Universiteit Leiden
ICT in Business and the Public Sector

The critical success factors of the implementation of ISO 9001 and ISO 27001 in an IT organization

Name: Tim van Berghem BSc
Student-no: s2257874

March 9, 2024

Supervisors:
1st: Dr. Werner Heijstek
2nd: Drs. Bas Kruiswijk

MASTER THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Abstract

Introduction: Combining the ISO 9001 (Quality Management) and ISO 27001 (Information Security Management) standards can bring additional benefits to organizations. The reason for this lies in how both standards are structured following the ISO Institute's "High-Level Structure". This structure allows for better integration of ISO standards due to a shared core methodology. Proper integration can bring benefits in all stages of an ISO standard implementation process and beyond.

The ISO 27001 standard has historically had a very high adoption rate amongst organizations that develop software products or those that provide software development services (IT sector). Especially when compared to other sectors. Meanwhile, this sector has had a very low adoption rate for the ISO 9001 standard (Mcadam and Fulton, 2002).

This imbalance of information security management and quality management goes against the prior finding that software that is of high quality will often have a lower number of security vulnerabilities, and software that is free of vulnerabilities will tend to be found of higher quality (Walker, 2020).

Objectives: This research aims to explore the reasoning for, IT sector companies to pursue a combined ISO 9001 and ISO 27001 implementation. Additionally, this research aims to explore the effects that a combined ISO 9001 and ISO 27001 implementation can have on IT sector companies. The goal of this research is to provide companies in the IT sector with a better understanding of the relationship between quality- and information security management. To help them provide their clients and the community with more secure software solutions that are of higher quality.

Methods: This study has held eight one-on-one interviews with representatives of nine Dutch IT companies looking into implementing the ISO 9001 and/or 27001 standards, or who have already achieved the implementation of one or both ISO standards. The results have been processed using qualitative data analysis and are grounded by relating it to prior related research.

Results: Interviewees noted experiencing a higher level of employee involvement by communicating intentions and goals early in the ISO standard implementation process. Employees were involved in documenting their processes and were encouraged to learn about related processes. This potentially helps with integrating the guidelines of the ISO standards into day-to-day activities (internalization).

The level of internalization is found to affect the benefits that are experienced from the implementation of the ISO standards. It was also found that organizations often started out wanting to get ISO-certified due to client demand, but have seemingly found additional benefits after internalizing the standards. ISO 27001 is noted to traditionally be a client requirement, but ISO 9001 certification requirements by clients are said to be increasing.

This research has found that the level of affinity that employees have with a given subject potentially impacts the ease of implementation of a related ISO certification. 78% of respondents with both ISO 9001 and 27001 certifications have said that their IT employees have this higher level of affinity with information security.

Thus, making an ISO 27001 certification easier to implement first. Combined with this research's findings that a second implementation is stated to be easier than the first implementation, there is a potential benefit in leading with an ISO 27001 standard implementation and following this up with the ISO 9001 standard.

A high rate of technological changes seems to have a limited effect on the implementation of both ISO 9001 and 27001 standards. It was found that all ISO standards that follow the "High-Level Structure" already encourage organizations to write their processes down at a high level. Thus, being less dependent on a specific technology and more on one's way of working.

Conclusion: Combining the ISO 9001 and ISO 27001 standards has the potential to benefit IT companies even more than in other sectors due to overlapping business processes related to software development being core components in both standards. The level of success is dependent on how well an organization manages to fit the ISO standards to their organization's cultural identity and way of working. Writing down the processes on a high level ensures the maintainability of the management system and allows the organization to be more adaptable to changes.

Acknowledgements

First of all, I would like to thank my wife for supporting me through a time that was very difficult for me. Writing this thesis in the middle of a pandemic started to feel like the biggest mountain to climb. But you have been the one to help me chop away at it, piece by piece.

Second, I would like to thank my supervisors from Leiden University, Werner Heijstek, and Bas Kruiswijk, for their guidance and patience throughout the project. It has been a pleasant few months of working with enlightening sparring sessions. Their insights and feedback have elevated the quality and depth of this thesis.

Lastly, I would like to extend my gratitude towards the folks at Motion10, who have made their office feel like a second home for the period of this work. Specifically, I would like to thank Bob de Jong for his guidance and facilitating efforts. I would also like to thank Sander Faber of EY, who helped me find my direction early on in my research process. As well as, every one of the interviewees for their time and insights.

If you happen to be reading this and are struggling with mental wellness. Talking to a trained professional can be exceptionally useful. If needed you can always reach out to me and ask me about my experiences. Please just reach out! You are not alone in this.

Tim van Berghem,
Rotterdam,
March 9, 2024

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter is dedicated to introducing the subject. Allowing the reader to get accustomed to the subject matter. As well as introducing the background, intentions, and scope of this research.

1.1 Research Background

The sector of Information Technology (IT) is a fast-moving landscape. Innovations are the topic of conversation and clients expect to see these innovations implemented in the products they purchase. They ask for good quality software. Said clients wish to receive software with the desired quality, within their preferred budget, and within their desired time frame. The core of software quality starts at a quality software creation process (Ijaz et al., 2016). The International Organization for Standardization has published guidelines on how to implement such processes with the ISO 9001 standard.

The product and the data it processes also need to be secured from internal and external threats. It could sometimes be expected of the software supplier to ensure this, even if there have been no contractual agreements made that require this. In the case of O'Cliance versus an anonymous IT firm in the Netherlands, the judge ruled that despite there being no network security requirements in the contract, the client was right to assume that security was included with the product. The IT company should also have refused the assignment if the client was unable to uphold their end of the security measures (ECLI:NL:RBAMS:2018:10124, Amsterdam, 2020). An IT company could get certified in the ISO 27001 standard to prove to their clients or any other party that they have taken sufficient preventive measures against information security threats.

Information, quality, availability, and continuous improvement are core pillars of both ISO 9001 and ISO 27001 standards. Both are management systems that help to get more grip on the processes and continuity of their business. They also share the same philosophy of continuous improvement by incorporating the Deming Cycle (Plan-Do-Check-Act) in their guidelines (NEN, 2020). And with the introduction of the High-Level Structure, the standards can now be integrated more seamlessly (Rousse, 2020).

The High-Level Structure (HLS) is a set of clauses that all future ISO management system standards are required to follow. This HLS system allows for easier integration between different ISO standards by using a shared core with added contextualized requirements for the specific management system (Greensill, 2015).

The ISO standards are published by the International Organisation for Standardization. This organization is composed of standardization bodies from more than 160 countries, with each member country being represented by one standardization body. This organization focuses on developing and publishing international standards in subjects such as environment control, scientific testing processes, working conditions, technology, and more. These standards are developed in a collaborative effort from the member organizations (ISO, 2020a).

1.2 Problem Statement

Considering that the IT sector has a higher-than-average rate of ISO 27001 adoption, accounting for over 20% of all ISO 27001 certifications in 2018 (ISO, 2021), one can assume that Software Security is perceived as an important pillar of the work process. On the other hand, the IT sector has shown to have an especially low rate of ISO 9001 adoption at approximately 1.95% of the total amount of ISO 9001 certifications (Mcadam and Fulton, 2002).

This phenomenon contradicts the reliance that Software Quality and Software Security have on each other. A software application that is of high quality will often have a lower number of vulnerabilities, which in turn leads to better security. Similarly, a secure software application that is free from security vulnerabilities will tend to be of higher quality (Mouratidis and Giorgini, 2006) (Walker, 2020).

Why is the adoption rate of ISO 9001 so much lower than that of ISO 27001 if the principles of these two standards are so intertwined? This question has become more relevant with the introduction of a new method of structuring the ISO standards, the High-Level Structure (HLS), which should help in making it easier to achieve the qualities of both standards (NEN, 2020).

1.3 Purpose of the Research

1.3.1 Business purpose

The purpose of this research is to analyze what IT companies need to do to successfully implement the ISO 9001 and 27001 standards. As well as to find out if and how a simultaneous implementation, of ISO 9001 and 27001, could be more beneficial for an IT company.

In other sectors, clients are increasingly requiring the implementation of quality and risk management systems (del Castillo-Peces et al., 2018). This research aims to find out if the same is true for the IT sector. If this turns out to be true, the outcomes of this research will become even more important for future companies that are faced with the requirement of proving their aptitude in quality and risk management. Something that can be proven with ISO 9001 and/or 27001 certifications.

This research will attempt to help IT organizations achieve a higher rate of success in the combined implementation of the ISO 9001 and 27001 standards.

1.3.2 Scientific purpose

Studies have looked at a variety of topics concerning ISO 9001 and ISO 27001 implementation projects. Ranging from financial benefits to implementation processes. However, none of these researchers/research groups have looked at the IT sector in specific. This is an interesting industry to look at considering that there is a high disparity between ISO 9001 and 27001 certified IT companies (ISO, 2021) (Mcadam and Fulton, 2002). What is the reasoning for this disparity in adoption rate? And consequently, if there are sector-specific barriers or drawbacks, how these can be overcome?

This research will dive into what drives IT companies to pursue and practice ISO 9001 and/or 27001 implementations. As well as to look at which barriers and benefits can be experienced in this process.

This research also looks at the relationship between the ISO 9001 and 27001 standards, and what a double implementation means for the IT sector. A generalized approach to a double implementation has previously been proposed by (Wang and Tsai, 2009). In which they detailed a method of combining the documents from both 9001 and 27001 standards. However, their research was based on ISO standards without the High-Level Structure. Thus, opening up this topic for a revisit of the current structure and IT sector business climate.

1.4 Research question

1.4.1 Main research question

The main objective of this study is to uncover the best method of implementing both the ISO 9001 and 27001 standards in an IT company. As a result, the following research question has been formulated.

"How can IT companies best implement
the ISO 9001 standard in conjunction with the ISO 27001 standard?"

1.4.2 Sub-research question

To answer the main research questions, and have the answer be better grounded in evidence, the research question has been divided into several sub-research questions;

- *How do the structures of the ISO 9001 and 27001 standards relate?*

This subquestion helps us understand why there is such a big gap between ISO 9001 and ISO 27001 certification rates of IT companies. It is also essential in shaping the interview questions.

- *Why do IT organizations choose to pursue ISO 9001/27001 certification?*

Understanding what drives companies to want to achieve ISO certification is important in determining the best method of implementing the standards. With this, we aim to uncover the reasoning behind the difference in adoption rates.

- *What are the criteria for IT companies to consider an ISO 9001/27001 implementation a success?*

This partially overlaps with the previous sub-question. Different states of success can be considered by different companies. Which state of success is most important for IT companies shapes the method of implementation.

- *What are the differences between the implementation of ISO 9001 and 27001 at IT companies as compared to the implementation at other types of companies?*

Where previous research has focused on other sectors such as factories and public service organizations, this research focuses on the IT sector. How much of the previous findings can still be applied to the IT sector? And where is a modified approach required?

- *How can the philosophy of the ISO 9001 and 27001 standards be internalized into an IT organization's day-to-day activities?*

In previous research, the commitment of employees and management has been proven key in a successful ISO implementation (Almeida et al., 2018). Considering IT companies still need the support of these actors for the workflows, it can be hypothesized that this will likely be a key component of the ISO implementation for an IT company as well. This covers both the implementation process, as well as, the internalization of the standard in day-to-day activities.

- *Does a high rate of technological changes affect ISO 9001 and/or 27001 implementations for IT companies?*

It is hypothesized that a high rate of technological changes affects IT companies' ISO 9001 and/or 27001 implementations. This research aims to find out if this is true. And if so, what can be done to limit the negative effects of these changes?

1.5 Research question terminology

For the sake of clarity, it is important to define some of the concepts that are mentioned in this research. This is not only for readers outside of the field of IT but also because different definitions are being used throughout the industry, thus requiring a single definition used in this research.

Concept	Definition	Source
ISO 9001	”ISO 9001 is defined as the international standard that specifies requirements for a Quality Management System (QMS). Organizations use the standard to demonstrate the ability to consistently provide products and services that meet customer and regulatory requirements.”	(ASQ, 2020)
ISO 27001	”ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to apply to all organizations, regardless of type, size or nature.”	(ISO, 2020c)
IT-organizations	”IT-organisation means the assets (including without limitation rights in relation to hardware and software) [...] which are employed wholly or predominantly in connection with the provision of IT Services to the [...] business.”	(Alstom, 2020)
Change-Management	”Change management means to plan, initiate, realize, control, and finally stabilize change processes on both, corporate and personal level. Change may cover such diverse problems as for example strategic direction or personal development programs for staff.”	(Recklies, 2001)
Management system	”A management system is how an organization manages the interrelated parts of its business to achieve its objectives. These objectives can relate to several different topics, including product or service quality, operational efficiency, environmental performance, health, and safety in the workplace and many more.”	(ISO, 2020c)
Audit	”systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled”	(ISO, 2015)

Table 1.1: Research question terminology

1.6 Scope

A few restrictions have been made to keep this research feasible within the given time frame and to increase the focus toward a clear research goal.

Firstly, this research will focus on the ISO 9001 and ISO 27001 standards. There are a few other ISO standards with overlapping features, but the chosen standards are the ones that are seemingly most relevant to the IT sector.

This also includes the ISO 90003 standard which describes the ISO 9001 standard for the IT sector. Since this standard does not give extra rules or requirements for the management system. It can be seen as an additional elaboration of the guidelines from the ISO 9001 standard. Since no prior research has been performed on recent versions of this ISO standard, nor could any empirical experts be found, this standard has been left out of the scope of this research.

The IT sector in particular has been chosen as this sector historically has one of the lowest adoption rates for the ISO 9001 standard (Mcadam and Fulton, 2002). While, on the other hand, having the highest adoption rates for the ISO 27001 standard (ISO, 2021). There is yet to be research that could explain this disparity in adoption rates.

As this research will follow the structure of an exploratory case study (Yin, 2018). Considering the time-consuming nature of this method. Only a small amount of exploratory case studies can be held. Case study subjects will be selected based on the nature of their business (IT services or products.). These companies can be at various stages of ISO 9001 and/or 27001 implementations, but all levels of certification will be represented. The reason for allowing companies that are not fully certified is due to the contrasting opinions they can bring in. This might show barriers and motivations for certification that companies with certification would not think about.

Chapter 2

Theoretical Framework

This chapter will present an overview of concepts and previous research that are relevant to the implementation of ISO 9001 and/or ISO 27001. At this stage, these concepts and research are not limited to the IT sector.

As most of the research on the standards has been carried out in an isolated scenario, the research on the two standards will first be covered separately. Finally, any research that has delved into the crossover of the two standards will be referenced to link the standards together.

2.1 International Organisation for Standardisation

The ISO standards are published by the International Organisation for Standardization. This organization is composed of standardization bodies from more than 160 countries, with each member country being represented by one standardization body. This organization focuses on developing and publishing international standards in subjects such as environment control, scientific testing processes, working conditions, technology, and more. These standards are developed in a collaborative effort from the member organizations (ISO, 2020a).

2.2 ISO 9001 - Quality Management System

2.2.1 ISO 9001 standard

ISO 9001 is the international standard for quality management. The definition of 'quality' is described by Klimovich as an idea that is both objective and subjective. Objective because its characteristics can be observed and compared to requirements. But at the same time subjective as these requirements are provided by humans with inherent biases. Therefore, Klimovich gives the following definition;

> *A comprehensive assessment that examined the inherited quality of the goods, services, or market at large, and the subjective characteristics that have been selected by consumers or clients at the moment of use (Klimovich, 2018).*

The ISO 9001 standard specifies requirements for a Quality Management System (QMS). The standard provides guidelines on procedures, controls, and documentation for a QMS to help a company identify mistakes, streamline its operations, and maintain a consistent level of quality (Kartha, 2004). ISO 9000 certification does not guarantee quality; it guarantees consistency of approach (Gartner, 2020).

The ISO 9001 standard is written generically, with the intent of applying to any type of organization. Regardless of size, structure, or products and services, it provides (Sampaio et al., 2009). The ISO 9001 standard is just one of the standards in the ISO 9000 family, which altogether describes the principles of a QMS. ISO 9000 describes the basic principles and definitions of the standard family. And ISO 9004 describes guidelines for performance improvements. Additionally, there are a couple of sector-specific applications (ISO, 2015). Most notably, ISO 90003 for software engineering. ISO 90003 will be discussed in *Chapter 2.2.4*.

Over the years, the ISO 9001 standard has seen a series of updates and revisions. The latest iteration is the ISO 9001:2015 standard. The main changes with this revision are a larger focus on leadership and commitment, putting risk-based thinking at the core of the standard, shifting to process-based working (thus crossing business unit lines), and better integration with other ISO standards through the introduction of the new high-level structure (HLS) guidelines (Netherlands, 2020).

ISO 9001 specifies the requirements of a QMS. As such it does not provide quality itself but provides guidelines for creating a system that allows companies to get more grip on their processes. Thus, allowing them to get more control over the quality of their output products or services (Natarajan, 2017) (Sousa-Poza et al., 2009) (Chountalas et al., 2019)(ISO, 2021).

Several models describe a QMS for businesses, such as 'Buy With Confidence', 'Lean Six Sigma', and the ISO 9001 standard. Amongst those, the ISO 9001 standard is the most commonly implemented international standard, reaching 1.180.965 certified company sites in 2018 (ISO, 2021).

The ISO 9001 standard incorporates the Plan-Do-Check-Act cycle (PDCA cycle) and risk-based thinking. The PDCA cycle, also known as the Deming cycle, was developed by William Edwards Deming and describes four activities that lead toward the sought-after improvement (Dudin et al., 2014).

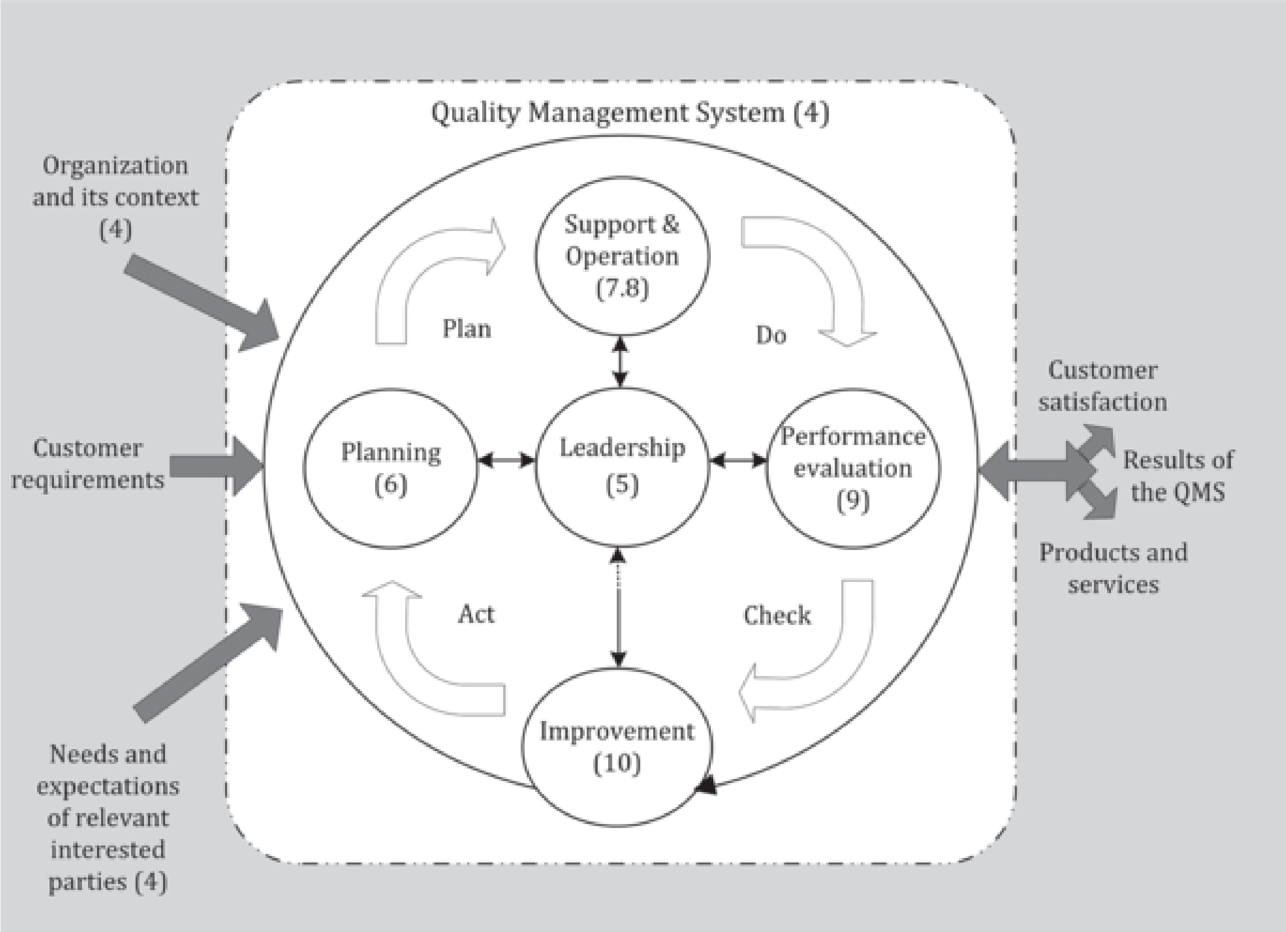

Quality Management System (4)
Organization and its context (4)
Customer requirements
Needs and expectations of relevant interested parties (4)
Support & Operation (7.8)
Plan
Do
Planning (6)
Leadership (5)
Performance evaluation (9)
Act
Check
Improvement (10)
Customer satisfaction
Results of the QMS
Products and services

Figure 2.1: PDCA cycle in the ISO 9001 standard (ISO, 2020b)

Within the standard, it is explained that the PDCA cycle is enabling organizations to ensure that its processes are adequately resourced and managed (ISO, 2019). Within the PDCA cycle, there are specified moments at which an organization reflects on flaws in its current approach and on opportunities that can improve this approach. Those opportunities for improvement are then acted on. This process is conducted continuously.

With this continuous cycle of improvement, the ISO implementation does not stop at the moment it is first implemented or when the company receives its certification. Only when properly internalizing the act of continuous improvement, will the certified organization experience the large number of benefits that an ISO 9001 implementation can bring (Heras-Saizarbitoria and Boiral, 2013) (Cai and Jun, 2018).

2.2.2 ISO 9001 - Adoption Benefits and Motivations

Organizations have different reasons for wanting to implement and/or get certified in the ISO 9001 standard. These reasons can come from internal or external sources and can impact the level of success an organization has with implementing and internalizing the standard (Sampaio et al., 2009). The benefits that are realized depend on the motivation from which an organization seeks certification, the level of internalization, and whether or not a culture of quality is preemptively present in the organization (Heras-Saizarbitoria and Boiral, 2013) (Cai and Jun, 2018).

The different benefits that can be experienced can be divided into internal and external benefits (Boiral, 2012).

2.2.2.1 Internal benefits

The first thing that is often mentioned in previous research papers is the internal wish to improve the quality of products and services. Reasoning that closely matches our previously stated quality definition by Klimovich.

> *A comprehensive assessment that examined the inherited quality of the goods, services or market at large, and the subjective characteristics that have been selected by consumers or clients at the moment of use (Klimovich, 2018).*

Although the definition encompasses much more than solely the quality of goods and services, it is the one that most often comes to mind when thinking about quality.

Implementing the ISO 9001 standard is not a guarantee for higher quality products or services. Rather, the standard is a method by which an organization can implement and improve processes that enable the production and delivery of said higher quality products (Alcina A. de Sena Portugal Dias, 2016), (Jose Tari et al., 2013), (Heras-Saizarbitoria et al., 2014). This is reflected in the second internal reasoning, improving internal processes.

Out of all the research done on the subject of the operational impact of ISO 9001 implementation, 94% have demonstrated a significant improvement in productivity after certification

(Naveh and Marcus, 2005) (Gonzalez-Torre et al., 2001) (Mcadam and Fulton, 2002). Nevertheless, according to several articles, this link remains relatively weak or even insignificant (Escanciano et al., 2001) (Santos and Escanciano, 2002) (Terziovski et al., 2003) (Prabhu et al., 2000) (Sun, 2000) .

According to some studies, there are positive links to be found between the implementation of the ISO 9001 standard and financial performance (Chow-Chua et al., 2003) (Mokhtar and Muda, 2012). However, it could also be interpreted in multiple ways. Either that ISO 9001 implementation improved the firm's performance, or that ISO 9001 implementations were more likely to be done by well-performing organizations (Castka and Corbett, 2015) (Naveh and Marcus, 2005).

What is most important for determining whether the companies experience any financial and/or operational improvements is whether the company internalizes the ideas of the ISO 9001 standard in their daily operations. Instead of just getting certified for the sake of having a certification. However, Alcina A. de Sena Portugal Dias notes that the increase in financial performance and productivity is not necessarily significant and that it varies per sector. Despite this, companies still seek to get ISO 9001 certified to improve their efficiency and financial performance (Alcina A. de Sena Portugal Dias, 2016) (Naveh and Marcus, 2005).

2.2.2.2 External benefits

Several studies have found that the external motives for pursuing ISO 9001 are more prevalent. They state that the goal of these organizations is to cope with external pressures and establish their position in the market. (Douglas et al., 2003), (Jose Tari et al., 2013), (Heras-Saizarbitoria and Boiral, 2013), (Wiele and Brown, 1997). The difference between coping with external pressures and gaining an externally oriented, competitive advantage, is whether or not your competitors already have ISO certifications.

If an organization is one of the first in its sector to pursue ISO 9001 certification it can be seen as a unique selling point. It serves as an indication of a quality process. A process that is more likely to produce consistent quality products or services. However, if the market is already saturated with ISO 9001-certified companies, gaining an ISO 9001 certification will merely keep that company in the conversation for the job. Companies without an ISO 9001 certification would not enter and/or stay in the market. An ISO 9001 certificate was needed to survive in these markets (Alcina A. de Sena Portugal Dias, 2016).

Moreover, some business opportunities or tenders outright require a company to be ISO 9001 certified before they are considered during the bidding process. This seems to be especially prevalent in tenders for public sector organizations (Sampaio et al., 2009). The added benefit of getting certified in ISO 9001 instead of other quality management certifications, is that ISO 9001 is an internationally recognized standard. It allows the organization to start bidding for jobs and tenders all across the globe. As well as, reducing the need for more audits when entering these markets (Boiral, 2012) (Sampaio et al., 2009).

Another external benefit of adopting ISO 9001 is the enhancement of the organization's public image. Customers, suppliers, and stakeholders are signalled that the company is committed to quality management and continuous improvement. Boiral states that increased credibility can lead to increased customer satisfaction and loyalty.

Important to note, is that nearly three-quarters of the studies did not address drawbacks or ineffectiveness factors of the ISO 9001 standard. This makes it seem like the standard is some form of utopian method of leading your business. However, the standard does appear to have its drawbacks. This is important to keep in mind when planning to work toward certification. If these drawbacks are not accounted for accordingly, it can result in a more difficult implementation process and/or less effective benefits after certification (Boiral, 2012).

2.2.3 ISO 9001 - Adoption failure causes and effects

Not all reasons for adopting the ISO 9001 standard will translate into actual benefits for the implementing companies. There is a wide range of failure causes that make meeting a company's goals for a successful ISO 9001 implementation more difficult or even go as far as to experience the possible drawbacks of an implementation (Sampaio et al., 2009).

One of the factors linked to the possible failure of an ISO 9001 implementation is organizational size. Al-Rawahi and Bashir state that larger-sized organizations generally had more success in implementing the ISO 9001 standard. According to them the implementation for larger organizations was less demanding than for smaller ones due to more readily available financial, and human resources (Al-Rawahi and Bashir, 2011). These larger organizations (more than 250 employees) also tend to already have more structured and documented processes. Making it easier to create the required documentation for ISO certification (Bhuiyan and Alam, 2005), (Garengo and Biazzo, 2013).

Historically, most researchers have assumed that the ISO 9001 system is consensual and monolithic across different sectors and that the standard does not get modified to fit the needs of the specific sector or organization. Managers of smaller organizations (less than 250 employees) generally believe ISO 9001 to be a *"mechanistic, consensual and monolithic system that in nature, promotes bureaucracy and paperwork." (Boiral, 2002)* This would thus impede an organization's ability to be flexible and adaptive in a business environment that is evolving and full of uncertainties (Mcadam and Fulton, 2002). However, more recent studies have found that there are differences in this experience depending on the sector of the organization and whether they were a service or manufacturing company (Singh et al., 2006).

More recently, the ISO 9001 standard has evolved to be more flexible and less demanding on a bureaucratic level. Leading Dellana and Kros to argue that smaller organizations have a greater potential to focus on more customer-oriented approaches due to their flexibility. While, at the same time, still delivering on the promise of a constant level of quality goods and services (Dellana and Kros, 2018).

It was found that both manufacturing and service industry organizations require similar levels of resources to get ISO 9001 certified. Both types of organizations also have similar motivations for implementing the standard and face similar difficulties when implementing the standard. However, there are significant differences in the range of management practices associated with the standard (Singh et al., 2006).

Not only does this mean that a service industry company needs to be careful with implementing insights from ISO 9001 implementations from the manufacturing industry and vice versa. But, they also need to be careful with the consultants and auditors that they hire, as they can have experience solely in the other industry and thus give the wrong advice on how to best implement the standard (Singh et al., 2006).

Further specification of the standard per industry is also a possibility to make the standard better fit your organization. This negates the spirit of ISO itself to be universally applicable, but it can improve the fit and benefits of the standard for some organizations. The tailoring of the standards has already happened in some industries, such as in automotive (ISO/TS 16949) and in medical devices (ISO 13485) (Singh et al., 2006) (Kartha, 2004).

2.2.4 ISO 9001 - ISO 90003

The IT sector has its own tailored version of the ISO 9001 standard, ISO 90003:2018. It has specifically been designed to incorporate the ISO 9001 quality management system into Software Engineering companies. The standard had initially seen life in 2014. This first iteration was based on the ISO 9001:2009 standard. This was succeeded by a 2018 update, which introduced the High-Level Structure. Levelling it with other standards like ISO 9001, 14001, and 27001. Which has already incorporated this structure since 2015.

ISO 90003 is relevant for IT companies that are developing, distributing, and maintaining software, including related support services. The ISO 90003 standard includes more information on the scope of changes relevant to the sector by making additions to ISO 9001 chapters including risk, support, monitoring, and operations. In the end, companies that use the 90003 standards, still get certified in ISO 9001 (iso, 2018).

2.3 ISO 27001 - Information Security Management System

2.3.1 ISO 27001 standard

ISO 27001 is the international standard for information security and risk management. America's federal Committee on National Security Systems defines information security as:

> *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability" (cns, 2015).*

In an ever-increasingly digital society, an organization's information, also phrased as data, is becoming an increasingly important asset. This data is not only limited to the organization's data but also the data of their clients. Keeping this data safe and secure is now often silently expected. The inability to keep this data safe can have major consequences such as; reputational damage, loss of clients, and fines (Renvall, 2018).

The ISO 27001 standard specifies requirements for an Information Security Management System (ISMS). With an ISO 27001 certificate, a company can demonstrate its proficiency in information security measures and the management of security risks. ISO 27001 certification can also help cover legal liabilities and serve as evidence of good conduct (Calder, 2006) (iso, 2019).

Similarly to the ISO 9001 standard, ISO 27001 is generic in its wording. Allowing the standard to be implemented in a wide range of company types. ISO 27001 is a part of the larger 27000 families. ISO 27000 is the glossary that describes the wording of the 27001 families. ISO 27002 is an extension of ISO 27001. Bringing more technical depth for companies that need it. ISO 27003 is a guideline for how to implement ISO 27001. ISO 27004 describes key performance indicators for your security measures. ISO 27005 is another extension to the ISO 27001 standard, describing risk management practices. ISO 27006 is a guide for companies on the certification and registration process of ISO 27001 (iso, 2019).

The 2013 iteration of the ISO 27001 standard has been deemed current after the 2018 review cycle (iso, 2019). This iteration was the first of the ISO standards to adapt the High-Level Structure, which we will discuss in *chapter 2.4*. Another part that is now similar to the ISO 9001 standard is the integration of a Continuous Improvement cycle. It implements the Plan-Do-Check-Act (PDCA) cycle, as is explained in chapter 2.2.1, and the image 2.1.

ISO 27001 also has its competitors and counterparts. Such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Critical Security Controls (CIS). Among more industry-specific standards such as the Payment Card Industry Data Security Standard (PCI DSS) for the credit card industry, and System and Organizational Controls 2 (SOC 2) have been developed specifically for the finance sector but are also used in healthcare and cloud service providers. Out of these standards, ISO 27001 is the most widely adopted standard globally, as NIST CSF and SOC 2 are primarily adopted by USA-based firms.

The ISO 27001 standard defines a total of 114 controls that give guidance and restrictions. Implementing these procedures can have a significant impact on the internal processes of a company. Companies must be able to internalize them into their present systems and processes to be successful. However, the reasoning and the consequences experienced benefits can differ greatly between organizations (Renvall, 2018).

2.3.2 ISO 27001 - Adoption benefits and motivations

Adopting an Information Security Management System based on the ISO 27001 standard is a strategic decision made by an organization's higher management. In the spirit of the standard, this is to preserve confidentiality, integrity, and availability of information by applying a risk management process (von Solms and von Solms, 2004). However, similarly to the ISO 9001 standard, the adoption of the ISO 27001 standard can bring numerous other benefits to an organization. The benefits of adoption can come from internal or external factors.

2.3.2.1 Internal benefits

Perhaps the most direct benefit or motivation for adopting the ISO 27001 standard is the reduced risk of data breaches. By implementing the controls and best practices outlined in ISO 27001 for addressing risks and vulnerabilities, organizations can minimize the risk of data breaches and the resulting negative consequences (von Solms and von Solms, 2004).

Some organizations might aim to use the implementation of the ISO 27001 standard for the improvement of their financial performance. However, Boehmer and Hsu believe that there are insignificant findings for this. They contribute this to ISO 27001 being more of an obligation instead of a competitive advantage, or unique selling point. They do however state that this might not be true for sectors where this expectation of ISO 27001 certification might not be the standard (Boehmer, 2009) (Hsu et al., 2016).

The implementation of an information security management system, such as ISO 27001, can contribute to the added formality and visibility of an organization's security practices. Along with raising the organization's confidence in the confidentiality, availability, and validity of their intellectual property and information that is critical to organizational decision-making. If information of this nature were to be leaked or gained maliciously, the organization could experience large financial and competitive disadvantages. (AbuSaad et al., 2011).

2.3.2.2 External benefits

"Compliance reasons" is the biggest driver for ISO 27001 ISMS implementation and certification as noted by Woollven in their 2018 survey. With a total of 78.4% indicating it as one of their goals. (Woollven, 2018)

Some organizations may require their partners and suppliers to be ISO 27001-certified as a prerequisite for doing business with them. This means that achieving ISO 27001 certification can open up new business opportunities for your organization. Around 72% of correspondents to an international survey said that they received either regular or occasional requests to provide ISO 27001 certification in 2016 (Woollven, 2018). By providing proof of compliance with a globally known standard, these organizations significantly reduced their need for repeated client audits (Ganji et al., 2019).

By demonstrating that the organization has implemented a formal and recognized information security management system, the organization can gain the trust of its customers and stakeholders. This can be especially important for organizations that handle sensitive customer data, such as financial institutions and healthcare providers (CISA, 2022). By meeting the stringent requirements of the ISO 27001 standard, organizations can demonstrate their commitment to data security and build a positive reputation in their industry (Ganji et al., 2019) (Tu and Yuan, 2014).

Implementing the ISO 27001 standard can help to protect the organization's reputation by reducing the risk of data breaches and other information security incidents. In turn, improved trust and a good reputation for risk management can lead to improved marketability, as you can differentiate the organization from its competitors and make it more attractive to potential clients (Woollven, 2018) (Hsu et al., 2016).

The ISO 27001 standard aligns with many data protection regulations and laws, such as the EU's General Data Protection Regulation (GDPR). Implementing the standard can help organizations comply with these regulations and avoid potential fines and penalties. The effects of ISO 27001 can be even greater for international organizations, as the standard is internationally known and recognized (Ganji et al., 2019) (Woollven, 2018).

2.3.3 ISO 27001 - Adoption failure causes and effects

The primary causes of ISO 27001 adoption failure are a lack of support from higher management, lack of resources, work culture, lack of understanding of security standards, lack of awareness of the importance of security standards, resistance to change, lack of careful planning, the complexity of ISO 27001, lack of comprehensive documentation, and the difficulty of identifying organizational assets.

Most research notes the lack of higher-management support to be the biggest cause adoption failure of the ISO 27001 standard. Management support is important for the implementation of the ISO 27001 standard because it ensures that the implementation is taken seriously, that necessary resources are allocated, and that the implementation is sustained over the long term. Without management support, the implementation may be more difficult and may not be successful in the long run (Muh. Sidratul et al., 2019) (Renvall, 2018) (Ndegeya and Uwase, 2022).

The second biggest factor is the resistance to change from the employees to the implementation of an ISO standard. People may be resistant because they are comfortable with the current way of doing things, unsure of how the changes will impact their work, or concerned about the potential negative consequences. The difference between IT and non-IT organizations is most prevalent here as IT workers generally have a better understanding of why information security is important for both the organization and themselves (Ruhwanya and Ophoff, 2020).

To overcome resistance, it is important to communicate the reasons for the changes and the benefits they will bring and to provide adequate training and support to help people understand and adapt to the new policies and procedures. This is where the support from top- and middle-management support will be important (Muh. Sidratul et al., 2019) (Renvall, 2018) (Ndegeya and Uwase, 2022).

The ISO 27001 standard has 14 domains, which contain a total of 114 controls. This level of complexity is another limiting factor in the implementation of ISO 27001. Renvall states that many organizations are hesitant to start an ISO 27001 implementation due to a lack of understanding of the security standards. Success in the planning stage, the evaluation phase of information security conditions, and the risk management stage affect the smooth implementation of ISO 27001. Consultation from an ISO 27001 implementation expert is the best method of alleviating this issue (Muh. Sidratul et al., 2019).

A lack of awareness of the ISO 27001 ISMS being implemented among the employees can result in a lack of proper implementation and maintenance of the ISMS, which can lead to vulnerabilities in the organization's information security measures. Organizations need to identify and define the roles and responsibilities for information security and actively communicate them to employees and other relevant parties (Renvall, 2018) (Ndegeya and Uwase, 2022).

Guidelines for required information security behaviour within an organization are not yet part of the ISO 27001 standard. This causes difficulties in the effective internalization of the ISO 27001 standard, and with this, the realization of the full benefits that implementation of ISO 27001 can provide (Topa and Karyda, 2019).

The amount of human and financial resources required for an ISO 27001 implementation is often underestimated (Ndegeya and Uwase, 2022). A later study confirmed this, although they found the underestimation of the human resource factor to be most prevalent (Renvall, 2018).

large organizations may benefit more from the implementation of information security system standards since they are more dependent on formalization and standardization than smaller companies and have a greater amount of assets (Chang and Ho, 2006).

Lack of comprehensive documentation is named as one of the limiting factors against the implementation of the ISO 27001 standard (Muh. Sidratul et al., 2019) (Renvall, 2018). However, other studies counter this argument. Stating that the comprehensiveness of the documentation does not decide the quality and success of an ISO 27001 implementation, but that understandability and clarity are much bigger contributors to success (Ndegeya and Uwase, 2022) (Tu and Yuan, 2014).

An ISO 27001 ISMS strategy can only be properly formed if all of an organization's assets related to information security are known. These include information processing assets, confidential documents, physical assets, and technological assets. Proper communication and indexation of these assets are key. If lacking, the strategy and planning phases will not be able to properly cover all assets. Leaving the organization open to attacks on these weaker fronts. As well as, resulting in time and budget calculations being unmet (Muh. Sidratul et al., 2019) (Renvall, 2018).

Lastly, the cost of investment in information security processes has been named as a significant reason preventing organizations from pursuing an ISO 27001 implementation (Boehmer, 2009). Organizations often find the costs and amount of time that needs to be invested into gaining and maintaining ISO 27001 certification too high (Woollven, 2018). Gillies states that this is a reason for low adoption in sectors with limited availability of skilled resources.

2.4 ISO 9001 and 27001 - Integrated Management System

Information, quality, availability, and continuous improvement are core pillars of both the ISO 9001 and the ISO 27001 standards. Both are tools for management to get more grip on the quality and continuity of their business. They also share the same philosophy of continuous improvement by incorporating the Deming Cycle in their guidelines (Rousse, 2020).

The ISO 9001 standard for Quality Management and ISO 27001 standard for Information

Security Management are also similar in their approach to a management system. In recent versions of the standards, a High-Level Structure has been introduced that aims to make the standards easier to align. This allows for easier integration of both standards into a single management system. The implementation of this could be done simultaneously or at a later date (Wang and Tsai, 2009).

2.4.1 Integrated Management System - Benefits and Motivations

The integration is also helped by the fact that both standards are PDCA cycle-based management system standards. Meaning that many clauses in the ISO 9001 and 27001 standards are the same or similar. Simon et al. and Hoy and Foley both argue that this can have the benefit of not needing to repeat documentation and processes (Simon et al., 2013) (Hoy and Foley, 2014).

Other benefits come from the already established document control procedures, communication channels, and the governance structure in which the management system is discussed. Using this pre-existing infrastructure for the implementation of a new ISO standard might enable the saving of resources. Methods for generating awareness and improving internalization of the new addition to the management system in the organization's processes and culture. However, how much this helps is difficult to quantify since it changes with each organization (Hoy and Foley, 2014).

Differences in implementation methods stem from the different ways an organization is structured and managed. An agile method of working requires a different implementation method than a waterfall developing method. How this is implemented is solely at the discretion of the organization that is implementing the standard. This is because the ISO 9001 and 27001 standards are formulated generically, as to make them applicable to a wide range of organization types. Each organization can implement the standard to a level that is adequate for its organizational purposes. However, this means that during the certification audit, the organization must be ready to support their reasoning for implementing the standard in this way (Hoy and Foley, 2014) (Simon et al., 2013).

According to Zutshi and Sohal, and Kraus and Grosskopf, a reduction in the amount, duration, and cost of auditing could also be experienced. The effort of planning, preparing, and follow-up activities related to the auditing process were also reduced (Kraus and Grosskopf, 2008) (Zutshi and Sohal, 2005). Integrated audits can be performed after the implementation when two or more management systems of different disciplines are implemented in an organization Kymal et al..

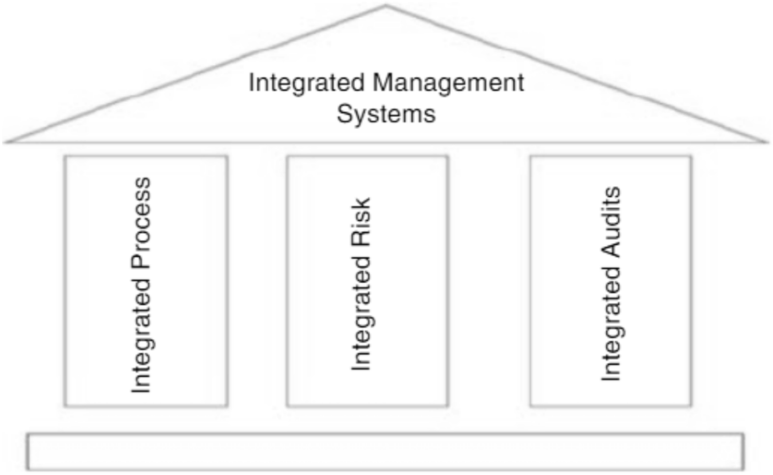


Figure 2.2: Integrated audit process for integrated management systems (Kymal et al., 2015)

2.4.2 Integrated Management System - Adoption Failure Causes and Effects

There are still some potential risks found with the ineffective implementation of an integrated management system (ISO 9001 27001). One of them is the potential of conflicting documentation and processes for the different system standards (Celik, 2009). Furthermore, the information management systems used by different teams may conflict. For example, in the case of measuring objectives and key performance indicators for each system, ISO 9001 and 27001 have different objectives. The implementing organization will then need to find a trade-off that best fits their needs (Zeng et al., 2011).

The resource availability and management commitment issues that have been mentioned as failure causes and effects for the individual standards are an even bigger risk during the implementation of an integrated management system (ISO 9001 27001). Organizations that fail to manage these risks for a single ISO standard implementation should certainly not try to implement both standards simultaneously. As this will only aggravate the previously mentioned issues and increase the risk of failure to implement any of the ISO standards (Zeng et al., 2011) (Hoy and Foley, 2014) (Zutshi and Sohal, 2005).

Chapter 3

Methodology

Now that the theoretical framework has been presented, we have gained a base information on which this research can build and try to expand on this. To find data about the experiences of those who have implemented ISO 9001 and/or 27001 management systems, this research has used a qualitative multiple-case study research design. Consists of interviews with top management, information security managers, or quality managers. The chapter methodology will discuss the methods that have been used and the considerations that have been made while trying to answer the research questions. The goal is to give a clear understanding of how the research has been structured and executed.

3.1 Research design

For our research questions, the decision has been made to use a qualitative exploratory research design in combination with structured surveys. As discussed by Ponelis, this method has been accepted as a way to develop conceptual and theoretical models that might be novel, yet are grounded in literature. From this exploratory research, a structured survey has been developed that aims to answer the research questions with qualitative responses from subject matter experts. (Ponelis, 2015)

The main research question has been split into multiple sub-questions. These sub-questions are more focused on different sections of the research. Using sub-questions allows the research to build more coherently to a conclusion, and aims to help in answering the main question. See table 3.1 for a summary of the sub-questions, their respective methodology, and which instrumentation is used for answering them.

Question	Methodology	Instrumentation
Sub-1: How are ISO 9001 and ISO 27001 related?	Thematic analysis	Desk-research (literature) Semi-structure interviews
Sub-2: Why do some IT-organisations choose not to pursue ISO 9001/27001 certification	Thematic analysis	Semi-structured interviews Survey analysis
Sub-3: How can you positively change the mentality of an organisation's management and employees towards a culture of quality and information security	Thematic analysis	Desk-research (literature) Semi-structure interviews
Sub-4: When is an ISO 9001/27001 implementation considered a success?	Thematic analysis	Desk-research (literature) Semi-structured interviews Survey analysis

Table 3.1: Research Sub-Questions and Used Instrumentation

Thematic Analysis has been chosen as a methodology for answering the sub-questions. It is a method for identifying and analyzing patterns of meaning in a data set. It illustrates which themes are important in the description of the phenomenon under study as stated by Hayes. The qualities of this method have been discussed by Braun and Clarke and later confirmed by Joffe. (Hayes, 1997) (Braun and Clarke, 2006) (Joffe, 2011)

3.2 Participants

This research is exploratory and builds on the experience of those who have implemented ISO 9001/27001, or those who have attempted implementation. Therefore, it is necessary to get in contact with those individuals with experience in implementing ISO 9001/27001 in the field of IT. This subsection discusses the sampling strategies and how the researcher got access to the sample group.

3.2.1 Sampling

A group of nine companies, with a varied background in experience with ISO 9001 and/or 27001 implementations. Ranging from having thought about implementing either standard, but deciding not to pursue it. To those who are actively attempting to get certified. And finally, those who have already achieved one or both of the certifications. During the sampling, an attempt was made to evenly spread the participants over the three levels of experience with ISO 9001/27001 implementations.

Since ISO 9001 has gone through some iterations over its life cycle, the sampling will be limited to those with experience with ISO 9001:2008 or newer versions. With this new iteration, the ISO 9001 and 27001 standards have undergone a major revision to create a better alignment of both standards. Therefore, all participants will be asked to state the ISO 9001 and 27001 versions in which they are certified.

3.2.2 Sampling bias

The sampling of companies is likely to experience selection bias, as the number of willing participants available to the researcher was limited. The biggest gap is the lack of IT organization that has been certified in ISO 27001 but lacks ISO 9001 certification. The total number of interviewees per category is also rather low. With two companies having no certification. One company has just the ISO 9001 certification. And six more companies have achieved both ISO 9001 and 27001 standards. This selection bias could lead to a less reliable data set (Thomas, 2017).

The low number of interviewees per category could result in outlying answers being over-represented in the research results. Interviews also had to be held online. This could have led to a decreased understanding of an interviewee's true feelings and meaning, as social clues are more difficult to understand when talking virtually. Other possible effects could have been a potential participants' attitude towards virtual meeting tools, health conditions of potential participants, and social and technological barriers (Nikolopoulou, 2023).

Sampling bias and self-selection bias are the types of bias that are most likely to occur in this type of research. Sampling bias, caused by non-random sampling, has been impossible to completely remove from the sampling as the number of interviewees was too limited. The same is true for self-selection bias. There is a chance that those who volunteered to partake in the interview were part of an organization that exhibited a specific set of traits that could make implementing ISO 9001 and/or 27001 easier or more difficult. Personal judgment needed to be used in both cases to come to a purposive sampling.

3.2.3 Access

The effect of 'snowball sampling', meaning asking the interviewees to refer the research to potential other subjects, needed to be relied on to maximize the available respondents for the interviews. Interviewees were asked to refer other subject matter experts who could potentially be interviewed. A selection of the results from this snowball sampling will still take place to make sure the sample group is evenly spread over the parameters.

Network effects are also being used online through social media. LinkedIn will be used as the platform through which new leads for participants are to be generated. This will be done through videos in which new information about the research and 'fun facts' about the ISO 9001 and ISO 27001 standards are shared. The goal is to create more engagement and spread awareness about the research. The reasoning behind this is that people are more likely to respond to requests such as filling in a survey when they are engaged with the cause or when they can benefit themselves from doing so (Porter and Whitcomb, 2005) (Nair et al., 2008).

3.2.4 Participants

- **No certification**: The interviewee from company one is the Chief Operating Officer (COO) and ISO project initiator of an IT consulting firm with 150 employees. The organization's efforts are split across IT consulting services and product development. This organization is actively looking to get certified in both ISO 9001 and 27001. The organizational structure is described as a *"medium level of the hierarchy, but with open communication"*.

- **No certification**: The interviewee from company two is the managing director at an IT consulting company with around twenty-five employees. The company provides both low-code and traditional software development services. The Company was aware of both ISO 9001 and 27001 but has not pursued implementing the standard(s). The organizational structure is seen as *"open and flat"*.

- **ISO 9001 Certified**: The interviewee from company three is seen as the quality expert within their forty-employee large company. The company is evenly split between a non-IT consulting department and an IT department that works on a singular product. The organizational structure is seen as *"open and flat"*.

- **ISO 9001 and 27001 certified**: The interviewee from company four is the information- and quality manager for an ICT company with around 200 employees. The company is split into multiple entities which all have different levels of ISO certification depending on their needs. This includes ISO 9001, 14001, and 27001. This organization is self-described as having *"somewhat of a hierarchy"*.

- **ISO 9001 and 27001 certified**: The interviewee from company five is the COO of an

IT consulting firm with close to two hundred employees in the Netherlands. The organization primarily provides IT consulting services and has achieved both ISO 9001 and 27001 simultaneously. They describe their organizational structure as *"Clearly defined roles and hierarchy but with open communication lines"*.

- **ISO 9001 and 27001 certified**: The interviewee from company six is an information security employee at a software product development company that focuses on the healthcare sector with around fifty employees. They have both ISO 9001 and 27001 certifications, along with NEN 7510 (Information Security Management in Healthcare). The company described this organization's structure as *"traditional"*.

- **ISO 9001 and 27001 certified**: The interviewee from company eight quality assurance employees at a company that provides both consultancy services and standard software product solutions. They have around 35 employees and have achieved both ISO 9001 and 27001 standards. The company described this organization's structure as *"hierarchical"*.

- **ISO 9001 and 27001 certified**: The interviewee from company seven is the information security officer at the software development branch for one of the Netherlands' major employment agencies. This team of over sixty employees provides software solutions and management of external tools for the rest of the sixteen hundred-employee large organization. This organization is self-described as having *"somewhat hierarchical"*.

- **ISO 9001 and 27001 certified**: The final interviewee is the Quality Manager and Security Officer for a company with around forty-five employees. This company has recently been merged from three separate companies into a single entity. The structure has been described as flat, with self-steering project teams. The company is certified in ISO 9001, 27001, and NEN 7510 (Information Security Management in Healthcare).

3.3 Ethics

In the case of this research specifically, the topic of ethics is about the decisions and dilemmas that potentially affected this research. Research ethics are a part of ensuring the safety and informed commitment of the subjects. There are several important principles related to ethical considerations. These considerations are based on models by Bryman and Bell, and

Roshaidai and Arifin and are given in the next section with an explanation of how this research will consider them. (Bryman and Bell, 2011) (Roshaidai and Arifin, 2018)

1. **Research participants should not be subjected to harm, both physically and non-physically.**

   This study will respectfully treat all stakeholders and participants to ensure the working environment is safe and that the interview or survey questions do not invoke negative emotions.

2. **Respect for the dignity of research participants should be prioritized.**

   The opinions, knowledge, and other personal findings of the participants will be treated with respect and dignity.

3. **Full consent should be obtained from the participants before the study.**

   All participants will receive a disclaimer before being subjected to an interview or survey questionnaire. This disclaimer will inform the participants of the goals of the study, as well as the way the study will handle their responses and other collected information. Collected information was anonymized and the participants were able to review their answers after transcription had been performed.

4. **Participants should be fully informed and understand the implications of the study.**

   As stated above. The participants will receive a disclaimer that will fully inform them about the implications of the study and the way they will be treated as participants. If any questions arise, the participants are free to contact the researcher via email or by phone (contact information is given in the disclaimer).

5. **Participants should be legally and ethically competent to consent.**

   All participants are of the ages of 18 and above and are primarily considered to be competent to consent. If any questions about a participant's ability to consent do arise, they will be disqualified from the study.

6. **The protection of the privacy of research participants has to be ensured.**

   All personal identifiers such as names, addresses, and contact information will be kept strictly private unless agreed upon otherwise. The same is true for any recordings, transcriptions, and email conversations. The recordings of the interviews and direct personal identifiers will be destroyed after the research has concluded. Any other materials will be made anonymous and safely stored for one year to ensure any questions about the study can be answered adequately.

7. **An adequate level of confidentiality of the research data should be ensured.**

   As previously stated, the recordings, transcriptions, and email conversations will be kept strictly between the researcher and the respective participant. Unless agreed upon otherwise.

8. **The anonymity of individuals and organizations participating in the research has to be ensured.**

   As can be read by the participants in the disclaimer before being subjected to any interview or survey, the personal information and any re-traceable opinions or experiences will be kept strictly between the researcher and the respective participant.

9. **Any deception or exaggeration about the aims and objectives of the research must be avoided.**

   The aims and objectives of the research will be made clear before the participant is subjected to any interviews or surveys. The aims and objectives of the research have been discussed and corrected in accordance with the thesis supervisor from Leiden University.

10. **Affiliations in any forms, sources of funding, as well as any possible conflicts of interests have to be declared.**

    All affiliations and/or conflicts of interest will be declared to the participants via the disclaimer. Leiden University has no known conflict of interest with any of the participants or their organizations. Motion10 is facilitating the research. This party does have potential conflicts of interest with the participants. Therefore, it is critical for the integrity of the research that Motion10 does not receive the collected research information. Motion10 will receive the same information that will be shared when the research is made public. This is also communicated to the participants.

11. **Any type of communication concerning the research should be done with honesty and transparency.**

    The researcher will communicate the aims and objectives of the research clearly and frequently with the participants and stakeholders. The researcher will be adequately available for any questions that might arise for the duration of the research and a period afterwards.

12. **Any type of misleading information, as well as the representation of primary data findings in a biased way must be avoided.**

    The thematic analysis methodology of coding and representing primary data-based findings will be used for this research. This methodology is a peer-reviewed method of avoiding biases by identifying and analyzing patterns of meaning in data sets. It illustrates which themes are important in the description of the phenomenon under study (Hayes, 1997) (Braun and Clarke, 2006).

3.4 Validity and Reliability

To ensure the research comes to results that are grounded and correct, the collected data must be valid and reliable. This study will use the following definitions of validity and reliability;

3.4.1 Validity

For research to be valid, the main claims and evidence should be plausible enough to be accepted at face value. If this cannot be done, evidence should be provided to explain why. Furthermore, the evidence should strongly imply the validity of the main knowledge claim and be sufficiently plausible, or credible to be accepted. Increasing layers of evidence should then be presented if the previous pieces of evidence do not meet the previously mentioned criteria (Thomas, 2017).

> *"Validity refers to integrity, the application of the methods, and the precision in which the findings accurately reflect the data." (Noble and Smith, 2015)*

Any empirical generalizations that are made based on a finite set of respondents should be sufficiently plausible and credible to be accepted. These generalizations can be grounded by providing theoretical evidence that supports these generalizations.

3.4.1.1 Reliability

Reliability refers to the ability to achieve the same result when performing the same research actions by a different researcher on a different occasion.

> *"The consistency of the analytical procedures, including accounting for personal and research method biases that may have influenced the findings." (Noble and Smith, 2015)*

Thomas states that, in interpretive research, personality traits will always affect the interpretation of the results. The same is true during the interviews. The personality traits of the interviewee, interviewer, and interpersonal relationship will affect the given answers. The validity of the results can also come into jeopardy because of this, as the personal bias of the researcher may lead to inaccurate estimations of relationships between variables and the weight of each of these variables. (Thomas, 2017)

3.4.2 Ensuring credibility of the findings

Noble and Smith have stated nine strategies that aim to ensure the trustworthiness of the findings. These strategies are stated in the next section with an explanation of how this research will incorporate them. (Noble and Smith, 2015)

1. **Accounting for personal biases which may have influenced the findings.**

   The researcher will try to get rid of any personal biases in its questioning during interviews or surveys to avoid bias. The questions are tested by a linguistic expert from Motion10 and an independent supervisor from Leiden University.

2. **Acknowledging biases in sampling and ongoing critical reflection of methods to ensure sufficient depth and relevance of data collection and analysis.**

   This research aims to avoid sampling bias by randomly selecting participants while at the same time keeping a balance in the number of participants between those with ISO certification and those who are trying to get certified or have failed in doing so. Furthermore, critical reflection on each participant's personal biases will be taken into consideration when analyzing the data.

3. **Meticulous record keeping, demonstrating a clear decision trial and ensuring interpretations of data are consistent and transparent.**

Records for data, theoretical sources, participants, and leads are securely stored and kept up-to-date after usage.

4. **Establishing a comparison case/seeking out similarities and differences across accounts to ensure different perspectives are represented.**

   A wide variety of participants have been sought for the interviews. This spreads over those with both ISO standards implemented, those with a single implementation, those who are yet to attempt to get certified, and those who have failed to get certified. Similarities and differences between these levels of ISO certifications will be sought out with the use of qualitative coding.

5. **Including rich and thick verbatim descriptions of participants' accounts to support findings.**

   Complete transcriptions will be kept from the interviews.

6. **Demonstrating clarity in terms of thought processes during data analysis and subsequent interpretations.**

   During data analysis, the researcher will keep meticulous notes on his thought process on different findings. These notes will help form a reading line which, together with a storyboard, aims to give a clear demonstration of the researcher's thought process.

7. **Engaging with other researchers to reduce research bias.**

   Methods will be peer-reviewed by other researchers from the University of Leiden. A supervisor from Leiden University and Motion10 will also give guidance on the applied methods.

8. **Respondent validation: includes inviting participants to comment on the interview transcript and whether the final themes and concepts created adequately reflect the phenomena being investigated.**

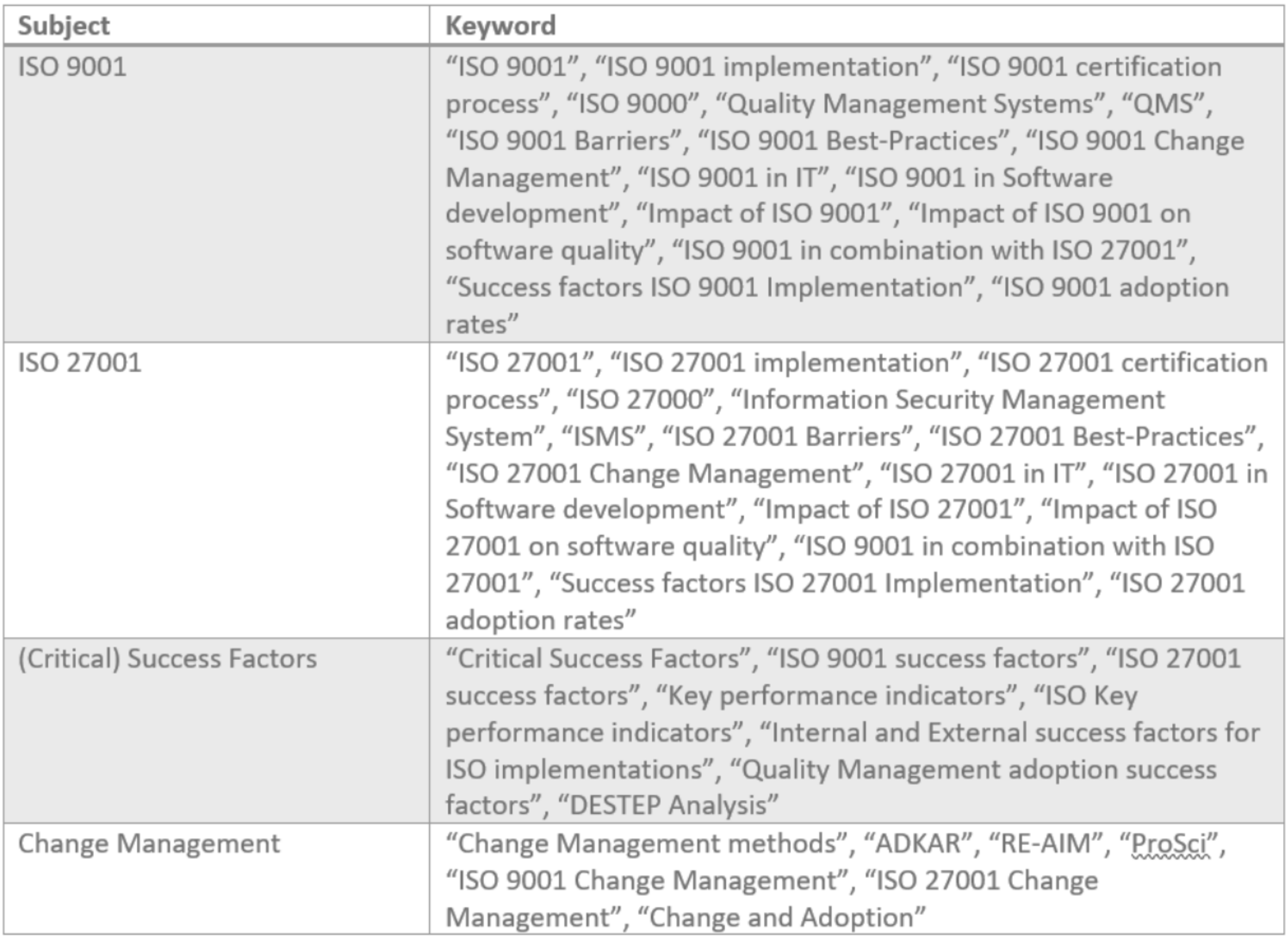
   Interview participants will be sent transcripts of the interviews. They are free to suggest additions or request redactions if they require the information to stay confidential. Proper reasoning will be required for revision to be accepted by the researcher.

9. **Data triangulation, whereby different methods and perspectives help produce a more comprehensive set of findings.**

Different perspectives will be incorporated through the wide variety of participants as well as through different theoretical perspectives. The researcher will take the perspectives of the end-users, top management, as well as that of change management.

3.5 Data gathering and instrumentations

A collection of instrumentations has been applied to gather the data required for this research. The first is desk research, which uses specific keywords to find articles related to the subject. The keywords that have been used can be seen in figure 3.1. A literature search was performed, and databases such as that of the Leiden University library. Finding an article often resulted in a snowball effect which allowed for more related articles to be found through recommended articles or citations.



Subject	Keyword
ISO 9001	"ISO 9001", "ISO 9001 implementation", "ISO 9001 certification process", "ISO 9000", "Quality Management Systems", "QMS", "ISO 9001 Barriers", "ISO 9001 Best-Practices", "ISO 9001 Change Management", "ISO 9001 in IT", "ISO 9001 in Software development", "Impact of ISO 9001", "Impact of ISO 9001 on software quality", "ISO 9001 in combination with ISO 27001", "Success factors ISO 9001 Implementation", "ISO 9001 adoption rates"
ISO 27001	"ISO 27001", "ISO 27001 implementation", "ISO 27001 certification process", "ISO 27000", "Information Security Management System", "ISMS", "ISO 27001 Barriers", "ISO 27001 Best-Practices", "ISO 27001 Change Management", "ISO 27001 in IT", "ISO 27001 in Software development", "Impact of ISO 27001", "Impact of ISO 27001 on software quality", "ISO 9001 in combination with ISO 27001", "Success factors ISO 27001 Implementation", "ISO 27001 adoption rates"
(Critical) Success Factors	"Critical Success Factors", "ISO 9001 success factors", "ISO 27001 success factors", "Key performance indicators", "ISO Key performance indicators", "Internal and External success factors for ISO implementations", "Quality Management adoption success factors", "DESTEP Analysis"
Change Management	"Change Management methods", "ADKAR", "RE-AIM", "ProSci", "ISO 9001 Change Management", "ISO 27001 Change Management", "Change and Adoption"

Figure 3.1: Desk Research Keywords

The second method used is semi-structured interviews. This method allows for some flexibility that is required for finding new empirical knowledge and for expanding on models. Yet, still allows for comparable results through thematic analysis. The interview questions are based on the results of the desk research and are aimed at testing or expanding those findings to the current knowledge in the IT sector. During the interviews, notes will be kept on non-verbal or implied communications which could alter the meaning of some answers. The interview will be transcribed afterwards. The interviewee will receive a copy of the transcript for review and is free to add to this if they can think of something they missed during the interview. The interviewer will conduct the interviews based on the bias-reducing steps, as stated by McNamara and Chenail. There is space for adopting new knowledge or questions that arise during the interviews which can alter or add to future interviews. (McNamara, 2020) (Chenail, 2011)

More on the sampling of the group of interviewees can be found in *Chapter 3.2.1*.

3.6 Procedure

The questions are structured in a way that will ease the interviewee into the interview. Interview structuring such as that advised by Thomas, and (Chenail, 2011), is used to contact potential interviewees. The purpose, duration, confidentiality measurements, and a general idea of the questions will be made explicit to the interviewee well ahead of the interview. Interviews were planned for an hour and took place in or around the offices of the interviewees. The participants were free to choose whether they felt more comfortable talking in a conference room or a public setting, like a cafe. (Thomas, 2017) (Chenail, 2011)

Interviews were attempted to be held in a face-to-face setting to best be able to interpret any verbal and non-verbal cues. However, due to the global pandemic, this was not always possible. Video conference calls were used as the second best available option in these situations Janghorban et al.. Interviews were transcribed and coded immediately after the interviews were held and were supplemented with notes that were kept on non-verbal communication from the interviewee. The transcripts were sent to the interviewee for final review. The interviewee then had the opportunity to add to his or her story in case they had forgotten any information. The transcribed interviews and recordings will not be made public for confidentiality and anonymity. (Janghorban et al., 2014)

3.7 Analysis

After transcribing and coding the interviews, as well as, collecting and cleaning up the surveys, a collection of analyzable data has been accrued. From this data, one can start to draw valid and reliable conclusions. These conclusions are drawn through the use of the thematic analysis method (Braun and Clarke, 2006) (Joffe, 2011).

Thematic analysis is a method for identifying and analyzing patterns of meaning in a data set. It illustrates which themes are important in the description of the phenomenon under study (Hayes, 1997). Braun and Clarke have presented the six phases of conducting thematic analysis, which can be seen in figure 3.2. (Braun and Clarke, 2006)

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

Table 3.2: Phases of Thematic Analysis

These six phases of conducting thematic analysis have been incorporated into this research to uphold the reliability and validity of the conclusions and with that the research.

For the coding process, the choice has been made to use the open-coding method by Corbin and Strauss as opposed to the template coding method by King. Open coding is a better fit for this research as it leaves space for new concepts and insights. Template coding is much more limiting and is less applicable for the exploratory nature of the research as stated by Blair. (Corbin and Strauss, 2008) (King, 1999) (Blair, 2015)

It is important to describe the meaning of a category as clearly as possible, for example, by writing an appropriate memo. The grounded theory calls this a code memo, while in qualitative content analysis, category definition is the preferred term (Banks, 2014).

Category definitions have a dual function: firstly, they document the framework of the analysis for the scientific community and the reviewers of a publication. Secondly, the category definitions form the basis of the coding guide used by the coders. This means that the better the definitions and the clearer the examples, the better the coding and the higher the probability of achieving a good match between the coders will be.

The findings from previous research that have been discussed in the literature review are used to ground the findings of the semi-structured qualitative interviews. Another layer of differentiation will be incorporated by selecting a randomized but varied set of participants. These measures together should result in a conclusion with as little bias (Carter et al., 2014).

3.8 Qualitative survey

A qualitative survey has been chosen to extract the most in-depth information from the participating organizations. The aim was to link their experiences to the existing literature about ISO 9001 & 27001 implementations in other sectors.

The interview is divided into different parts, being: introduction to the interviewee and organization, pre-ISO 9001 and/or 27001 implementation(s), ISO 9001 and/or 27001 implementation(s), post-ISO 9001 and/or 27001 implementation(s), Double implementation, no ISO 9001, and no ISO 27001. A short explanation per part will be provided below.

3.8.1 Introduction to the interview

The interview starts with a couple of control questions. These questions aim to ease the interviewee into the conversation and set benchmarks for comparing the interviewed organizations. These benchmarks are important for accurately comparing the results of the subjected organizations. These background questions are key as multiple other studies have shown that these might have an impact on ISO 9001/27001 implementations in other sectors, as will be explained in table 3.3.

3.8.2 Pre-ISO implementation

The pre-ISO implementation questions cover topics like motivation and goals of the ISO implementations. Studies have shown that these topics are inherently linked to the level of success in achieving certification. As well as, experiencing more benefits and fewer negatives due to the implementation as will be explained in table 3.3.

3.8.3 ISO implementation

The method of implementation is an integral part of how much success an organization has with implementing any new tool or certification (Poksinska et al., 2006). These questions cover the entire process of implementing the standard and getting audited for certification.

3.8.4 Post-ISO implementation

Implementing the standard and getting the certification is just the first step of the ISO 9001 and 27001 standards. Jose Tari et al. states that internalization of the standard is a key factor in achieving the biggest benefits of implementing an ISO standard. Furthermore, he states that not actively practising the guidelines of the standards can be costlier and more time-consuming over a longer period.

Also discussed in this chapter are the experienced (dis)advantages of the implementation of an ISO 9001 and/or 27001 standard(s).

3.8.5 Double implementation

Multiple studies have found that both advantages and challenges can be experienced by implementing both ISO 9001 and 27001 simultaneously (Calvache et al., 2015) (Zeng et al., 2007) (Poksinska et al., 2006) (Alcina A. de Sena Portugal Dias, 2016). These questions aim to find out which of these (dis)advantages have been experienced by the interviewee organizations.

3.8.6 No ISO 9001

In the section, 'No ISO 9001', interviewees will be presented with questions that are aimed to delve into their organization's reasoning for (hypothetically) wanting to implement and get ISO 9001 certified. Other presented questions are aimed at delving deeper into the organization's relationship with quality management.

3.8.7 No ISO 27001

In the section, 'No ISO 27001', interviewees will be presented with questions that are aimed to delve into their organization's reasoning for (hypothetically) wanting to implement and get ISO 27001 certified. Other presented questions are aimed at delving deeper into the organization's relationship with information security management.

3.8.8 End of interview

The 'end of interview' section is used for administrative topics and for allowing the interviewee to elaborate on any topics they have previously discussed, or topics which they feel should have been discussed in the interview.

3.8.9 Interview question list

Table 3.3 shows the breakdown per question explaining the use of each question asked. While most questions aim to answer the research questions, others only serve as a purpose for people to feel inclined to answer.

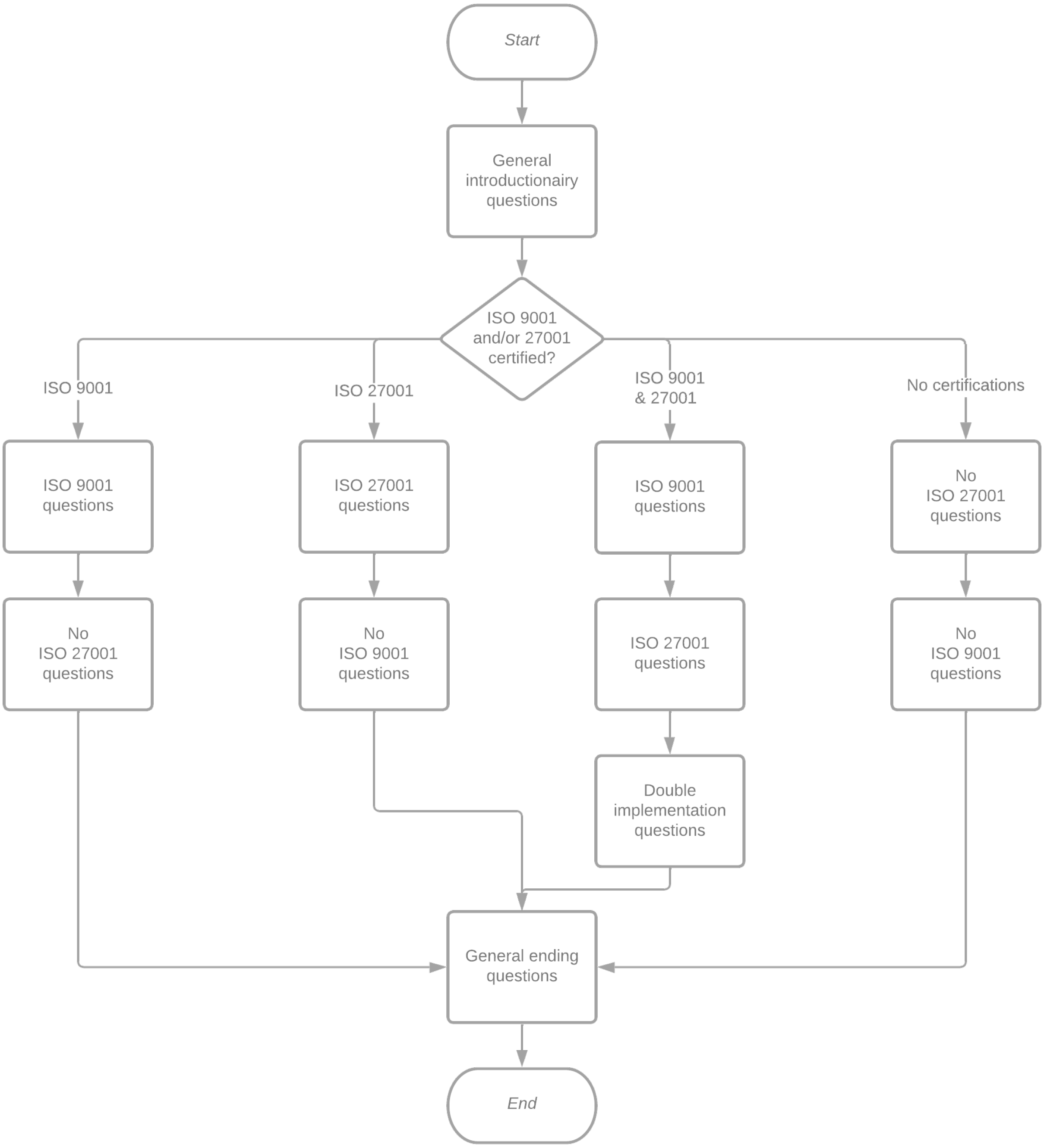


Figure 3.2: Questionnaire flowchart

Survey question	Reason
What is your name and role within your organization?	Administrative reasoning. Answers are redacted in the published document for confidentiality. Asking personal questions at the beginning of an interview is an icebreaker to ease the mood.
How many employees does the organization consist of?	According to Zeng et al. the size of an organization can have an impact on the success of implementing ISO 9001 and/or 27001. Smaller organizations may face resource constraints or lack of expertise.
Can you provide an estimate of last year's revenue?	According to Zeng et al. the level of financial resources that are available to an organization can impact their reasonings and ability to implement ISO 9001 and/or 27001
How would you describe the structure of the organization (Hierarchical, flat, etc.)?	Poksinska et al. has stated that organizations with more complex structures and operations may face greater challenges in implementing and maintaining the ISO standards. A higher level of complexity may require more time, resources, and coordination to achieve compliance with the standards.
What project management methods do you use?	According to Poksinska et al. the method of setting up the team or individuals responsible for the implementation of the ISO 9001 and/or ISO 27001 standards can influence the success of the process. However, the best project management method seems to be related to the structure of the organization.

Does your company find it difficult to attract new IT staff?	Used for determining a possible relationship between a lack of employees to the lack of human resources invested in implementing an ISO 9001 and/or 27001 standard.
Do you agree, or disagree with the following statement: ”Changes within IT are moving faster than in other sectors”?	Used for the hypothesis question of this research. To be followed up on later in the interview.
In which versions of the ISO 9001 and/or ISO 27001 standard are you certified?	To document which version and iteration of the ISO 9001 and/or 27001 the organization has been certified in. Determines the remainder of the questions that are to be asked to the interviewee.
What was the motivation behind the decision to go for an ISO 9001/27001 certification? (Have there been situations that you wanted to avoid, market considerations, legal, competition, etc.)?	Multiple studies have shown that organizations with strong internal motivations are more likely to realize the full benefits of an ISO 9001 and/or 27001 implementation, as they are more likely to stay committed to the internalization of the standard into daily operations (Heras-Saizarbitoria and Boiral, 2013) (Santos and Escanciano, 2002) (Naveh and Marcus, 2005).
When would you define the implementation of the standard as a success? Were any specific goals set beforehand?	Related to the question about motivations. Aimed to clarify the definition of success for an ISO 9001 and/or 27001 implementation is the same across all interviewees.
Can you describe the implementation process? Did you do this independently or with a consultant?	Open question for the interviewee to share their experience during the implementation process
Did you perform the implementation on your own or did you hire a consultant?	According to Singh et al., a consultant can help increase the likelyhood of a successful ISO 9001 and/or 27001 implementation.

During the implementation, did you take into account the standard project management technique used within your organization?	According to Poksinska et al. the method of setting up the team or individuals responsible for the implementation of the ISO 9001 and/or ISO 27001 standards can influence the success of the process. However, the best project management method seems to be related to the structure of the organization.
How did you ensure that the standard is embedded in the daily activities of your employees.	Organizations that internalize the ISO 9001 and/or 27001 standards in their daily operations seem to experience more of the benefits that these standards can offer than those who do not (Heras-Saizarbitoria and Boiral, 2013) (Santos and Escanciano, 2002) (Naveh and Marcus, 2005).
What were the roles of the employees who participated in the implementation process?	Aimed at finding out how many resources were allocated to the project (Al-Rawahi and Bashir, 2011), and to which level the implementation of the ISO 9001 and/or 27001 standard has been diffused across the organization (Alcina A. de Sena Portugal Dias, 2016).
Do you use special software to maintain the management system?	The researcher has hypothesized that IT-companies tend to use IT solutions whenever possible. Perhaps this could also be of influence in their standard internalization.
What did you learn from the implementation process? What went well, and what would you do differently?	Open question for the interviewee to share their findings on the implementation process and to share if and what they would improve on the process if they had to redo the implementation.

What is the most important thing to take into account before, during, or after an ISO implementation process?	Open question for the interviewee to share more on what they see as the biggest pitfall during an ISO 9001 and/or 27001 implementation process.
How has the way your employees deal with Quality Improvements/Information Security changed since the ISO implementation process?	Organizations that internalize the ISO 9001 and/or 27001 standards in their daily operations seem to experience more of the benefits that these standards can offer than those who do not (Heras-Saizarbitoria and Boiral, 2013) (Santos and Escanciano, 2002) (Naveh and Marcus, 2005)..
What disadvantages do you experience after the implementation of the standard (Bureaucracy, cost, culture, etc.)	For finding the experienced disadvantages of implementing an ISO 9001 and/or 27001 standard in their organization. Used for laying links between the implementation process and the experienced disadvantages of the standard(s)
What advantages do you experience after the implementation of the standard? Are there any advantages in operational performance?	For finding the experienced benefits of implementing an ISO 9001 and/or 27001 standard in their organization. Used for laying links between the implementation process and the experienced benefits of the standard(s)
How big do you estimate the influence of the speed of the technological changes in IT to be, on the implementation of ISO 9001/27001?	For answering the hypothesized question ”Does a high rate of technological changes affect ISO 9001 and/or 27001 implementations for IT companies?”

Do you think that a higher degree of modularity in the standard or your management system software will be able to better facilitate the speed of changes in technology.	For answering whether a proposed solution to the hypothesized problem, ”Does a high rate of technological changes have an effect on ISO 9001 and/or 27001 implementations for IT companies?”, would be a good solution. Relevant as the introduction of ISO 9001:2015 and ISO 27001:2013 have introduced higher levels of modularity in the standards (ISO, 2019).
Double implementation: Have you implemented the ISO 9001 and 27001 standards simultaneously?	Control question to find out whether the organization implemented the ISO 9001 and 27001 standards sequentially or simultaneously. As multiple studies have found that both advantages and challenges can be experienced with implementing both simultaneously (Calvache et al., 2015) (Zeng et al., 2007) (Poksinska et al., 2006) (Alcina A. de Sena Portugal Dias, 2016).
Double implementation: To what extent is the acquired knowledge and documentation overlapping between the two standards? Is there a way to reuse this information when implementing a second standard?	Calvache et al. have found that implementing the standards together can lead to more efficient use of resources and shared documentation.
Double implementation: Are any quality management and information security management systems integrated, or do you use separate systems for this?	Research by Calvache et al. and Disterer have found that implementing the standards together can increase efficiency by reducing duplication of effort, and unifiying their approach to continuous improvement.

Double implementation: Has the High Level Structure Influenced your choice in this respect?	The High Level Structure has been introduced by the International Organization for Standardization (ISO) for improving the interoperability amongst the ISO 9001 and 27001 standards (ISO, 2019).
Have you looked at the ISO 9001 standard before?	Open question aimed to find out what the interviewee knows about the ISO 9001 standard.
No ISO 9001: How is quality improvement currently being looked at within the organization? Is the course of this being reviewed? If so, at which level is this happening?	Question for potentially explaining the company reasoning to not having started, or not looking to pursue an ISO 9001 certification.
No ISO 9001: Can you give an example where a delivered service or product could not meet the quality requirements of the customer?	Aimed at finding out if the organization has had to deal with the quality of their service or products not meeting their clients expectations and how the organization generally handles these situations. This could potentially help to delve deeper into the organizations relationship with Quality Management.
No ISO 9001: How big do you estimate the influence of the speed of the technological changes in IT to be, on the implementation of ISO 9001?	For answering the hypothesized question ”Does a high rate of technological changes affect ISO 9001 and/or 27001implementations for IT companies?”
No ISO 9001: From what motivation would your company possibly DO want to implement an ISO 9001 standard?	For the interviewee to share their (hypothetical) reasonings for (potentially) wanting to get ISO 9001 certified
No ISO 9001: From what motivation would your company possibly NOT want to implement an ISO 9001 standard?	For the interviewee to share their (hypothetical) reasonings for (potentially) not wanting to get ISO 9001 certified
No ISO 27001: Have you looked at the ISO 27001 standard before?	Open question aimed to find out what the interviewee knows about the ISO 27001 standard.

No ISO 27001: How is information security currently handled in your organization? Are there any formalized plans? Do employees pay attention to possible security hazards?	Question for potentially explaining the company's reasoning to not having started, or not looking to pursue an ISO 27001 certification.
No ISO 27001: Has your company ever had to deal with an information security breach? If so, what was the impact? If not, what could hypothetically be the impact of this?	Aimed at finding out if the organization has had to deal with information security breaches and how the organization generally handles these situations. This could potentially help to delve deeper into the organizations relationship with Information Security Management.
No ISO 27001: How big do you estimate the influence of the speed of the technological changes in IT to be, on the implementation of ISO 27001?	For answering the hypothesized question "Does a high rate of technological changes affect ISO 9001 and/or 27001 implementations for IT companies?"
No ISO 27001: From what motivation would your company possibly DO want to implement an ISO 27001 standard?	For the interviewee to share their (hypothetical) reasonings for (potentially) wanting to get ISO 27001 certified
No ISO 27001: From what motivation would your company possibly NOT want to implement an ISO 27001 standard?	For the interviewee to share their (hypothetical) reasonings for (potentially) not wanting to get ISO 27001 certified
Is there anything you would like to add to your statements, or is there anything I forgot to ask?	Open question for the interviewee to add on anything they have already discussed, or to add something on a topic that they feel should have been discussed during the interview.
If I have any additional questions, may I contact you at a later date?	Facilitating question

Table 3.3: Breakdown of survey questions

Chapter 4

Results and Discussion

This chapter will draw upon the main themes and present the findings from the interviews. Each of the research sub-questions will be answered using the findings from the interviews. These findings will also be grounded in the literature whenever possible.

4.1 How do the structures of the ISO 9001 and 27001 standards relate?

Information, quality, availability, and continuous improvement are core pillars of both the ISO 9001 and the ISO 27001 standards. Both are tools for management to get more grip on the quality and continuity of their business. They also share the same philosophy of continuous improvement by incorporating the Deming Cycle in their guidelines (Rousse, 2020).

The ISO 9001 standard for quality management and ISO 27001 standard for information security management are also similar in their approach to a management system. In recent versions of the standards, a High-Level Structure has been introduced that aims to make the standards easier to align. This allows for easier integration of both standards into a single management system. The implementation of this could be done simultaneously or at a later date (Wang and Tsai, 2009).

The integration is also helped by the fact that both standards are PDCA cycle-based management system standards. Meaning that many clauses in the ISO 9001 and 27001 standards are the same or similar. This can have the benefit of not needing to repeat documentation and processes (Simon et al., 2013) (Hoy and Foley, 2014).

Other benefits come from the already established document control procedures, communication channels, and the governance structure in which the management system is discussed. Using this pre-existing infrastructure for the implementation of a new ISO standard might enable the saving of resources. Methods for generating awareness and improving internalization of the new addition to the management system in the organization's processes and culture. However, how much this helps is difficult to quantify since it changes with each organization (Hoy and Foley, 2014).

Differences in implementation methods stem from the different ways an organization is structured and managed. An agile way of working requires a different implementation method than a waterfall developing method. How this is implemented is solely at the discretion of the organization that is implementing the standard. This is because the ISO 9001 and 27001 standards are formulated generically, as to make them applicable to a wide range of organization types. Each organization can implement the standard to a level that is adequate for its organizational purposes. However, this means that during the certification audit, the organization must be ready to support their reasoning for implementing the standard in this way (Hoy and Foley, 2014) (Simon et al., 2013).

According to Zutshi and Sohal, a reduction in the amount, duration, and cost of auditing could also be experienced. The effort of planning, preparing, and follow-up activities related to the auditing process were also reduced (Kraus and Grosskopf, 2008) (Zutshi and Sohal, 2005). Integrated audits can be performed after the implementation when two or more management systems of different disciplines are implemented in an organization. (Kymal et al., 2015)

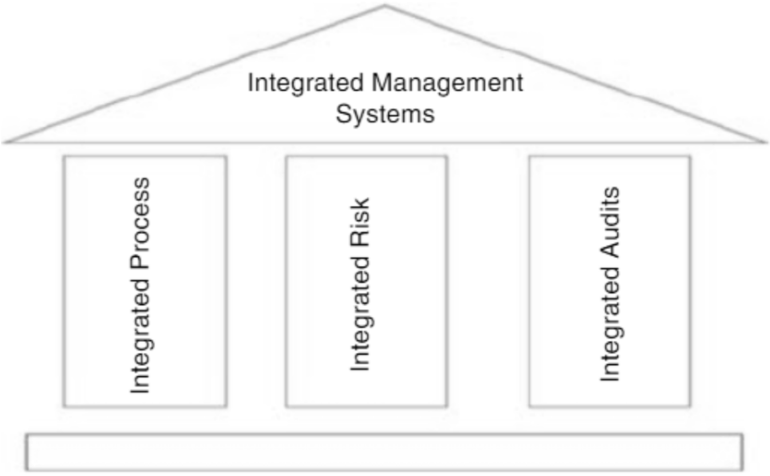


Figure 4.1: Integrated audit process for integrated management systems

There are still some potential risks found with the ineffective implementation of an integrated management system (ISO 9001 & 27001). One of them is the potential of conflicting documentation and processes for the different system standards (Celik, 2009). Furthermore, the information management systems used by different teams may conflict. For example, in the case of measuring objectives and key performance indicators for each system, ISO 9001 and 27001 have different objectives. The implementing organization will then need to find a trade-off that best fits their needs (Zeng et al., 2011).

The resource availability and management commitment issues that have been mentioned as failure causes and effects for the individual standards are an even bigger risk during the implementation of an integrated management system (ISO 9001 & 27001). Organizations that fail to manage these risks for a single ISO standard implementation should certainly not try to implement both standards simultaneously. As this will only exacerbate the previously mentioned issues and increase the risk of failure to implement any of the ISO standards (Zeng et al., 2011) (Hoy and Foley, 2014) (Zutshi and Sohal, 2005).

One company has stated that when the ISO 9001 standard is present, it has become easier to implement the ISO 27001 standard. This is due to the process of information handling also being a part of the ISO 9001 standard. According to them, the introduction of the HLS has improved the ability of the standards being used alongside each other. Besides that, it has also made it faster and easier to implement a second standard. This is due to the implementation processes that can be reused, such as the analysis of stakeholders, requirements, and responsibilities. As well as the creation of awareness, and competence through training, communication processes, and the control of system documents being shared.

The core message that you cannot have quality software if it is not secure and vice versa, is repeated by multiple of the interviewed parties. With this statement, they say that the relationship between the QMS and the ISMS transcends into the quality and security of the software itself. According to the company, A program that gets hacked and is turned against the user is thought of by the client as not having good quality in addition to being insecure. A program that is of poor quality often has more vulnerabilities, which leaves it insecure despite countermeasures being in place.

"In the end, you can not supply your customers with a product that is of good quality, but not safe. Or a product that is safe, but not good quality. So that is linked to each other. Where 9001 has added

value for us is that it forces you to take a better look at your supporting processes. So you need to take a look at your sales process and your contracts. How do you make sure that you dot your i's right there? This also includes your after-care program. Which includes project evaluations, complaint handling, maintenance, etc... These are 9001 parts that do not get enough attention in the ISO 27001 standard." (company 4)

This shows the increased importance of a double implementation of a QMS (9001) and an ISMS (27001) for an IT company as compared to other sectors. Information security is not just a side job for the IT sector. It is a part of their core business processes.

4.2 Why do IT organizations choose to pursue ISO 9001/27001 certification?

Getting certified to fulfill client requirements seems to be closely related to the type of clients that an organization is focusing its efforts on. If an organization's clients tend to require ISO 9001 and/or ISO 27001 certification it can be seen as a requirement to get certified to even be considered for certain jobs. However, any unique selling points that could have been gained seem to no longer be relevant to the IT sector when too many competitors have already achieved this certification as well.

Despite earlier stated numbers suggesting that there is a lower amount of ISO 9001-certified IT companies (Mcadam and Fulton, 2002), one of the companies experienced something contradicting. In their experience, the returns for getting ISO 9001 certified might be on the decline. As the company mentioned: *"You do take some competitors out of consideration during work offer processes if your customer requires the ISO 9001 standard and they do not have it. However, the ISO 9001 standard has become more or less a standard for the services we provide. So the returns there are decreasing steadily."* (company 3)

Company 6 agrees with this sentiment. Stating that the amount of clients that are asking for ISO 9001 is "quite limited and even seems to be declining".

The awareness of the potential need to pursue an ISO 27001 implementation seems to differ depending on the type of organization. As one of the companies that has both IT and non-IT organizational branches notes. *"Awareness amongst our software developers is bigger than amongst our [non-IT] consultants out of the nature of their job. What I have noticed is that there have been a few improvements to our product and the increased attention to the companies that* *we hire to support our work."* (company 3).

Companies 7 and 8 both mention the requirement of ISO 27001 certification by the clients in their sector (healthcare). Without this certification, they would be completely unable to operate in this sector. The same is true in the public sector (governmental agencies), according to company 9.

Company 9 also experiences it from the other side of the client requirements. They are now the ones asking these questions to their suppliers and customers. Due to this, some of them have started to obtain the certifications. This in turn helped them be able to collaborate more closely with said clients and/or suppliers without having to go through a risk mitigation process.

Next to client retention and the quality of their products, company 5 mentioned a certification reason that has not been mentioned in any other research. *"Because we originated from a small organization in which certain people had a lot of important specific knowledge. We want to reduce this so that people may be able to take a holiday once in a while. So we are active in making our organization able to take a hit. That requires structural thinking about your organization, which can be outside of your normal thought patterns."*

Another new factor for getting certified in ISO 27001 is saving time during a tender process. *"You can partly do this by showing your clients that certificate, proving that an external party is auditing your information security. A different option would have been to perform individual audits for each client and their needs. This would mean a lot of extra reports, and now we can just show them our certificate. Everything extra that our clients require will still need to be audited individually. But it can largely be replaced by the ISO certificates."* (company 5). Company 6 finds this to be true for both ISO 9001 and 27001 certifications.

Additionally, company 6 has stated that having to write out all of your processes for the ISO standards not only benefits your customers. *"But also your value as a company towards a merger partner"*. The certification itself is said to increase the company's value. But it also helps in aligning the business processes of both companies.

Because the ISO 9001 and 27001 standards make an organization write out an overview of its way of working, it also helps the organization reflect and gain a better understanding of its core qualities.

"Making that transition from a 'Cowboy Company' (read: fast-changing, focus on latest technology)

to a more established and structured company is something that an ISO standard implementation can contribute to. "We used to always say yes. And now we know what we do and do not want to do. We have become more secure about ourselves as a whole. It has helped us. If you know the strong points of your organization, then you know which type of jobs you can say yes to and where you can deliver a qualitative product." (company 4)

Organizations do seem to see a bigger need for pro-activity in the realm of data protection. *"Data is increasingly becoming more important in the world. And that the worth and risks of that data are huge for an organization like ourselves, and those are increasing. So we want to get this under control to not be confronted afterward with things that went wrong."* (company 1). This is also mentioned by company 7 as a key point for implementing the ISO 27001 standard. *"You have to shield that data and always give as little rights as possible. [...] The data you share with third parties as well."*

Company 5 adds pro-activity towards their clients in this as well. Mentioning that the GDPR (General Data Protection Regulation) regulations have made them look outside of their organization for data protection as well. *"You have become a much larger part of the supply chain, where you used to be the IT silo"*. Thus an organization that is looking to get ISO 27001 certified should not only look towards themselves but also look at their suppliers.

The role of an IT organization towards a client also seems to shift. *"We are now more in an advisory role. Now we are in a position where if the client does not meet the agreements that we have made on a quality or information security level, we can say something about it. And that you include this in your risks, as it can be something that comes around to you."*. (company 5). The same sentiment is shared by company 4.

Company 8 states the following in regards to choosing ISO 9001. *"Purely to keep the quality of the code in order. So that the code works efficiently and well that there is no downtime in the system. Because your clients rely on our systems to be running."*

Going for ISO 9001 and/or 27001 certifications is not necessarily valued by everyone. The reasoning for this does vary.

Company 1 mentions hesitancy for both standards due to fear of writing unused documentation. *"Reasons to not pursue [ISO 9001] would be a fear of writing documents that no one is reading afterward. So losing the added value is something we are weary of. It needs to lead to a benefit for our clients and our revenue right. You can only spend your time once. [...] If our employees feel* *that they need to write a lot of documents that are not useful. Then I think the energy for following the standard would quickly disappear."* This fear is also shared by Company 2.

Company 2 mentions a lack of human resources as a big reason for not looking towards getting a certification in any of the ISO standards. They, just like all other companies, were having issues hiring enough knowledgeable IT employees. This seems to translate into not having the resource capabilities. *"I am not going into a certification project. That is not one of the things that is currently on our minds. The people that you need for such a project are often your 'hotshots', and we need those at our customers."*

For company 3, ISO 27001 certification just wasn't enough of a benefit or requirement when looking at the type of product that they were providing.

4.3 What are the criteria for IT companies to consider an ISO 9001/27001 implementation a success?

The reasoning for a company to get certified in ISO 9001 and/or 27001 does not necessarily have to be the same as their criteria for a successful implementation of the standards. The same could potentially be said for the success criteria before implementing one or both of the ISO standards, as compared to when the implementation has been completed.

Most of the organizations that have been interviewed have at least partially implemented one or both ISO standards due to the clients requiring them to be certified. Therefore, all of them also mention achieving the certification as one of their criteria for success.

Where things start to differ is when you compare organizations that have already achieved an ISO certification with those that are yet to implement the standard. One of the companies that do not have ISO 9001 and ISO 27001 implemented mentions getting certified as their primary success criterion. While the other company without both certifications also mentioned being more proactive in finding and solving issues, and protecting competitive advantages.

This latter view aligns with those who have implemented the ISO 9001 and/or 27001 standards. Some also started by implementing one or both standards due to their goal of getting certified. However, they would later start to find other reasons as to why they would start to describe their implementation process as a success.

"It has truly helped us as a company. There are always a couple of loose ends, which you know that

you need to improve them. This process has forced us to find solutions for these issues. And it forces you as an organization to think about how you want to do things. It gives a lot of clarity to your co-workers, including new colleagues. Because you describe how you work, so it is easier to catch up." (company 4).

What is also noteworthy is the possible relationship between already having implemented one of the standards and seeing the success criteria to be focused more towards internal improvements as opposed to external factors. Where the company that only has an ISO 9001 certification mentioned topics such as system availability and data integrity as their primary success criteria, among the external factors of *"company image"* concerning ISO 27001 and being able to bid for jobs due to an external certification requirement with both of the standards.

Lastly, it seems that if any success criteria have been formulated, besides getting the certification, they are more often a high-level goal.

"Well the implementation itself would be the biggest of our goals. But apart from that we did not have any specific goals for the certification itself. Although, at the time we did have goals that suggested the direction of certification. The expansion of our clients with larger customers where we needed to map our processes. The entering of the healthcare market explicitly required us to have our 27001 measures in place. So there were goals that were aimed at achieving the certificate. But nothing as to have a maximum amount of nonconformity, etc." (company 5).

A notable exception to this is company 7. For their ISO 9001 implementation, they specifically challenged themselves to increase awareness on the topic of code quality amongst their employees. And gave this more prominence in the way that they produced their products. They say to have achieved this goal. But this benefit has not previously been mentioned by any other interviewed company.

4.4 How can the philosophy of the ISO 9001 and 27001 standards be internalized into an IT organization's day-to-day activities?

Internalization is the concept of effective adoption of principles and practices by managers, decision-makers, and operators in their daily work (Briscoe et al., 2005). They describe a higher, more rigorous, or more active fulfillment of the requirements of the ISO standard (Jose Tari et al., 2013) (Cai and Jun, 2018). Which, in the case of the ISO 9001 and 27001 standards, means that the philosophy of the standard is embedded in the day-to-day activities and thought processes, of the employees and managers.

The level to which an organization applies the requirements of the quality standards in their day-to-day activities as a way of integrating the philosophy of that standard and seeking to continuously improve on the current situation is called the level of internalization (Naveh and Marcus, 2005). If an organization wants to experience the full benefits of an ISO standard, it needs to go further than just documenting its processes, filling in records, and defining responsibilities. Organizations will need to make the requirements of the standard a part of their daily practices and strive to improve these processes through continuous improvement efforts (Garstenauer et al., 2014) (Lin and Wu, 2007).

This entails knowledge transformation and knowledge transfer through education and process improvement in a cycle of continuous improvement. The employees require explicit knowledge of the firm's processes through documentation and experience, to be able to improve the processes by coding and documenting the improved processes. Thus spreading the new information across the rest of the organization (Cai and Jun, 2018). This continuous process is translated into four major ISO 9000 internalization processes: documentation, process improvement, education, and auditing (Table 4.1).

High-level categories	Low-level categories
Education	Management training Employees training Auditors training Persuasion Continuous training
Documentation	Employee interviews Employee self-report
Process improvement	Resolving differences between co-existing procedures Gap correction Developing new procedures
Auditing	Continuous internal auditing External auditing

Table 4.1: ISO 9000 internalization processes (Cai and Jun, 2018)

Better quality of delivered products or services leads to higher job satisfaction as employees get positive reactions to their work. Seeing the results that the ISO standards can have on their quality of work will, in turn, result in a higher level of affective commitment to the standard and its internalization within the company (Heras-Saizarbitoria and Boiral, 2013).

This is reflected in the interview results where is shown that delivering poor quality of work or experiencing data breaches can negatively impact employee job satisfaction (companies 1 and 2).

All companies with ISO 9001 and/or 27001 certifications have noted that they have at least one person appointed as the dedicated quality and/or information security manager. They have also all used the expertise of an external consultant to help them get acquainted with the ISO standards during their implementation process. However, having an external consultant is not seen as essential as long as you know within your company, or are willing to invest the time in getting this knowledge. *"If you are planning on training a dedicated person within your company to be the quality or information security manager who is going to extensively learn about the standard, then I think you can do it without a consultant."* (company 4)

Company 4 also noted that a consultant can help because they look at your organization with a fresh mindset, and have a lot of experience in facilitating the process. *"An internal employee tends to go with the status quo of the current workflow. An external consultant is better equipped to show empathy for the status quo, but still be hard on things that are required for the certification. The consultant can be a bit harsher in this as he or she does not have to be the friendly coworker during the next lunch."* (company 4)

five of the seven companies that have achieved ISO certifications mention that they have incorporated their employees in the writing of the Quality and/or Information Security Management system. They state that the people who are the most capable of describing their way of working are the employees themselves. Those employees were then assisted by the internal quality/information security manager and their external consultant. They also state that this helps them internalize the thought process that is dictated by the standards of their employees. And it also helps their employees gain more insights into their processes and those of their colleagues.

The other organizations used a more centralized approach in which the internal quality/information security manager picked a couple of key users and wrote the management system with their help. They did mention that they would like to somehow change the perceived tone of processes being dictated by the ISO standard towards being their own standardized best practices.

"In the beginning, they come in and perform a lot of interviews about how we work. They wrote some things down and then a few key figures in our organization came in for a few sessions to check

if the written-down methods were how we wanted to work. Following that we established a set of procedures detailing how we would like to be working. We would adapt the organization where this did not match the specified working instructions. So in some places, we needed to adapt our change management to make it more robust. This was mostly 9001-directed. Following this we would look at our Quality Management System, partly with the help of the consultant, partly on our own, to see which parts of the 27001 standards were not covered by our 9001 management system and add them." (company 5)

This organization does state that they were struggling with the internalization of the standards during the earlier stages of the implementation. Employees were hesitant and had concerns about specific cases. They mention that shifting the story from *"This is the direction we are heading"* to *"How this would make their work easier"* is what helped in this process. *"In that aspect, we also took a good look at who would emotionally not be able to deal with certain changes and help facilitate these people by having conversations with them to keep the expectations as real as possible."* (company 5)

Company 6 experienced something similar. *"Chief Information Officer (CIO) and I largely manage the management system, and we are part of the leadership of the company. So basically, we kind of interview ourselves. This year, however, we took a different approach. I invited all employees to an online session to talk to each other about how they think things are going. And whether we are doing enough in terms of information, quality, and where the risks are. I do believe in that idea of keeping it alive."*

Companies 4, 6, and 9 also state that they feel the benefit of continuously training and assessing their employees to gauge engagement with the standards. According to them, this not only keeps the guidelines of the ISO standards fresh in their minds but also helps them to find where they still have to improve their internal and external processes.

Making sure that the standard is easy to locate is also mentioned as an important step by two of the companies. How this is done is left to the organizations themselves. Both companies 4 and 5 have detailed descriptions of workflows in the working spaces of the departments themselves, and a more general overview of the management team in which they describe responsibilities, reports that are to be made, and what is being monitored.

Company 4 quoted a competitor from during an ISO management knowledge exchange session, on a situation where the management system was not readily available and how this would negatively affect the internalization of the standard. *"Our consultancy firm also* *hosts group sessions which I sometimes attend. In this session, there is also someone who wrote it down in Word documents which can be found somewhere in their network. But now she is very surprised that their co-workers never look at the documents. She showed me the documents that were on a map, with more maps inside and even more documents and maps inside. I can understand why none of her co-workers look at it."*

Company 5 stated that there is a risk to the employees only looking at their processes in the Management System. *"People were too focused on their processes in 'the blue book' [their Management System]. 'The blue book' does not describe outputs and inputs, it only describes what the process does. So this can mean things like supplying the administration with an Excel document, while they are expecting a PDF file. This created a lot of discontent among our employees"*

Their organization has now adopted sessions in which they look at the gaps in their handover process. *"This means sitting together and taking a look at how we are working. You write down what you do, how you do it, and how and to whom you hand over your results. Your coworker does the same, which allows you to see how they expect you to do the handover. And often there is a gap between what is transferred by one employee and what is expected by the following employee. This process was started last year and has helped streamline communications. As well as create more of an understanding for what the other employees are doing and what they need to succeed."*

Keeping the standard light, maintainable, and agile is mostly mentioned in how to write and maintain a Quality and/or Information Security Management system. *"Bureaucracy works less well in these cases. The personality of the average IT staff member tends to clash with such a way of working."* This is what company 3 said when asked how to best internalize the ISO standards in their way of working.

This aligns with one of the proposed ways to deal with overburdening by documentation. Which is to incorporate the creation of Quality Management System documentation in activities such as review meetings and the writing of design documents. This way of working is based on the teachings of an *"agile"* way of working. Where it is the goal to try to avoid documenting things that do not contribute to the finished system or process. However, it is unknown if this would also work for the ISO 27001 standard documentation (Stålhane and Hanssen, 2008).

4.5 What are the differences between the implementation of ISO 9001 and 27001 at IT companies as compared to the implementation at other types of companies?

One company stated: *"I think that during this process (referring to ISO 9001 implementation process) there have been many things that have already been picked up and incorporated into our business. [...] I think that we have implemented the parts of it, which are most important for our company"* (company 3). They referred to the fact that parts of the ISO 27001 standard had already been covered during their initial ISO 9001 management system implementation.

They later stated that they felt sufficiently safe in how they secured their information. Thus, feeling no need to get ISO 27001 certified at that time. However, they did feel that getting ISO 27001 certified would be *"shorter and less intense"* because some requirements had already been met.

Company 4 mentioned *"ISO fatigue"* to be a big reason for not implementing both ISO 27001 and ISO 9001 and the same time. According to them the process of implementing ISO 27001 took 1.5 years to complete. After this, they took the time to further internalize the processes of the ISO 27001 standard. *"You are glad you are certified, the auditor comes each year. And after two years things have finally settled down and everything is embedded in your daily activities. So we felt like we were ready for another project, let's do ISO 9001. We have always thought that ISO 9001 would not be so much work. Which it was not. This is because, as an IT company. If you are ISO 27001 certified, you inevitably think about quality in a lot of ways."*

Company 6 has found no issue with doing a simultaneous implementation of both ISO 9001 and 27001 standards. *"It is certainly somewhat related, isn't it? Safety is an aspect of quality, of course. Vice versa as well. [....] We did it at the same time, partly for the reason we just discussed. But also that many aspects of how you deal with them are pretty much the same. So that was very efficient to do together."*

Company 5 has done a simultaneous implementation of both ISO 9001 and ISO 27001 standards. *"At the time it was quite a lot of work. Because the standard was deviating quite a bit. But with the new standards I would say, just do them at the same time. Because organizational changes happen anyway. And you do need to take the time to introduce the changes. Otherwise, you are just double reserving this time. Besides this, these are two subsequent standards that make me think it is better to do them together. This will allow you to look at your entire organization at the* *same time and not be introducing changes constantly. As you want to come to a time where you can just operate as usual within the certification."*

When asked if they would do anything different in this process, the company responded that they would like to spread the process out over a longer period. *"As an organization you pick a focus point, which means that the rest around this takes a back seat. Which could result in gaps starting to form in what you have already built up. It most certainly is not a linear curve towards the top."* They also mentioned that this would help give them more chances to talk to employees and to help alleviate their concerns.

The company refers to a possible stronger link between quality software and secure software, or at least the process of developing and maintaining the software. This lines up with the findings of Mouratidis and Giorgini and Walker that stated that a secure software application that is free from security vulnerabilities tends to be of a higher quality.

Company 4 also mentions how they felt that the processes that they needed to describe for the ISO 9001 standard supplemented those which they needed to describe for the ISO 27001 standard well. They said that after already implementing ISO 27001, implementing ISO 9001 forced them to take a better look at their supporting processes. Parts that they said did not get enough attention in the ISO 27001 standard but did have an impact on both (perceived) quality and security.

All interviewees have stated that there is a larger affinity for the topic of information security among their IT employees. This makes them more likely to understand the need for and requirements of the ISO 27001 standard.

There also seems to be a substantial overlap between ISO 9001 and ISO 27001 in regards to describing an organization's way of working in their Management System. Companies 4, 5, 7, and 8 mentioned their experience of implementing the second ISO standard to be easier. *"You find that the things that you have to pay attention to in your process for implementing the 27001 standard do correspond to some parts of 9001 as well. And so you benefit from it. There is some overlap."* (company 7)

Finally, the continuously returning idea that software quality and software security are linked also indicates a stronger relationship between both standards for the IT sector than in other sectors. As is noted by company 3, *"Because we do supply a certain measure of quality through the ISO 9001 standard we can expect ourselves to be able to provide a certain quality of* *the product that is quite safe to use."* This experience is shared by company 6: *"It is certainly somewhat related, isn't it? Safety is an aspect of quality, of course. Vice versa as well."*. And company 8: *"If the code is just not right, then it can't be a good product. If it is not efficient or it contains many errors, that could be dangerous."*.

4.6 Does a high rate of technological changes affect ISO 9001 and/or 27001 implementations for IT companies?

Three out of five companies agreed with the statement: *"The technological advancements in the IT sector move at a faster pace than in other sectors."* Stating that this is a natural consequence of the sector itself and that the only places where you could see the same thing would be in other highly technological sectors.

One of the companies with ISO 9001 stated the following regarding the question *"How big is the impact of the rate of change". "I think it has a big influence on the quality system in our IT department. Because that constantly needs to be altered. [...] We have seen a movement to the cloud in recent years. This has made saving changes in a centralized way more difficult to realize. You might be tempted to say, It is saved in the cloud so it is secure there. But that might not always be true. Perhaps the ISO 27001 standard is better adapted for these changes. But ISO 9001 describes things that are more difficult to pin down like that. So these changes are important to take into consideration for your quality system, and this requires the biggest amount of work on changes."* (company 3).

Company 2 was positioned more in the middle of the spectrum with their answer. *"In a software package sense, it would. But I think as a senior developer, or a lead developer, I should be able to expect them to understand the quality standards and to use them in their processes. I think those techniques themselves do not change that quickly, it is more of an evolution. Things like code reviews, or unit testing do not change the techniques used too much. But yeah, that does not change the techniques completely. So you would not need to reinvent the wheel every three to five years."*

Company 4 disagreed with the statement. Saying that the ISO standards do not tell you how you should accomplish your goals. Only that you have thought about the impact of your choices throughout the process and that these risks are managed. They say that the certification teaches you to think about the changes that you experience as an organization. *"It all starts with taking a step back and thinking about what you are going to do, why are you going to do it, what are the risks and how can you minimize those risks."*

Company 5 disagrees, saying that other sectors also relied on IT advancements in addition to the advances that are being made in their sector. Thus arguing that the rate of technological changes that need to be managed might be even bigger in some other industries. *"For us, it is just a new product. The rate of change does not matter. But for other companies, it is a part of their business and in time it can dictate their ability to work efficiently or effectively."*

According to company 6, there should be no issue with a high rate of technological change as long as you describe the process at a high over level. The only exception they see is client sector-specific requirements, such as healthcare or public sector clients with different requirements.

The modularity of the management system also does not seem to be a requirement from the perspective of an IT organization. In regards to this company 3 says the following:

"You constantly make changes in your management system. Constant deliberations on what you should do with your product. What do our clients demand of us and what is practical? New ideas are also constantly popping up in technological development. These changes a coming at such a rapid pace that cutting up the work instructions or management system into smaller, adaptable pieces seems to be quite difficult. Because it is an evolving thing."

Company 4 agrees with this, saying: *"We have not written it down in detail like that. It remained more High-level. How do you get a company that makes build-to-order software to follow a specific standardized way of working? Because every project is different. You can not escape having to write your work instructions at a high level."*

Company 6 is advocating for a type of starter package for getting your ISO certifications. *"Give me a base for my ISO management system and then 90% of what we have now created ourselves should just be ready to use."* This interviewee found that large parts of an IT organization's way of working is something that is mostly standardized among their peers. Thinking it to be better for their business processes to match the ISO standard than for the ISO standard to match their specific business processes.

Only company 1 thinks that modularity would make maintaining their management system easier. *"There used to be a lot of physical documents, and I think that will be increasingly easy to implement in all types of systems where you can reuse those documents, and where you only need to change it a single time."*

There seems to be inconclusive evidence that the rate of technological changes affects ISO

9001 and/or 27001 implementations for IT companies. Most notably, both organizations that have been certified in both standards and can therefore be argued to have the most experience in this matter, disagree with the statement. Neither does the modularity of the standard seem to be of any influence.

The one detail throughout the stories of those who have already implemented the standards, and those who are yet to be certified, is the relation between needing to maintain the standard throughout changes. Those who view this as an issue, rate the impact of technological changes on their ISO 9001 and/or 27001 to be higher. The solution seems to be to describe the Quality/Infomation Security Management System in a high-level method. Keeping the details of a process to a minimum allows for parts of the process to be swapped out. This includes the technologies that are used.

Chapter 5

Conclusions

5.1 Conclusions

Mcadam and Fulton (2002) have found that IT organizations are struggling with adopting quality standards like ISO 9001. This is reflected in an adoption rate of 2% of all ISO 9001 certifications awarded in the IT sector in 2018. A low number compared to 20% of all ISO 27001 certifications (ISO, 2021). All despite newer versions of the ISO 9001 and 27001 standards attempting to make the standards easier to combine through the introduction of the High-Level Structure (NEN, 2020).

This research aims to uncover the possible reasons for an IT organization to get certified in both ISO 9001 and ISO 27001 standards and how a combined implementation of the ISO 9001 and ISO 27001 standards is impacted by the IT sector background. It should bring a more complete understanding of factors that could help or hinder a combined implementation of both standards and serve as a source of information for IT companies that are thinking about implementing the standards.

The goal of this research is to add scientific value by exploring the reasoning for, and effects of, a combined ISO 9001 and ISO 27001 standard implementation in the IT sector. Attempting to fill in gaps left by previous research on a combined implementation of the standards. As they have been performed on either older versions of the ISO 9001 and 27001 standards, or have not focused on the IT sector.

This research has found that the method of implementing an ISO standard can not be narrowed down to a single best practice. The reason for this is that each IT organization will have unique characteristics that make it difficult for a single standardized approach to fit all of its needs. This can also be seen in the interviewed organizations that have achieved an ISO certification. As all of them have used different implementation methods, and have appointed different amounts of resources to the implementation, while still being able to get certified.

The possible causes for these differing methods in other sectors are listed as (Hoy and Foley, 2014);

- Reasoning for implementing the ISO standards
- Acceptance criteria for the implementation of the ISO standards
- Simultaneous or sequential implementation of the ISO standards
- Available resources for the implementation of the ISO standards
- Level of experience with implementing the ISO 9001 and/or 27001 standards that is available (Internal or external)
- Work culture of the organization
- Structure of the organization
- Product and/or service offerings of the organization
- Target audience of the organization

This research has found one new potential cause for a differing method of implementing the ISO standard. This cause is the level of affinity that employees have with a given subject. 5 out of the 6 companies with both ISO 9001 and 27001 certifications have stated that their employees have a higher level of affinity with the topic of information security. All five of these companies have said that this made the process of implementing information security measures for the ISO 27001 standard easier due to a higher level of subject understanding and higher levels of commitment to making information security improvements.

Combined with the interviewee's experience that a second implementation is found to be easier, there is a potential benefit in leading with an ISO 27001 standard implementation and following this up with the ISO 9001 standard. This is due to the two standards sharing the same High-Level Structure (Zeng et al., 2011), and having a symbiotic relationship. As IT products and services can only be of good quality if it is secure and IT products and services can only be secure if it is of good quality (Mouratidis and Giorgini, 2006) (Walker, 2020). This benefit is only potential as the employee's level of affinity for the topics of the ISO 27001 standard determines whether this is true for a specific organization.

Other findings of this research are that a shared implementation is even more beneficial in the IT sector as compared to other sectors. Our interviews have found this to be due to overlapping business processes being components in both standards. Potentially resulting in a cheaper and faster implementation of a second ISO standard with the High-Level Structure, combined internal and external audits, and a shared Management System across both standards.

Implementing both standards at the same time can be a viable option if there are no major organizational changes that have to be made to achieve certification. Otherwise, this could lead to ′ change fatigue′, which results in more resistance and employee unhappiness.

The level of commitment from management and employees is stated as the biggest reason for failed ISO standard implementations by interviewees. Followed by poor communications, lack of resources (time, employees, money), lack of awareness, insufficient training, difficulty in identifying key processes and records, and culture (Hoy and Foley, 2014).

Interviewees noted finding success by communicating intentions and goals early in the ISO standard implementation process. Employees were involved in writing down their processes and were encouraged to learn about related processes within the organization. Both the interviewees as well as previous research by Cai and Jun (2018) have found that this helps in better internalizing the ISO standard.

The level of internalization also affects the benefits that are experienced from the implementation of the ISO standards. This research has found that organizations often started out wanting to get ISO-certified due to client demand, but have seemingly found additional benefits after internalizing the standard in their daily operations.

A high rate of technological changes seems to have a limited effect on the implementation of both ISO 9001 and 27001 standards. Interview correspondents have stated that this is likely due to the standard already encouraging organizations to write their processes at a high level. Thus, being less dependent on a specific technology and more on one′s way of working. Describing processes on a high level could help prevent the management system from becoming time-consuming to maintain (Stålhane and Hanssen, 2008).

5.2 Limitations

As previously stated in *chapter 3*, Methodology, there were some limitations found to interview subject sampling, the analysis of data, interpretations of the findings, and the conclusions that are drawn from this. Future research should strive to overcome these limitations so that it can fill in potential gaps left by this research. This section shall list these limitations and suggest future improvements or approach angles.

5.2.1 Sample and selection bias

This research was limited to the available interview subjects. The biggest gap is the lack of IT organization that has been certified in ISO 27001 but lacks ISO 9001 certification. The total number of interviewees per category is rather low. Two companies have no ISO certifications at the time of speaking. One company has only an ISO 9001 certification. Six of the interviewed companies have achieved both ISO 9001 and 27001 standards.

The low number of interviewees per category could result in outlying answers being over-represented in the research results. Interviews also had to be held online. This could have led to a decreased understanding of an interviewee's true feelings and meaning, as social clues are more difficult to understand when talking virtually. Other possible effects could have been a potential participants' attitude towards virtual meeting tools, health conditions of potential participants, and social and technological barriers (Nikolopoulou, 2023).

5.2.2 Social desirability bias

Social desirability bias occurs when respondents give answers to questions that they believe will make them look good to others, in this case, the interviewer, concealing their true opinions or experiences. This may cause interviewees to describe their situation more optimally in regards to the truthful situation (Grimm, 2010).

Two of the interviewees came from the personal circle of the researcher. A change in the responses given by this person could be a factor due to the existence of a personal relationship.

This social desirability could also not only be limited to their optics but also to preserve the social status of their organization. The level of openness of an interviewee will be related to their perceived relationship with the interviewer (researcher). There is no guarantee that this could have changed their responses, despite best efforts to express the measures that would be taken to ensure anonymity.

5.2.3 Cultural and personal bias

The cultural and personal biases of a researcher could have had an impact through each stage of this research. This includes prejudices in the sampling selection based on the researcher's preferences, the level at which they trust a respondent's words to have value, and how these results are interpreted (Yingst, 2020).

In this research, it is tried to remain as unbiased as possible. However, it can never truly be ruled out that some form of bias has occurred in this research process.

5.2.4 Methods/instruments/techniques used to collect data

Due to the fluent nature of an interview, it sometimes became difficult to ask all interviewees the same question in a similar manner. This is due to some interviewees answering multiple at once. Resulting in the loss of structure. In this research, the guarding of the process to make sure every question was asked with the same wording should have been more strict.

As previously mentioned in *chapter 5.2.1*, it is likely that a certain level of sampling bias has impacted the results of this research.

The open-coding method (Corbin and Strauss, 2008) was used for the first half of the interviews. This method was abandoned halfway through this research due to the large time investment with very little return on the discoverability of key topics. A slimmed-down version of this method was used to match the discussed topics to the sub-questions of this research. It should be noted that this results in the possibility that there is a difference in interpretation between the first and the latter set of interview results.

It proved difficult to combine the interview results due to the wide variety of experience levels with the ISO 9001 and/or 27001 standards. There were large differences in how the standards were perceived between those who did not have certifications, versus those who do. This does show to some degree how opinions might change between those two stages of certification.

However, coming to a unified answer on how IT companies can best implement the ISO 9001 standard in conjunction with the ISO 27001 standard, has led to the research needing to explain the differences between a given set of answers. The limited amount of respondents are now being divided even further between those with an ISO certification and those without certification. Resulting in a smaller effective sampling size.

5.3 Future work recommendations

This research has created a new pavement for future research. Although this research has its limitations, it does show the potential opportunities for a combined management system of both ISO 9001 and ISO 27001 standards for IT companies that want to get certified and/or internalize the practices of the standard.

The relationship between these standards in the field of IT could be explored in a more broad or more specified way. Future researchers might consider the following topics for their research.

- All of the interviewed organizations noted that they had issues with hiring and maintaining enough IT professionals. The reasoning for this could vary between organizations, but it is possibly a challenge throughout the IT sector. It could be interesting to see the effect that an ISO 9001 and/or 27001 implementation could have on an organization's ability to recruit more IT employees or to keep them employed for longer durations.
- There were very few companies available that used the ISO 90003 guideline for their ISO 9001 implementation. This ISO 90003 guideline is specifically made for the IT sector and could help implement the standard in the IT sector. Additional research into the effects of this particular set of guidelines is therefore advised.
- It would be advised to further specify the sampling group, as the effective sampling size per group (ISO certified / not certified) was rather limited in this research, with the primary focus preferably being the group that has both ISO 9001 and ISO 27001 certifications. By interviewing those who have experience with both standards you are more likely to gain insights into what is important for an integrated management system to be realized. This group could be specified even further with organizations that have implemented both standards simultaneously.
- This research was limited to the IT sector in The Netherlands. The answers given could be influenced by Dutch culture. Future research could look into other countries to investigate if cultural differences will result in differing research results.
- In *Chapter 4* it was discussed that the success criteria are more often noted as high-level

goals. It could be argued that the level of success is more difficult to quantify at this level of detail. There might be a bigger relationship between being able to measure how successful the implementation of a Quality and/or Information Security Management System is for an organization and the experienced benefits of such an implementation. A deeper understanding of this relationship could uncover more specific best practices for future combined implementations.

- In *Chapter 5.1.4*, a change was made in the coding method that was used for this research. There is a potential that this has resulted in a difference in interpretation of the interview results. Future research should choose a fitting method from the beginning and stick to it to prevent this potential issue.

Bibliography

(2015). Bai rmf resource center.

(2018). Iso/iec/ieee 90003:2018.

(2019). Iso/iec 27001:2013.

AbuSaad, B., Saeed, F., Alghathbar, K., and Khan, B. (2011). Implementation of iso 27001 in saudi arabia – obstacles, motivations, outcomes, and lessons learned.

Al-Rawahi, A. and Bashir, H. (2011). On the implementation of iso 9001:2000: A comparative investigation. *The TQM Journal*, 23:673–687.

Alcina A. de Sena Portugal Dias, I. H. S. (2016). Iso 9001 performance: A holistic and mixed-method analysis.

Almeida, D., Pradhan, N., and Jr, J. M. (2018). Assessment of iso 9001:2015 implementation factors based on ahp. *International Journal of Quality Reliability Management*, 35(7):1343–1359.

Alstom (2020). Definition of it-organisation.

Amsterdam, R. (2020). Ecli:nl:rbams:2018:10124.

ASQ (2020). What is iso 9001:2015 – quality management systems?

Banks, M. (2014). Analysing images. In *The Handbook of Qualitative Data Analysis*, pages 153–169. SAGE Publications, Inc., 1 Oliver's Yard, 55 City Road London EC1Y 1SP.

Bhuiyan, N. and Alam, N. (2005). A case study of a quality system implementation in a small manufacturing firm. *International Journal of Productivity and Performance Management*, 54:172–186.

Blair, E. (2015). A reflexive exploration of two qualitative data coding techniques. *Journal of Methods and Measurement in the Social Sciences*, 6(1):14.

Boehmer, W. (2009). Cost-benefit trade-off analysis of an isms based on iso 27001. pages 392–399.

Boiral, O. (2002). Iso 9000, côté jardin et côté cour. *Gestion*, 27(4):34.

Boiral, O. (2012). Iso 9000 and organizational effectiveness: A systematic review. *Quality Management Journal*, 19(3):16–37.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101.

Briscoe, J. A., Fawcett, S. E., and Todd, R. H. (2005). The implementation and impact of iso 9000 among small manufacturing enterprises. *Journal of Small Business Management*, 43(3):309–330.

Bryman, A. and Bell, E. (2011). *Business research methods*. Oxford University Press, Cambridge ; New York, NY, 3rd ed edition.

Cai, S. and Jun, M. (2018). A qualitative study of the internalization of iso 9000 standards: The linkages among firms' motivations, internalization processes, and performance. *International Journal of Production Economics*, 196:248–260.

Calder, A. (2006). Regulatory compliance and iso 27001.

Calvache, C., Garcia, F., Piattini, M., Pino, F., and Baldassarre, M. (2015). A 360–degree process improvement approach based on multiple models. *Revista Facultad de Ingeniería*, 1:95–104.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., and Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5):545–547.

Castka, P. and Corbett, C. J. (2015). Management systems standards: Diffusion, impact and governance of iso 9000, iso 14000, and other management standards. *Foundations and Trends® in Technology, Information and Operations Management*, 7(3–4):161–379.

Celik, M. (2009). Establishing an integrated process management system (ipms) in ship management companies. *Expert Systems with Applications*, 36(4):8152–8171.

Chang, S. E. and Ho, C. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, 106:345–361.

Chenail, R. (2011). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *The Qualitative Report*, 16(1):255–262. Retrieved from https://nsuworks.nova.edu/tqr/vol16/iss1/16.

Chountalas, P. T., Magoutas, A. I., and Zografaki, E. (2019). The heterogeneous implementation of ISO 9001 in service-oriented organizations. *The TQM Journal*, 32(1):56–77.

Chow-Chua, C., Goh, M., and Boon Wan, T. (2003). Does ISO 9000 certification improve business performance? *Int. J. Qual. Reliab. Manag.*, 20(8):936–953.

CISA (2022). Why should my organization implement the iso 27001 standard?

Corbin, J. and Strauss, A. (2008). Basics of qualitative research (3rd ed.): Techniques and procedures for developing grounded theory.

del Castillo-Peces, C., Mercado-Idoeta, C., Prado-Roman, M., and del Castillo-Feito, C. (2018). The influence of motivations and other factors on the results of implementing ISO 9001 standards. *European Research on Management and Business Economics*, 24(1):33–41.

Dellana, S. and Kros, J. (2018). Iso 9001 and supply chain quality in the united states. *International Journal of Productivity and Performance Management*, 67:00–00.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *J. Inf. Secur.*, 04(02):92–100.

Douglas, A., Coleman, S., and Oddy, R. (2003). The case for iso 9000. *The Tqm Magazine*, 15:316–324.

Dudin, M. N., Frolova, E. E., Gryzunova, N. V., and Shuvalova, E. B. (2014). The deming cycle (PDCA) concept as an efficient tool for continuous quality improvement in the agribusiness. *Asian Social Science*, 11(1).

Escanciano, C., Fernandez, E., and Vazquez, C. (2001). Iso 9000 certification and quality management in spain: results of a national survey. *The TQM Magazine*, 13(3):192–200.

Ganji, D., Kalloniatis, C., Mouratidis, H., and Malekshahi Gheytassi, S. (2019). Approaches to develop and implement iso/iec 27001 standard - information security management systems: A systematic literature review. 12:228–238.

Garengo, P. and Biazzo, S. (2013). From iso quality standards to an integrated management system: an implementation process in sme. *Total Quality Management & Business Excellence*, 24(3-4):310–335.

Garstenauer, A., Blackburn, T., and Olson, B. (2014). A knowledge management based approach to quality management for large manufacturing organizations. *Engineering Management Journal*, 26(4):47–58.

Gartner (2020). Iso 9001 definition.

Gillies, A. (2011). Improving the quality of information security management systems with iso27000. *The TQM Journal*, 23(4):367–376.

Gonzalez-Torre, P., Adenso-Diaz, B., and Gonzalez, B. (2001). Empirical evidence about managerial issues of iso certification. *The TQM Magazine*, 13(5):355–360.

Greensill, J. (2015). The new iso high-level structure - pwc auditor training.

Grimm, P. (2010). Social desirability bias.

Hayes, N. (1997). Theory-led thematic analysis: Social identification in small companies. In *Doing qualitative analysis in psychology*, pages 93–114, Hove, England. Psychology Press/Erlbaum.

Heras-Saizarbitoria, I. and Boiral, O. (2013). Ceremonial adoption of iso 9000 in smes: The role of internal contingencies. *SSRN Electronic Journal*.

Heras-Saizarbitoria, I., Cilleruelo, E., and Allur, E. (2014). Iso 9001 and the quality of working life: An empirical study in a peripheral service industry to the standard's home market. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 24(4):403–414.

Hoy, Z. and Foley, A. (2014). A structured approach to integrating audits to create organisational efficiencies: Iso 9001 and iso 27001 audits. *Total Quality Management Business Excellence*, 26(5–6):690–702.

Hsu, C., Wang, T., and Lu, A. (2016). The impact of iso 27001 certification on firm performance. *2016 49th Hawaii International Conference on System Sciences (HICSS)*.

Ijaz, Q., Asghar, H., and Ahsan, A. (2016). Exploratory study to investigate the correlation and contrast between iso 9001 and cmmi framework: Context of software quality management. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, pages 388–391.

ISO (2015). *Quality management systems : requirements*. ISO/IEC, Geneva.

ISO (2019). Iso 9001:2015 - how to use it. https://www.iso.org/files/live/sites/isoorg/files/store/en/PU

ISO (2020a). About us - international organization for standardization.

ISO (2020b). Iso/iec 27001:2013 [iso/iec 27001:2013].

ISO (2020c). Management system standards.

ISO (2021). The iso survey of management system standard certifications - 2021 - explanatory note. https://www.iso.org/the-iso-survey.html.

Janghorban, R., Roudsari, R. L., and Taghipour, A. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-being*, 9(1):24152.

Joffe, H. (2011). *Thematic Analysis*, pages 209 – 223.

Jose Tari, J., Heras-Saizarbitoria, I., and Pereira, J. (2013). Internalization of quality management in service organizations. *Managing Service Quality: An International Journal*, 23(6):456–473.

Kartha, C. (2004). A comparison of iso 9000:2000 quality system standards, qs9000, iso/ts 16949 and baldrige criteria. *The TQM Magazine*, 16(5):331–340.

King, N. (1999). *Doing Template Analysis*, page 426–450. SAGE Publications, Inc.

Klimovich, N. S. (2018). Definition of quality integrated assessment through the spectacle of marketing. http://edoc.bseu.by:8080/handle/edoc/77379.

Kraus, J. L. and Grosskopf, J. (2008). Auditing integrated management systems: Considerations and practice tips. *Environmental Quality Management*, 18(2):7–16.

Kymal, C., Gruska, G., and Dan Reid, R. (2015). *Integrated management systems: QMS, EMS, OHSMS, FSMS including aerospace, service, semiconductor/electronics, automotive, and food*. Quality Press.

Lin, C. and Wu, C. (2007). Case study of knowledge creation contributed by iso 9001:2000. *International Journal of Technology Management*, 37(1/2):193.

Mcadam, R. and Fulton, F. (2002). The impact of the iso 9000:2000 quality standards in small software firms. *Managing Service Quality*, 12:336–345.

McNamara, C. (2020). General guidelines for conducting interviews.

Mokhtar, M. Z. and Muda, M. S. (2012). Comparative study on performance measures and attributes between ISO and non-ISO certification companies. *Int. J. Bus. Manag.*, 7(3).

Mouratidis, H. and Giorgini, P., editors (2006). *Integrating security and software engineering*. IGI Publishing, Hershey, PA.

Muh. Sidratul, M. A., Farani, W., Wahyudin, B. K., Insan Rizky, M., Hidayanto, A. N., Ayuning Budi, N. F., Pinem, A. A., and Baskoro Yudhoatmojo, S. (2019). Analyzing the relevance of inhibiting factors in implementing iso 27001 using the dematel method (case study: Electronic procurement service center (lpse) of the ministry of finance, republic of indonesia). In *2019 5th International Conference on Computing Engineering and Design (ICCED)*, pages 1–6.

Nair, C., Adams, P., and Mertova, P. (2008). Student engagement: The key to improving survey response rates. *Quality in Higher Education*, 14(3):225–232.

Natarajan, D. (2017). *ISO 9001 Quality Management Systems*. Springer International Publishing.

Naveh, E. and Marcus, A. (2005). Achieving competitive advantage through implementing a replicable management standard: Installing and using iso 9000. *Journal of Operations Management*, 24(1):1–26.

Ndegeya, R. and Uwase, R. (2022). *Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs*. PhD thesis, Lulea ˚ University of Technology.

NEN (2020). High level structure (hls): basis van de nieuwe iso-normen.

Netherlands, T. (2020). Nen en iso 9001 norm.

Nikolopoulou, K. (2023). What is social desirability bias? — definition examples.

Noble, H. and Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, 18(2):34–35.

Poksinska, B., Dahlgaard, J. J., and Eklund, J. A. E. (2006). From compliance to value-added auditing – experiences from swedish iso 9001:2000 certified organisations. *Total Quality Management & Business Excellence*, 17(7):879–892.

Ponelis, S. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies*, 10:535–550.

Porter, S. R. and Whitcomb, M. E. (2005). Non-response in student surveys: The role of demographics, engagement and personality. *Research in Higher Education*, 46(2):127–152.

Prabhu, V., Appleby, A., Yarrow, D., and Mitchell, E. (2000). The impact of iso 9000 and tqm on best practice/performance. *The TQM Magazine*, 12(2):84–92.

Recklies, O. (2001). Managing change – definition und phases in change processes. Recklies Management Project GmbH, Bernhard-Adelung-Straße 20, 65428 Rüsselsheim am Main, Duitsland.

Renvall, A. (2018). *Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs*. PhD thesis.

Roshaidai, S. and Arifin, M. (2018). Ethical Considerations in Qualitative Study. *International Journal of Care Scholars*, 1(2):30–33.

Rousse, M. (2020). Iso 27001 definition.

Ruhwanya, Z. and Ophoff, J. (2020). Critical analysis of information security culture definitions. In *Human Aspects of Information Security and Assurance*, IFIP advances in information and communication technology, pages 353–365. Springer International Publishing, Cham.

Sampaio, P., Saraiva, P., and Rodrigues, A. (2009). Iso 9001 certification research: Questions, answers and approaches. *International Journal of Quality Reliability Management*, 26.

Santos, L. and Escanciano, C. (2002). Benefits of the iso 9000:1994 system. *International Journal of Quality Reliability Management*, 19(3):321–344.

Simon, A., Bernardo, M., Karapetrovic, S., and Casadesus, M. (2013). Implementing integrated management systems in chemical firms. *Total Quality Management Business Excellence*, 24(3–4):294–309.

Singh, P. J., Feng, M., and Smith, A. (2006). Iso 9000 series of standards: comparison of manufacturing and service organisations. *International Journal of Quality Reliability Management*, 23(2):122–142.

Sousa-Poza, Altinkilinc, M., Searcy, C., asousapo, and Malti (2009). Implementing a functional iso 9001 quality management system in small and medium-sized enterprises.

Stålhane, T. and Hanssen, G. (2008). The application of iso 9001 to agile software development. pages 371–385.

Sun, H. (2000). Total quality management, iso 9000 certification and performance improvement. *International Journal of Quality Reliability Management*, 17(2):168–179.

Terziovski, M., Power, D., and Sohal, A. S. (2003). The longitudinal effects of the iso 9000 certification process on business performance. *European Journal of Operational Research*, 146(3):580–595.

Thomas, G. (2017). *How to Do Your Research Project: A Guide for Students*. Sage Publications Ltd, third edition.

Topa, I. and Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information and Computer Security*, 27.

Tu, Z. and Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *20th Americas Conference on Information Systems, AMCIS 2014*.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. *Comput. Secur.*, 23(5):371–376.

Walker, L. (2020). Why is software quality important to security?

Wang, C.-H. and Tsai, D.-R. (2009). Integrated installing iso 9000 and iso 27000 management systems on an organization. pages 265 – 267.

Wiele, T. V. D. and Brown, A. (1997). Iso 9000 series experiences in small and medium-sized enterprises. *Total Quality Management*, 8(2-3):300–304.

Woollven, C. (2018). Iso 27001 global report 2018: top 3 key takeaways - it governance uk blog.

Yin, R. (2018). *Case study research and applications : design and methods*. SAGE Publications, Inc, Thousand Oaks, California.

Yingst, T. E. (2020). Cultural bias.

Zeng, S. X., Shi, J. J., and Lou, G. X. (2007). A synergetic model for implementing an integrated management system: an empirical study in china. *J. Clean. Prod.*, 15(18):1760–1767.

Zeng, S. X., Xie, X. M., Tam, C. M., and Shen, L. Y. (2011). An empirical examination of benefits from implementing integrated management systems (ims). *Total Quality Management Business Excellence*, 22(2):173–186.

Zutshi, A. and Sohal, A. S. (2005). Integrated management system. *Journal of Manufacturing Technology Management*, 16(2):211–232.

Appendix A

Survey results

This Appendix should not be published in any form.

It was added at the request of the supervisors.

Contents: Survey results.