanding of technologies in general, it was so much easier to implement the human controls. Moreover, it was observed that such controls were then actually being followed by the employees, as they had a deeper understanding of the implications and the benefits of having information security.

Implementation issue	**Solution**
• Deployment of controls • Lack of change management ○ Lack of employee involvement • Low technical skill of people • Employees do not embrace the new security controls	• Be aware that the ISO 27001 introduces changes. • Manage change • Implement as many technical controls as possible • Hire people with better technical understanding

Table 29 - Summary of problems and solutions in implementation phase 6

6.1.7 Statement of applicability (SOA)

The literature review seemed to single handedly point to the fact that the standard is written in a bad way, it is not suited for startups and doesn't have startups in mind. From the literature only, one might think that if the standard is improved, the problems with the implementation can disappear. However, this was not proven by the cases. While the cases argue that the abstract way in which the standard is written is not helpful, with case B wanting the standard to change, the majority of the cases seemed to be of the opinion that the standard is good the way it is. It seems that it is the experience and the interest in security that might be missing. As mentioned in the cross-case report, the author of the thesis supports this opinion. In the Statement of the Applicability, the startups can easily pick the parts of the ISO 27001 that are not applicable to them, and therefore can be compliant that way.

The cases have pointed the spotlight to a different issue which might be connected to this one. Both cases B and C mentioned that they really struggle with security audits from their customers. This is something that the standard doesn’t have in mind, as this process is not standardized in any way. The audit is usually performed in a form of a questionnaire, but while each audit seems to look for the same nonconformities, the way the audit is performed is always different.

While some wanted to blame the ISO 27001 and the way it is worded, others seemed to see that as an advantage of the standard. This misalignment can mean that there is a bigger issue that this thesis failed to uncover, however the interviews did uncover one massive problem. It seems that the Statement of Applicability should be extended or edited to accommodate the supplier security evaluation. Cases seemed to be quite bothered by the fact that when the maturity level of their ISMS is being audited, each auditor has a different set of questions which have been identified as similar, but not the same. It is an interesting fact that the literature review was not able to identify this problem, however it is possible that the lack of available literature and research on the topic is responsible for that fact.

Therefore, the solution to this problem is quite straightforward. The supplier security evaluation process should be somehow standardized. However, company information security can still be considered quite a new thing, especially in the cases of startups, and therefore it is understandable from that perspective that no standardization of this process has yet been done. The author of this thesis sees this as a suggestion for future research.

Implementation issue	**Solution**
• Bad understanding of the standard • Supplier security audits not standardized	• Standardize the supplier security evaluation process • Read the standard carefully

Table 30 - Summary of problems and solutions in implementation phase 7

6.1.8 Policies / procedures

Cases and the literature agree quite clearly – the startups do not know what to put into the policies, because they think the policies are or must be complex, and it is not clear for them which documents do they actually need to produce. It seems that guidance on the documents that must be produced, or the templates of the documents is something that is only provided by online platforms, and here is where startups hit the problem of the lack of resources. As discussed, multiple times throughout the thesis, they cannot afford to hire a consultant to provide these templates and explain what each policy requires. Perhaps this does come back to the abstract way the ISO 27001 standard is written.

For that reason, it seems that until other research or the ISO come up with templates that startups can use, companies on the market will keep taking advantage and try to earn as much money as possible by providing these necessary templates and help. While this thesis and other research already provides the startups with at least the list of mandatory documents that need to be written up during the implementation process, it is unfortunate that no other viable solution was discovered and proposed by this thesis. Standardizing policies and procedures for startups and providing templates can be a good a good idea for a future research.

Implementation issue	**Solution**
• Lack of understanding about the mandatory documentation • Complexness of policies and procedures • Problems with writing mandatory business documents	• Open-source templates

Table 31 - Summary of problems and solutions in implementation phase 8

Table 32 below summarizes the problems and the solutions for each implementation step.

Implementation step	**Problems**	**Solutions**
Getting management support	• Lack of involvement of top management ○ Regulations not enforced	• Clarify management responsibilities and duties • Present cost of no security • Enforce regulations by giving out fines • Present potential losses (cost of no security)

Definition of the ISMS scope	● Project management ○ No ownership of the project ○ Lack of project planning ○ Unclear project goals / milestones	● Treat ISMS implementation as a project ● Communicate & include the entire organization ● Designate a project owner ● Split into smaller steps (milestones)
Definition of a security policy	● No delegation or roles and responsibilities ● Low understanding of the roles and responsibilities	● Clear definition of security roles by the standard
Risk assessment	● Identification of assets	● Get & use methodology for asset identification
Risk management	● Systems don't support security	● Get & use methodology ● Platforms must start to support security
Selection of controls	● Deployment of controls ● Lack of change management ○ Lack of employee involvement ● Low technical skill of people ● Employees do not embrace the new security controls	● Be aware that the ISO 27001 introduces changes. ● Manage change ● Implement as many technical controls as possible ● Hire people with better technical understanding

Statement of applicability (SOA)	• Bad understanding of the standard • Supplier security audits not standardized	• Standardize the supplier security evaluation process • Read the standard carefully
Policies / procedures	• Lack of understanding about the mandatory documentation • Complexness of policies and procedures • Problems with writing mandatory business documents	• Open-source templates

Table 32 - All implementation issues and solutions summarized

6.2 Discussion

It is clear based on the Table 32 above that there are many things that need working on. Startups can learn from the findings mentioned above and the author of the thesis truly believes that if they do, the implementation process of the ISO 27001 in startups can be improved. It was also proven that the principle of equifinality (Katz and Kahn, 1978) applies to the implementation of the ISO 27001 standard and its problems and solution. Multiple problems identified by the literature review and the various startups lead to unified solutions, and therefore the same output.

It has been established that there needs to be a project owner. This project owner needs to understand that implementing the ISO 27001 standard in a startup is not an easy task, especially when running this project internally only. While has been proven by this thesis that it is entirely possible to run the project in house, the project owner needs to start treating the implementation of the ISO 27001 as a big project. For these reasons, the project should be properly managed, and there should be theory and methodology present throughout the entirety of the project. This thesis offers examples of methodology that the startups can use, as well as a suggestion for a method to run the project, which should greatly help them with getting through the project successfully.

Secondly, the management needs to realize that they need to support the project, but it should be the responsibility of the project owner to define what is expected from the management, and how exactly is the management supposed to be involved. Furthermore, the change that the standard brings into the organization needs to be managed, either through involvement of more employees in the project, or any other forms of transparent communications. On top of that, startups should strive to implement as many technical controls as possible.

Unfortunately, it has been revealed that the work is not only on the side of startups, but also on the side of the standard, and organizations that the startups depend on. While startups can make the biggest improvements, there is also some work on the side of the ISO 27001. It has been identified that the ISO, or any other party should strive to standardize the supplier security evaluation process. This standardization would make it so much easier for standards to be compliant, as they could focus their resources better than answering questionnaires about their security levels. Moreover, if open-source templates are provided to startups, they can get through the process of implementation much easier, and the chances of the project to succeed are much higher. Additionally, all key systems startups rely on must start embracing the fact that they need to support secure solutions that the startups can implement should they need to.

To summarize, the research was able to highlight several key problems and issues that happen throughout the implementation process of the ISO 27001 standard in startups. Table 37 directly answers the main research question. Moreover, the thesis was able to come up with tips and solutions to those problems. On top of that, the solutions were

explained in detail and should practically help startups that are trying to avoid the aforementioned problems. These include solutions on how to run the project, how to include top management, how to enforce controls or how to manage change in the organization that the ISO 27001 inherently introduces. The author of the thesis is of the opinion that if the solutions are used, the implementation process of the ISO 27001 standard is startups will be improved. The research was also able to summarize what are the mandatory documents that startups need to complete in order to become ISO 27001 compliant.

It is also clear that both sides of the table have things to improve. As mentioned just above, the author believes that if startups are able to adopt the advice of this thesis into their implementation projects, it will improve the implementation and massively raise the chances of startups to be actually secure. However, it was identified that it is not only the startups that are solemnly responsible for improving the implementation process. Standardizing supplier security evaluation, providing open-source templates and the fact that platforms that startups use need to better support security controls can only be improved by the standard itself, or third parties. Therefore, the practical solutions and tips, along with the recommendations for third parties about the improvements to the process directly answer the research sub-question.

6.3 Future research

The thesis uncovered that there is a small misalignment and suggestion to what should be a part of the implementation process. The literature review of this thesis argued that the implementation process of the ISO 27001 ends with the implementation of ISMS, and therefore the 8 steps of implementation derived from Lami (2013). However, case C seemed to suggest that the implementation of the ISO 27001 is an ongoing process, and controls are implemented throughout the lifecycle of the ISO 27001. Case C brought up a valid point. Even the 10 steps to compliance by Lami (2013) do not mention the implementation of technical controls, but just the selection of those controls. And therefore, it is not quite clear where this belongs. Unfortunately, given the scope of the thesis and lack of research conducted around this topic, this thesis was unable to provide the answer for this question. It would therefore be a good idea for future research to try and understand where the implementation of security controls falls into, and whether it is an additional step that should be added to the 10 steps to compliance by Lami (2013).

As mentioned previously in the thesis, one of the key issues that needs to be fixed within the implementation process is the standardization of supplier security evaluation criteria. While this research has identified the problem, it is beyond the scope of this research to explore the various ways of how this process could be improved and standardized so that startups can have a much better experience throughout a security audit.

When it comes to standardization, the thesis has also shown that it would be beneficial for startups to be able to easily obtain templates for policies and procedures. While there are many paid solutions on the market, research into how such templates should look like and how could startups obtain them in an open-source format can be interesting.

One of the identified issues was also lack of definition and understanding of security roles. The thesis could not offer more detailed advice on what the roles and responsibilities should be, as the startups can have different setups and needs when it comes to defining the security organization. It would be beneficial if future research is performed on standardizing the security organization, its roles, and responsibilities.

Furthermore, the thesis has also shown that there is a problem with enforcing human controls into an organization. The author of the thesis is of the opinion that it would be beneficial for startups to have an understanding of how to deploy human security controls more efficiently, so that the organizations don’t have to rely solemnly on technical controls.