Stakeholders view on the output legitimacy of ISO/IEC 27001:

A qualitative interview study

Authors: Yasmin Kamil (960504), Sofia Lund (960308)

Spring semester 2022
Informatics, Thesis, Second Cycle, Advanced level, 30 Credits
Subject: Information Security Management
Örebro University School of Business
Supervisor: Fredrik Karlsson
Examiner: Sirajul Islam

Abstract

Purpose: To ensure information security, organizations need to establish an information security management system (ISMS) to control and manage information securely. The ISO/IEC 27001 standard is used by organizations to process an ISMS. The standard specifies security measures and requirements that can be implemented to provide organizations the ability to manage their information assets. The ability of the standard's problem-solving capacity can then come into question. Therefore, the purpose of this thesis is to explore the output legitimacy of the ISO/IEC 27001 from different stakeholders' views.

Research method: An interview study with different stakeholders working with information security management in different private organizations in Sweden was conducted. Using a deductive analysis, eight information security objectives were identified and depending on this, the output legitimacy of the ISO/IEC 27001 was explored.

Results: The findings present eight information security objectives. The level of output legitimacy of the standard varies from high-medium-low depending on which objective. The standard has a high level of output legitimacy when working with the objective "To maintain an ISMS". However, the output legitimacy is considered lower while working with the objective "To ensure technical security".

Conclusion: The aim of the ISO/IEC 27001 is to implement, establish, operate and monitor an ISMS, the findings have confirmed the standard has a high level of output legitimacy to maintain those aspects of information security. However, the standard does not have the capacity and the level of output legitimacy is low to be able to deal with technical security. To reach a high level of output legitimacy of ISO/IEC 27001, stakeholders need to understand that the standard is not intended to be a technical standard. Furthermore, stakeholders need to have the right knowledge and skills in information security to be able to navigate the work effectively, with the support of the standard.

Keywords: *ISO/IEC 27001, output legitimacy, stakeholder theory, instrumental stakeholder theory, information security, information security standard, information security management system, ISMS*

Acknowledgements

A lot of time and energy has been dedicated to being able to deliver the best possible results and quality for this master thesis. This would have not been possible to complete without the help and support from several people. Therefore, in this paragraph, we would like to extend a sincere gratitude to all parties involved.

First and foremost, we would like to express our gratitude to our master thesis supervisor Fredrik Karlsson, for taking the time, energy, effort and patience to guide us throughout this process with his valuable knowledge and experience. His input and the significant discussions have encouraged us to be able to complete this thesis in the best possible way. We would like to thank our examiner Sirajul Islam who has given us the constructive criticism to further improve our work. We would also like to express our gratitude to the professors at Örebro University in the Master's program in Information Security Management, who have provided us good skills in the field of information security and given us a good experience during the education despite the pandemic.

We would also like to thank Torbjörn Söderberg, Mattias Sjödin and Carina Åstrand at Kontract AB who made it possible for us to perform this master thesis. Without their support and interest in investigating this area of information security it would not have been possible to carry out this thesis. We would also like to extend a gratitude to all respondents who took the time to participate in this study and share their valuable opinions and experiences. Without their willingness to participate in this study, the results of this study would not have been generated.

Finally, we would like to extend a heartfelt gratitude to our families and friends who have supported us throughout the process of the master's thesis but also our education at the masters program. Without their emotional support, it would have been difficult to complete this in the best possible way.

27th of June 2022, Örebro
Yasmin Kamil & Sofia Lund

Table of Contents

1 Introduction

1.1 Background

The rapid technology and computer-based development of information systems have resulted in more opportunities in how to store, process, and transmit digital information in several business environments. Nevertheless, selecting the appropriate security measures has become a more complex matter for organizations (Dhillon & Backhouse, 2001). Despite the benefits technology has contributed, the number of attacks on information systems has increased. This is because organizations today provide and process information that is of a higher degree of sensitivity and value, which results in increased security risks (Nyman & Große, 2019). The results of new technologies have increased the number of entry points in computer networks, which has led to increased vulnerabilities (Culot et al., 2021). Evans et al. (2019) explain that the most common reasons behind security incidents are unintentional human error, technical errors, procedural errors, and weaknesses in physical controls that result in malicious actions. For instance, Verizon (2021) reports that 85% of data breaches that occur within organizations are due to human factors, where the employees unconsciously disclose confidential information to unauthorized actors. Therefore, organizations are in need to ensure the protection of their information infrastructure from security breaches that can be caused by either internal or external factors (Topa & Karyda, 2019). This has evidently increased the need to consider information security as an important aspect in an information society (MSB, 2018).

The purpose of information security is to ensure business continuity and minimize the effects of security incidents (Von Solms & Van Niekerk, 2013). Whitman and Mattord (2009) emphasize with information security, organizations can ensure the protection of their business-critical information assets as well as their software and hardware used for information management. Dhillon (2018) further explains that information security management (ISM), is about maintaining the integrity of the technical, formal, and informal systems of an organization. However, if there is discordance between the systems, security issues will arise. The reason for this is if an information security issue occurs within an organization, it will result in several negative consequences such as a loss of customer trust; productivity; financial and data losses; legal consequences; exposure of personal information; inappropriate computer use (Huang et al., 2010; Nyman & Große, 2019). Organizations must therefore implement security measures that can help to manage the confidentiality, integrity, and availability (CIA) of information assets (Dhillon, 2018).

To ensure information security within organizations, it is recommended to establish an information security management system (ISMS), which can support organizations control and manage information securely (Nancylia et al., 2014). The strategies and policies contained in an ISMS result in the ability to preserve and ensure the CIA of business-critical information assets (Fonseca-Herrera et al., 2021). An ISMS also enables organizations to manage their information assets more effectively (Susanto et al., 2011). If organizations do not have a suitable ISMS for their operations and information systems, it will affect the ability to secure guarantees for continuity (Santos-Olmo et al., 2016). By complying with standards such as the ISO/IEC 27000 series, organizations can ensure that they have implemented a suitable ISMS, as the standard series provides requirements that can be used to support the security of an organization’s information assets (Hamdi et al., 2019).

Organizations must take advantage of information security standards to implement appropriate security measures (Tjurare & Shava, 2017). However, it can be challenging to choose and implement a suitable ISMS standard (Susanto & Almunawar, 2018). Conversely, organizations need to indicate a commitment to secure business practices by adopting authoritative guidelines (Siponen & Willson, 2009). Considering that business partners can require that the organization can prove that they are protecting its information assets. Therefore, there needs to be evidence available to demonstrate how the assets are protected appropriately (Von Solms, 1999).

Beyond this, organizations primarily adopt information security standards for market assurance and governance (Shojaie et al., 2014). Moreover, information security standards are seen as necessary and influential tools today, in part due to the need for organizations to protect their valuable assets against cybercrime, hacktivists, and foreign governments (Andersson et al., 2020). In other words, organizations' information assets are essential and must be adequately protected. Especially, in increasingly interconnected business environments to minimize the effects of security incidents but also ensure continuity of organizations (Proença & Borbina, 2018).

The ISO/IEC 27001 standard is used by organizations to implement an ISMS. The standard specifies security requirements and measures that can be implemented within an ISMS to give organizations the ability to manage their information assets (Al-Dhahri et al., 2017). The security measure provides support for organizations to implement, establish, operate and improve the organization’s ISMS and the management system can be tailored to the needs of an organization (Orozova et al., 2019). The ISO/IEC 27001 standard presents an overview of the security measures. Meanwhile, ISO/IEC 27002 presents them in the form of extended guidelines, by only considering the technical and formal security measures. Organizations that are ISO/IEC 27001 certified can demonstrate that they have achieved an acceptable level of security. This in turn promotes customer confidence (Disterer, 2013). Furthermore, the standard does not only guide organizations on how the implementation of a management system should be conducted. It also aims to generate legitimacy and credibility for organizations (Douvreleur, 2019).

There are three domains of legitimacy distinguished as input, throughput, and output legitimacy (Scharpf, 1999; Schmidt, 2013). To achieve an output legitimacy while using ISO/IEC 27001, the standard must have the ability to solve problems collectively and successfully (Werle & Iversen, 2006). However, the output legitimacy of the standard can be questioned, whether it is effective in terms of information security (Uwizeyemungu & Poba-Nzaou, 2015). Therefore, security managers need to design and adapt the security work according to the stakeholders' values for the output legitimacy to not be questioned (Topa & Karyda, 2019). Freeman (1984) explains that each stakeholder has a “stake” in the organization, which is why their views are important to consider. At the same time, it is also crucial to consider how organizations choose to integrate their information security mechanisms into the process of working with information security standards (AlKalbani et al., 2016). Especially to gain legitimacy, as it is considered an important component for organizations since it enables growth, resource acquisition, strategic transformation, and sustainability (Niemimaa, 2016).

By developing and implementing specific strategies, organizations create the opportunity to gain legitimacy from all stakeholders (Cavusoglu et al., 2015). Such legitimacy depends primarily on how organizations integrate routines and various forms of information security

solutions by complying with information security standards. The provisions for implementing regulations force organizations to incorporate the legal requirements for information security to fulfill those obligations. This in turn results in organizations needing to implement significant changes such as standardizations of operational processes and practices, to indicate that there is a consistency between laws and regulations to gain stakeholder legitimacy concerning information security (AlKalbani et al., 2017). By involving stakeholders in the following process, it is possible to strengthen the perception of how legitimate standards are, which results in input legitimacy. Meanwhile, the effectiveness of the standards is strengthened with the support of the regulatory effects which results in an output legitimacy (Brunsson et al., 2012).

1.2 Problem statement

Topa and Karyda (2019) argue that information security standards are critical for dealing with information security. For example, the ISO/IEC 27001 lacks guidance on how the processes and implementation should be applied in practice (Ojalainen, 2020). Because the countermeasures specified in the standard are considered as too formal and comprehensive. The ISO/IEC 27001 standard explains *what* needs to be done, but it does not present *how* organizations should proceed to achieve the requirements. As a result, greater responsibility is handed over to the stakeholders' expertise. Additionally, the support from ISO/IEC 27001 to adapt the organization's ISMS to local legislation has also been discussed. The standard points out that the implementing organization should take responsibility for identifying the local laws and regulations. However, the standard does not provide any clear instructions on *how* organizations should conduct this, which can result in them facing complex challenges in complying with local laws (Culot et al., 2021). This in turn raises the question of the standard's ability to solve collective problems and meet the expectations of standard users, which also generates an issue about the output legitimacy of the standard. Given that output legitimacy is a result of the ability to coordinate and the effectiveness of a standard, where subordinates must believe in its legitimacy. Since it can lead to a positive spread, where both the standard and organization will produce an output legitimacy (Botzem & Dobush, 2012).

Considering that output legitimacy is about the problem-solving capacity or the effectiveness of policies or standards (Bäckstrand, 2006), it is necessary that the standard solves collective problems or meets stakeholders' expectations (Mayntz, 2010). Therefore, an organization's fundamental documents or policies need to function effectively to be in line with stakeholders' values (Schmidt, 2013). In other words, it is about to what extent the ISO/IEC 27001 have the capacity to solve issues in the most effective way to meet stakeholders' expectations (Mena & Palazzo, 2012). Therefore, it is important to perform a stakeholder analysis to gather and analyze information about stakeholders and develop an understanding of as well as identify aspects that can influence the decision-making process (Brugha & Varvasovszky, 2000). Given that new ways of governance are created, new approaches are also needed to legitimize security operations and measures (Schmidt, 2009). To address this, it is necessary to bring together relevant stakeholders as it can cause better and increased output legitimacy (Christou, 2018). In line with this, Culot et al. (2021) suggest conducting more theory-based research to investigate the effects and application of the ISO/IEC 27001. But also study the challenges and knowledge gaps that exist based on theoretical lenses for future studies. Using stakeholder theory it is possible to focus on the integration of business and social issues and how non-business pressures can affect stakeholders' motives in the implementation of standards as well as influence an organization's reputational performance and operations (Castka & Prajogo, 2013). Considering that the main idea of the stakeholder

theory is about building relationships with and creating value for stakeholders, it is important that organizations pay attention to stakeholder interest. Which in turn can create an increased value for the stakeholders that can result in benefit to the organization's performance (Gao, 2021). In addition to this, by considering the stakeholder theory, it is possible to draw attention to the stakeholders' interests when it comes to organization's information security objectives (Yaokumah & Brown, 2014). Depending on this, a foundation and justification are laid for why the following study is conducted, where the purpose of this thesis is to explore the output legitimacy of the ISO/IEC 27001 from different stakeholder views.

1.3 Research question

To address the purpose of the thesis, an interview study will be conducted with stakeholders in different private organizations in Sweden. The organizations are either ISO/IEC 27001 certified or comply with the standard to maintain their information security work. This is to have the ability to develop knowledge about the output legitimacy of the standard while stakeholders address issues concerning information security.

For this purpose, the following research question will be answered:

- What are different stakeholders in information security management view on the output legitimacy of ISO/IEC 27001 to achieve their information security objectives?

1.4 Scope

This study is of interest to stakeholders working in private organizations who are interested in exploring the output legitimacy of the ISO/IEC 27001 standard both at a national and international level. The results can support stakeholders to gain fundamental insights into how effective the standard is and its capacity to deal with information security and issues that are common among several stakeholders. Furthermore, the intended results can offer the academy a deeper understanding of the output legitimacy of the standard from a stakeholder view.

2 Related research

This section presents previous studies that concern the research topic.

2.1 Information Security Management System

Information security management (ISM) depends on technology, processes, and people (Ashenden, 2008; Nancylia et al., 2014). Meanwhile, Eloff and Eloff (2003, p.130) define an Information Security Management System (ISMS) as "*a management system used for establishing and maintaining a secure information environment*". In other words, the purpose of an ISMS is to ensure the confidentiality, integrity, and availability (CIA) of information assets (Pavlov & Karakaneva, 2011), and help organizations to control and manage information securely (Fonseca-Herrera et al., 2021). Susanto and Almunawar (2018) emphasize that information security is a business enabler and an integral part of the business. Therefore, more organizations need to pay attention to information protection by implementing an ISMS. A well-defined ISMS involves several issues that need to be addressed during the planning, management, and monitoring of information security (Eloff & Eloff, 2003). This in turn will help organizations with a continuous improvement process and be able to respond to threats and take corrective and preventive actions to control an incident (Fonseca-Herrera et al., 2021).

A well-functioning ISMS is about having well-established monitors, reviews, operations, and processes as well as continuously implementing and improving the organization's overall operations (Nancylia et al., 2014). There is, therefore, a need to identify the information security needs; implementation and improvement strategies; measurements of results of an organization. Furthermore, policies, procedures, guidelines, activities, and associated resources need to be in place. When an ISMS is successfully implemented it is governed by analyzing requirements to protect information assets, where suitable security measures are applied to ensure their protection (Singh et al., 2014). Eloff and Eloff (2003) also mention that ISM must take a holistic approach. Conversely, it is necessary to emphasize that although the organization has registered or certified an ISMS aligned with ISO/IEC 27001, it does not tell about its performance and quality for its implementation (Boehmer, 2008).

Singh et al. (2014) have further discussed ISM as a multidimensional approach, which impacts the internal and external factors on how to manage information security requirements and needs. The internal factors include for example business issues, strategic vision, and IT infrastructure. Meanwhile, external factors are about legal and regulation compliance; the security risk and threat environment; the current IT environment; and flexible market situations.

2.2 Information Security Management System Standards

Standards can be viewed as best practices with the wisdom of experts in the area (ISO, n.d.). They represent a list of requirements that a product or a system needs to achieve by providing solutions to recurring problems (Tofan, 2011). There are several information security standards that organizations are recommended to apply to ensure the protection of their information assets (Bakker, 2018). For instance, ISMS standards can help organizations systematically document, establish, and continuously manage procedures to ensure the security and reliability of an organization's information assets. Furthermore, ISMS standards can form the basis for securing the CIA of business-critical assets, which is the goal of

information security (Rezakhani et al., 2011). The ISO/IEC 27001, BS 7799, and NIST SP800 are examples of ISMS standards (Tofan, 2011; Susanto & Almunawar, 2018).

2.2.1 ISO/IEC 27001 and 27002

The ISO/IEC 27001 has been adopted widely internationally and recognized by stakeholders. It has the prestigious name of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (Tofan, 2011). The first version of ISO/IEC 27001 was designed and published in 2005 which was an evolution of BS 7799 (Shojaie et al., 2014). The most recent international version of the standard was released in 2013. One of the major changes is that the structure of the standard is aligned with other standards such as ISO/IEC 9001 and 14001. Another change is that the requirement for documented procedures and records was replaced with documented information as well as new requirements were added and certain requirements were eliminated (Ţigănoaia, 2015).

The standard specifies requirements for information security within the organizational framework, to establish, implement, maintain and improve a management system. The requirements are generic and can be applied no matter the size, type, or nature of the organization. However, it does not mandate any specific action, only guidelines (Swedish Standards Institute [SIS], 2017). The ISO/IEC 27000 series is based on risk management and considers the 114 security measures that can be found in the Appendix of ISO/IEC 27001. How these security measures can be implemented are further described in ISO/IEC 27002 (Shojaie et al., 2014; Swedish Standards Institute [SIS], 2020).

The ISO/IEC 27001 standard presents requirements for an ISMS to achieve certification. It specifies seven key elements to achieve the certification, which include establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the system. The standard is intended to be used in line with the ISO/IEC 27002 standard. The ISO/IEC 27001 standard aims to establish a structured set of information security measures, whose use will support achieving conformity with ISO/IEC 27001. Organizations can freely implement measures that are not specifically listed as long as they are effective and conform to ISO/IEC 27001 (Tofan, 2011). It contains best practices and security measures regarding security policy; governance of information security; asset management; human resources security; physical and environmental security; communication and operations management; development and maintenance; information security incident management; business continuity management; compliance (Tofan, 2011; SIS, 2017).

The current version of SS-ISO/IEC 27001:2017 applies as a standard in Sweden (SIS, 2017). However, there were no changes made to the version from 2013 and it was intended to seek approval by CEN/CENELEC for the EN designation (Heron, 2018). The changes in the standards are minimal and no new requirements were introduced. The 2017 version does include two Corrigendum/Amendments in Clause 6.1.3 and Annex A clause 8.1 (Piper, 2019). The changes include that information itself is seen as an asset and can be part of the inventory. The Statement of Applicability (SoA) also highlights four elements and is presented in bullet form (Heron, 2018). The SoA document presents the number of security measures; the name of the controls, and the result of the realization of the controls (Tanovic et al., 2014).

2.3 Output legitimacy

There are three domains of legitimacy that have been distinguished by Scharpf (1999) and Schmidt (2013) - input, throughput, and output legitimacy. Input legitimacy is based on the rhetoric of participation and consensus where choices are only legitimate in terms of how it reflects the will of the people (Scharpf, 1999). It is about stakeholder participation, where all participants have similar opportunities in the decision-making process for a formation of a standard (Kica & Bowman 2012). Throughput legitimacy is about the decision-making process and its quality. It focuses on processes and is analyzed in terms of efficacy, accountability, transparency, inclusiveness, and openness. (Scharpf, 1999). It requires mechanisms for processes and transparency to ensure that stakeholders are responsive (Kica & Bowman, 2012). Output legitimacy, on the other hand, focuses on the quality of problem-solving of laws or standards (Scharpf, 1999). This form of legitimacy focuses on the results of the decision-making process, and whether or not they can solve current stakeholder problems effectively (Kica & Bowman, 2012).

Output legitimacy has previously been operationalized through the concept of effectiveness. Effectiveness can be seen as institutional performance in terms of results. Depending on this, output legitimacy can be associated with the perception of the results among a wider range of stakeholders (De La Plaza Esteban et al., 2014). In the context of the implementation of standards, there are a variety of stakeholders to be involved in the process from senior management to employees (SIS, 2017). Botzem and Dobusch (2012) further explain that output legitimacy is primarily about the standard's effectiveness and problem-solving capacity. Therefore, it can be a predominant part of its dissemination. Considering that the dissemination of rules is a prerequisite for a lasting standardization regime since a high application of a standard can result in output legitimacy. Based on this, output legitimacy refers, in this context, to the relevance of the content in documents and can also be operationalized in changes of behavior of actors related to ISO/IEC 27001.

As mentioned, output legitimacy is generated from problem-solving capacities or expectations of standard adopters are met (Botzem & Dobusch, 2012). To achieve output legitimacy, it must be possible to solve problems collectively and successfully. The purpose from this perspective is "good governance" or in the case of standardization referring to "good" standards. However, organizations and stakeholders should not make differences between what standards an organization has adopted as long as the standard has been used beneficially (Werle & Iversen, 2006). According to Richardson and Eberlein (2011) a "good" standard, in a technical standard-setting, can be recognized on the assumption that experts in the area can recognize it based on its ability to resolve technical problems or make future developments easier. In this context, the output legitimacy is concentrated on the standard itself compared to the input that focuses on the standardization process. To achieve output legitimacy in standardization, it is necessary that the standard solves collective problems or meets stakeholders' expectations (Mayntz, 2010). Therefore, the higher the degree of acceptance of a standard, the higher its coordination ability will be, which is the core of output legitimacy. However, it is important to point out that what is gained in output legitimacy does not always result in a standard's overall and long-term stability, especially if it is a result of or reduces input legitimacy (Botzem & Dobush, 2012).

There have been few studies regarding the legitimacy concerning information security standards (Backhouse et al., 2006; Kallberg, 2012; Silva et al., 2016; Aldya et al., 2019; Lopes et al., 2019; Diamantopoulu et al., 2020; Annarelli et al., 2021; Andersson et al., 2022). Backhouse et al. (2006) and Silva et al. (2016) mention in their studies that during

standard development it is essential to include industry representatives to achieve legitimacy and credibility. Because when the participants experience that the standard as their own, they will later be able to defend it accordingly. A recent study by Andersson et al. (2022) also discovered the structures that affect the input and throughput legitimacy of information security standards. Meanwhile, Kallberg's (2012) study indicates that when establishing and maintaining a standard, it is important to create alliances and trust. These groups have an advantage over each other, with examples of NATO, the EU, the African Union, and the Union of South American nations. On the other hand, output legitimacy is closely related to its problem-solving capacity as well as effectiveness, which has been addressed to a limited extent.

Annarelli et al. (2021) explored the effectiveness and adoption of NIST managerial practices in Italy. They found that there was a lack of disciplinary measures in case of misconduct, the importance of investing in building awareness of people regarding cyberthreats, and the necessity for organizations to develop their customized policies. Previous research has also indicated that organizations that already have implemented ISO/IEC 27001 or are in the process of it have a better foundation for complying with GDPR (Lopes et al., 2019; Diamantopoulou et al., 2020).

Conversely, recent literature has highlighted the little effectiveness the standard has on emerging technologies. Cloud computing, the Internet of Things, and platform-based businesses make it more difficult to define the scope and boundaries of an ISMS (Culot et al., 2019). On the other hand, there has been research on how to measure the effectiveness of the implementation of information security measures in the standard with the support of ISO/IEC 27004 (Aldya et al., 2019).

3 Theoretical framework

3.1 Stakeholder theory

The stakeholder theory was first fully articulated by Freeman (1984) by drawing from various literature such as corporate planning, systems theory, and corporate social responsibility. Nowadays, the theory is mainly used to study the similarities and differences of businesses from a narrow and broad perspective (Freeman et al., 2020). Moreover, the theory is primarily used to examine the business planning process; ethical issues; strategic management; the organizational environment; project management, etc. Furthermore, the interest to involve the stakeholders as a means has also increased to be able to e.g., develop more successful information systems (Mishra & Dwivedi, 2012). The theory considers the stakeholder as a means and objective in a mutual and interconnected system, where each stakeholder contributes with benefit to the system for it to continue to develop (Freeman et al., 2020).

3.1.1 The three views of the stakeholder theory

The theory has emerged into three different views and properties - descriptive, normative, and instrumental (Mishra & Dwivedi, 2012). The descriptive view describes and explains the characteristics of an organization. The view focuses on describing the character of the organization; the mindset that the managers have to drive the management work; how the organization is managed (Donaldson & Preston, 1995). It describes how organizations can cooperate and have competing interests with an inherent value (Mishra & Dwivedi, 2012). The ISO/IEC 27001 standard describes the tasks and also the information security governance of organizations in a comprehensive way (Mataracioglu & Ozkan, 2011). To be able to establish the standard, there needs to be a description of the organizational environment, stakeholders, and security objectives (Beckers, 2015). In this case, to achieve an output legitimacy of the ISO/IEC 27001 standard, the descriptive view helps organizations describe which stakeholders they are responsible for; how they can maintain relationships with their stakeholders; how the organization can meet the needs and desires of stakeholders when it comes to information security (Tanadi et al., 2021).

The normative view is about interpreting the organization's function and identifying the moral or philosophical guidelines for operation and management (Donaldson & Preston, 1995). Stakeholders are seen as individuals or groups with legitimate interests in material and procedural aspects of organizational activities (Mishra & Dwivedi, 2012). In other words, the stakeholders are seen as an objective in themselves, and it is based on the principle of justice. This means that all human beings will be affected by the decisions that are made. This is because all people have a legitimate and equal interest (Bailur, 2006). The ISO/IEC 27001 standard can be tailored to any organization and promotes every individual's involvement (Beckers et al. 2012a; SIS, 2017). For an output legitimacy of the ISO/IEC 27007, it is possible to use the normative view to understand stakeholder relationships in relation to the standard which is based on morals and normative commitments as well as to understand the legitimacy concerning morals and ethics of stakeholders.

The instrumental view, which is the view this study aims to focus on, is used to identify the relationships or lack of relationships between the fulfillment of the traditional business objectives and stakeholder management (Donaldson & Preston, 1995). The view establishes a framework for examining the relationships between stakeholder management and the achievement of the organization's performance objectives (Mishra & Dwivedi, 2012). This is

done by organizations seeing their key interests as their competitive advantage. Because if the organization does not have deeper interactions and transactions with critical groups, it will result in failures (Bailur, 2006). The ISO/IEC 27001 standard reflects an international consensus regarding the best practices to ensure a management system that can satisfy the organization's as well as the stakeholder's requirements for product and service quality in connection with regulatory requirements (Dinu, 2017). Many organizations nowadays need a set of effective and specific indicators that can facilitate the implementation and use of security mechanisms. Therefore, the ISO/IEC 27001 standard is considered an appropriate way to ensure this (Wiedenhöft et al., 2014). To maximize the effectiveness from a stakeholder view, the instrumental view supports organizations to address stakeholders' needs and interests (Welcomer, 2002). The goal of this view is to identify relationships or lack of relationships in the presence of stakeholder management and the achievement of the performance objectives (Cesar, 2019). In this case, achieve effectiveness and capacity to solve problems when using the ISO/IEC 27001 standard. Thus, to meet the needs and increase the output legitimacy of the ISO/IEC 27001, the organization must establish, maintain, and continuously improve its business processes that are needed and its interactions with the support of key stakeholders (Algheriani et al., 2019). In other words, to understand the effectiveness of the ISO/IEC 27001 standard, the instrumental view can be used to understand how to meet stakeholders' objectives in relation to an ISMS and evaluate this.

3.2 Stakeholder theory in information security

The stakeholder theory has been used in information security research to primarily examine stakeholder roles. However, most studies focus on examining the relationship between a specific stakeholder and an information security team (Seltsikas & Soyref, 2013). For instance, research conducted by Cavusoglu et al. (2005) and Galbreth and Shor (2010) examined malicious stakeholders. Meanwhile, Hu et al. (2007) have, from a broader perspective, examined the relationships between external and internal stakeholders. When it comes to the use of the theory in relation to research about information security standards, Fenz and Neubauer (2018) have studied how organizations can in different ways achieve compliance with the support of information security standards. However, further research is required regarding the effectiveness or output legitimacy of the ISO/IEC 27001 standard with the support of key stakeholders. This is because such an investigation can provide a deeper insight into the output legitimacy of the ISO/IEC 27001 standard from a stakeholder view.

3.3 Definition and classification of stakeholder

One of the most used definitions of an organizational stakeholder is "*any group or individual who can affect or is affected by the achievement of an organization's objectives*" (Mansell, 2013, p. 30). However, stakeholders can be defined in various ways, as it can be defined in a narrow way which can be considered as the primary groups or with a broader definition that is called secondary or instrumental groups (Freeman, 1984).

Freeman's (1984) definition and grouping of stakeholders is that it includes a broader range of stakeholders. This has caused issues such as how to deal with all stakeholders simultaneously in field research (Wagner et al., 2012). This has been described as impossible and the criteria of prioritizing stakeholders have been a theoretical requirement. Seltsikas and Soyref (2013) also argue that an understanding of the complex relationships between and across the network of stakeholders is required when examining stakeholders in information security management.

To further identify stakeholders, there are various proposals for classifying stakeholders in terms of their respective levels of importance. The most common one is the model of Mitchell et al. (1997) called stakeholder salience. The contribution of which has been significant to the theory as it highlights that not all stakeholders are equal, as some stakeholders are more important regarding given issues (Wagner et al., 2012). Since stakeholders can be examined through lenses of power, legitimacy, and urgency. Stakeholders can be compared to these three criteria to identify their salience and then be categorized by high, medium, or low priority (Seltsikas & Soyref, 2013). In this study, a limitation is made to stakeholders who implement and maintain an ISMS with ISO/IEC 27001.

According to Seltsikas and Soyref (2013) senior management and core business teams have a high priority salience to organizational information security practice. Meanwhile consultants have a medium priority. De Vries et al. (2003) also mentions that consultants may have a stake in developing complicated standards in order to assist organizations to implement them. Furthermore, CISO:s has been pointed out to have an important role in ensuring effective and efficient IT security management (Karanja, 2016).

Drawing upon Seltsikas and Soyref's (2013) identification of stakeholder groups in information security processes, stakeholders relevant to ISO/IEC 27001 can further be identified. In line with the stakeholder theory, the ISO/IEC 27000:2018 defines a stakeholder as "*person or organization (3.50) that can affect, be affected by, or perceive itself to be affected by a decision or activity*" (SIS, 2020, p. 5). Susanto et al. (2012) further explain that a stakeholder can be seen as an organization, group, or person who has both a direct or indirect stake within an organization as it can influence and be influenced by policies, objectives, and actions.

Based on ISO/IEC 27001, Beckers et al. (2012a) present the stakeholder theory to identify and describe stakeholders' functional and non-functional requirements on information security by expressing the organizational security problems and objectives. Conversely, it is important to emphasize that the ISO/IEC 27001 standard presents stakeholders as "interested parties", who have the opportunity to express the security problems that exist via the security objectives during the implementation process of an ISMS (Beckers et al., 2012b). Sharma and Dash (2012) further explain that when an organization chooses to adopt the ISO/IEC 27001, it must be supported by concrete business analyzes. This means that the primary business objectives are listed, and a consensus is ensured. To achieve this, key stakeholders need to be involved in the process. As mentioned, to be able to identify key stakeholders' information security objectives, it is relevant to investigate the stakeholders with power, urgency, and legitimacy when it comes to information security (Seltsikas & Soyref, 2013). The MSBS's methodological support states stakeholders such as Chief Information Security Officers (CISO); IT managers; information security officers; data protection officers are relevant stakeholders to involve in the information security work within an organization. By this, these stakeholders can be considered to have the power, urgency and legitimacy when it comes to conducting and influencing how the information security work should be perfomed within an organization. Therefore, it has been relevant to pay attention to the view of these stakeholders in this study to explore the output legitimacy of ISO/IEC 27001 from a stakeholder view based on the information security objectives that they are striving to achieve.

4 Methodology

This section presents and justifies the research approach and methods used for data collection and analysis. The section also presents the epistemology and ontology; how the reliability and validity were ensured; the ethical considerations of the study.

4.1 Epistemology and ontology

The study had an interpretive paradigm in which the epistemological approach has been both subjective and intersubjective. The ontological attitude of an interpretivist reflects a perceived experience, cultural influence, and meaning while acknowledging the potential for realities (Kelly et al., 2018). As researchers, it has therefore been important to recognize the potential of multiple realities. In other words, the intersubjective perspective has provided the opportunity to understand central social constructions depending on personal experiences (Stolorow & Atwood, 1996). Therefore, it has been necessary to interpret the subjective attitudes and acknowledge the researcher's experiences that potentially shape the interpretations (Kelly et al., 2018).

4.2 Qualitative research approach

A qualitative research approach was considered suitable to explore the output legitimacy of the ISO/IEC 27001 from a stakeholder view. Bryman (2016) explains that a qualitative research approach creates the opportunity to collect and analyze empirical data based on the participants' contexts in a detailed way. Unlike quantitative research approaches, where there is more focus on quantified measurements and statements which makes it difficult to study social phenomena (Denscombe, 2018). The qualitative research approach enables researchers to develop knowledge and study cultural as well as social phenomena by understanding people within their context. Another reason why qualitative research studies were considered suitable compared to quantitative studies is due to the possibility of gaining a deeper understanding of the studied issues (Myers & Avison, 2002). The qualitative research approach made it possible to study the output legitimacy of the ISO/IEC 27001 standard from a stakeholder view and understand the phenomenon in its actual context. As Myers and Avison (2002) explain, such forms of research can be more challenging to detect in quantitative research. Because, with quantitative studies, patterns and conclusions are based on data that have been collected with the support of surveys or experiments (Oates, 2006).

4.3 Interview study

To explore the output legitimacy of the ISO/IEC 27001 standard from a stakeholder view, an interview study was conducted. By conducting interviews, it was possible to gain access to information from relevant actors. However, as Oates (2006) explains, such a discussion does not take place by chance but has been planned by the researchers by having designed some specific questions that are concerning the study. To be able to conduct the interviews with well-founded questions, the concept of output legitimacy in relation to the ISO/IEC 27001 standard and the instrumental view of the stakeholder theory was studied. The reason why the instrumental view was studied is to be able to formulate questions that focus on what information security objectives the stakeholders strive to achieve and how the standard can be used to effectively achieve them.

Considering the research purpose, it was relevant to perform interpretive interviews. This in turn, made it possible to explore and interpret the level of output legitimacy of ISO/IEC

27001 from a stakeholder view. Usually, in research, interpretive interviews are used to form an understanding of a phenomenon through people and what they consider to be important in the studied context (Myers & Avison, 2002). In this case, it was possible to gain access to and present other people's interpretations, by filtering them according to stakeholders' information security objectives to later be able to report the identified events.

4.4 Selection of respondents

The respondents were selected according to the recommendations from MBS's methodological support. This means that the respondents who participated have the power, urgency and legitimacy to influence the information security work at their organizations. In other words, they have a high to medium level of priority salience to organizational information security practice (Seltikas & Soyref, 2013). Appendix A presents an overview of the respondents; their responsibilities; to which organization they belong; in which type of organization they work; their categorization to stakeholder salience.

The respondents who participated in the study are working in different private organizations in Sweden. Public organizations were excluded since they are required to adapt and implement ISO/IEC 27001 (MSB, 2020). Ording et al. (2022) further explain that in Sweden the public sector is required to use ISO/IEC 27001, and also follow appropriate and consistent frameworks. This is because the public sector exchanges information within different authorities, therefore it becomes increasingly important to comply with consistent structures and frameworks. By this, the standard can be considered to have a high output legitimacy to achieve requirements from the government. Therefore, to explore the output legitimacy it is considered more suitable when the choice is not required. This made it possible to explore the reasons behind the implementation and the level of output legitimacy of the standard despite the requirements from the government. Another reason for the choice of the specific respondents is to increase the information content of the interviews because the right target group possesses knowledge in the studied area (Holme & Solvang, 1999).

4.5 Data collection

4.5.1 Individual interviews

Individual interviews were conducted with different stakeholders to explore the output legitimacy of the ISO/IEC 27001 standard. This was done to explore the level of the output legitimacy of the standard from the unique stakeholder's view. But also, what the stakeholder in his or her professional role experiences that the standard contributes concerning its information security tasks. Oates (2006) explains that interviews are usually conducted to gain access to information from others and it has an agenda with specific issues that are interesting to discuss with the respondents. In this case, there was an interest to discuss the level of output legitimacy of the ISO/IEC 27001 in relation to the respondents' information security objectives and work tasks. Denscombe (2018) explains that the advantage of conducting individual interviews is that the views raised during the interview come from one specific source, which is the interviewee. This in turn enables the researcher to easily locate special ideas for certain people.

4.5.2.1 Conducting the interviews

Appendix A presents the respondents who were interviewed for the purpose of the study. Before conducting the interview an information letter (Appendix B) was sent to the

respondents. This was done to allow respondents to think about their opinions and establish credibility for the researchers of the study (Oates, 2006). The information letter gave all the participants a fundamental insight into the scope and purpose of the study, but also the opportunity for the respondents to ask questions regarding the study before the interviews were conducted.

The respondents needed to sign a consent form (Appendix C) before conducting the interviews. The purpose of the consent form was to have a written agreement from the participants and that the information provided by them will be processed during the study. Oates' (2006) recommendations were followed, where the respondents, before giving consent to participate in the study, were informed about the scope of the study both in writing and orally to make them fully aware of their commitment and the nature of the research.

Both digital and physical interviews were conducted, as some respondents are based in cities other than the researchers. Therefore, digital tools such as Microsoft Teams and Zoom were used to conduct those interviews. An interview guide was used as a basis for having the ability to address relevant questions concerning the research purpose. Appendix D presents the interview questions and a motivation for why the questions were asked with support of existing research.

Oates's (2006) recommendations were followed by introducing the interviews by asking simple questions to create a safe environment for the respondents before more complex questions were discussed. The interviews were of a semi-structured type. This is because with semi-structured interviews it was possible to deal with questions that were of interest to explore for the study. It also gave the possibility to change the order of the questions depending on the conversation flow (Oates, 2006). In addition to this, it was possible to ask other questions that were not included in the interview guide and the respondents also had the space to answer the questions in a detailed way.

4.5.2 Literature review

A literature review was conducted to become familiar with and collect relevant information for the study. The literature review made it possible to gain deeper insight and develop knowledge in the studied area in an accurate way through an objective compilation of the research that has been conducted (Denscombe, 2018).

To find relevant literature, Web of Science and Scopus were used as search databases. Since they are considered to be comprehensive bibliographic databases that contain international citation indices. Therefore, it was appropriate to use these databases to gain access to peer-reviewed articles, as these databases primarily publish scientific articles that have been reviewed by subject experts before being accepted for publication. To search in the databases, Oates' (2006) recommendations were followed, where boolean expressions such as AND, OR, and NOT were used in electronic searches.

Keywords and terms were identified and used in various combinations during the search process (Appendix E*)*. Oates (2006) explains that by defining keywords and search terms, it will later be possible to use them methodically in the search process.

To have the ability to conduct a literature review, inclusion and exclusion criteria were identified according to Booth et al.'s (2016) recommendations (*see Table 1*). The inclusion criteria were chosen to ensure and more easily select literature that is relevant to the research

area. Meanwhile, the exclusion criteria were used to sort out articles that fulfilled at least one of the criteria.

Inclusion criteria	***Exclusion criteria***
Literature about standards and certification	Literature that compares with other standards not relevant to information security (e.g. ISO 9001, ISO 14001)
Literature about output legitimacy	Literature in languages other than English and Swedish
Literature that concerns stakeholders in management and standards	Articles where full access is not available (e.g. only abstract is available)
Literature about information security management	Non-peer-reviewed literature
Literature about information security management system	Literature that is not related to ISMS and frameworks/standards

Table 1. *Inclusion and exclusion criteria for literature search*

4.5.3 Standard review

The standards ISO/IEC 27001:2017 and 27002:2017 have been studied to understand which security measures they cover and do not cover for ISMS. This later created the foundation for being able to discuss the collected and analyzed empirical data in relation to the standards.

4.6 Data Analysis

4.6.1 Interview analysis

The audio recording of the interviews was transcribed and deductively analyzed. Hyde (2000) explains that the deductive analysis is based on an existing theory to investigate whether it is applicable in specific instances. In this case, to identify the relationships between stakeholder management and the achievement of the organization's performance objectives; the instrumental view of stakeholder theory was used to be able to identify the information security objectives of the stakeholders.

The textual analysis was performed by using the analysis tool MAXQDA. Which is a computer-assisted qualitative tool and is used to analyze text and multimedia in academic, business, and scientific institutions (MAXQDA, n.d.). The data analysis was performed during several iterations. For each iteration, it was possible to identify several information security objectives that each stakeholder actively strives to reach. The detailed objectives were grouped down to eight objectives addressing similar aspects of information security. For each objective, the results were organized according to what level of output legitimacy the ISO/IEC 27001 has from a stakeholder view.

Table 2 presents an example of how the data analysis was performed, where the identified objectives were coded as main categories. Meanwhile, the levels of output legitimacy (high/low) were coded as subcategories. The statements that the standard has a high level of

output legitimacy to achieve a specific objective were coded in the category "*High level of output legitimacy of the standard*". Vice-versa about the statements where the stakeholders experienced that the standard has a low level of output legitimacy. This type of coding was performed iteratively for each stakeholder and each identified objective.

Objective	**Data extract**	**Coded for**
#1 To maintain an ISMS	**"***It is a good foundation and sets requirements for what you need to be aware of, which also results in us being able to work in a qualitative, effective and secure way*" (S1)	High level of output legitimacy of the standard
	"*What is difficult in the standard is how to do things and find a balance regarding that"* (S1)	Low level of output legitimacy of the standard

Table 2. *An overview of how the objectives were coded.*

4.7 Validity and reliability

To ensure the quality of the research, it is necessary to use data of good quality. However, it can be difficult in qualitative research to check the quality and the findings by repeating the process since it can be challenging to copy a social context (Denscombe, 2018). To ensure the accuracy of the findings from the interviews it has been necessary to validate the data through respondent validation, which means the findings of the data analysis were checked together with the respondents. In the following way, it was possible to check the accuracy but also obtain confirmation of the interpretations made.

Before conducting the data analysis, a detailed review of the interview transcripts has also been conducted. This was done by allowing the respondents to take part in the transcribed material, where they had the opportunity to check the information content of the interviews and their statements to ensure that there were no misrepresentations. This resulted in a good foundation for the data-based conclusions and contributed to the increased credibility of the research (Denscombe, 2018).

As reality can be constructed in different ways and the generalizations made in this form of study is primarily due to different environments, times, people, and how the sample group is (Oates, 2006). It has been necessary to provide what type of organizations the various respondents are working in, for other researchers to be able to transfer the discussions and conclusions made in this thesis to their studies. In the following way, opportunities were opened for reusing the results of the study.

4.8 Ethical considerations

For the quality and implementation of the study, ethical considerations and guidelines have had an important role, especially when it comes to the research findings being used responsibly (Swedish Research Council, 2017). To ensure this, the four main principles of ethics presented by Denscombe (2018) were applied during the study:

- Principle 1: *protect the identity of the respondents*. All personal information regarding the respondents was stored locally on the researchers' computers in a

password-protected folder. The results of the interviews were presented anonymously to ensure that no one can identify the respondents.

- Principle 2: *participation in the study was optional and based on informed consent*. All respondents that were involved in the study, were informed that the participation was optional and that they could withdraw whenever they wanted. The participants were provided a consent form, where they can confirm that they have been informed about the study but also that they will provide information that will be processed during the study.

- Principle 3: *avoiding false pretenses and conducting the study with scientific integrity*. It has been necessary to be open and clear about what is happening and for what purpose the information is collected from the participants. Furthermore, it has also been important to maintain a high professional standard and honesty when handling data. Therefore, the data collection and analysis have been done objectively, and by being clear with and acknowledging other research contributions have been used in the study.

- Principle 4: *comply with national law*. Since the study deals with an amount of data that has been generated through interviews, it has been necessary to apply national data protection laws such as
    - GDPR,
    - The Swedish Data Protection Act (2018:218).

  To apply this principle, the names of respondents and the organization they work in were anonymised in the transcripts. All information that can identify the respondents identities was saved in a folder that only the researchers for the study had access to.

5 Results

This section presents the findings from the data analysis. The section introduces the identified information security objectives the various stakeholder groups are striving to achieve with the support of the standard. Thereafter, each information security objective is presented more extensively.

5.1 Stakeholder groups and information security objectives

This section presents the most common information security objectives the various stakeholder groups strive to achieve. It is mainly used to structure the presentation of the results section. The first column of the table presents the objectives that will later be presented in detail; the second column presents which stakeholder groups are striving to achieve a specific objective; the third column presents the anonymized codes of the stakeholders.

Objective	Stakeholder group	Stakeholders
#1	CISO, Information Security Manager, Data Protection Officer, Head of Security, Information security Consultant, IT Manager	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10
#2	CISO, Data Protection Officer, Head of Security, IT Manager	S6, S7, S8, S9, S10
#3	CISO, Information Security Manager, Data Protection Officer, Head of Security, Information security Consultant, IT Manager	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10
#4	CISO, Information Security Manager, Information Security Consultant, IT Manager	S1, S2, S3, S6, S7
#5	CISO, Information Security Manager, Data Protection Officer, Head of Security, Information security Consultant, IT Manager	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10
#6	CISO, Information Security Manager, Head of Security, Information Security Consultant	S1, S2 S5, S6, S7, S8, S10
#7	CISO, Information Security Manager, Data Protection Officer, Head of Security, Information security Consultant, IT Manager	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10
#8	CISO, Information Security Manager, Data Protection Officer, Head of Security, Information security Consultant, IT Manager	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10

Table 3. *Overview of the identified information security objectives various stakeholder groups strive to achieve.*

5.2 Objective #1: To maintain an ISMS

All stakeholders (S1-S10), agreed that the ISO/IEC 27001 standard is a good foundation for being able to work in a qualitative, effective, and secure way to ensure that there is an ISMS

in place for the organization. The standard can be used as a framework to follow up the work regarding information security in a structured way. It supports stakeholders to build a foundation for information security, as it contains several security measures and requirements that can guide them to build processes concerning e.g., information classification. However, S1 experiences that there are aspects in the standard missing today to be able to perform their tasks even more effectively, and explains it in the following way:

> "*If the standard didn't exist, we would probably have failed to implement 20% of the security requirements we have today, but if the standard was complemented with additional 20% of security measures that we lack, it would have been perfect"* (S1).

S2 believes that ISO/IEC 27001 can be seen as a body that explains what an organization needs to succeed in their information security work. But it is the organization's responsibility to what extent they choose to scope the standard to the entire organization or a specific business unit. However, several stakeholders such as S1, S2, S6 and S7 experience that the standard does not have a well-defined *how,* which describes how organizations should proceed. Therefore, stakeholders need to define their security measures based on their business and best practices as well as requirements set by clients and upper management. The stakeholders state that it can be challenging to define a *how* in a standard, as the standard is intended to function in different organizational contexts. On the other hand, S1 believes that defining the *how* would facilitate and increase the output legitimacy of the standard and when it comes to the implementation of the technical measurements. S7 explains that sometimes situations can arise where it is difficult to assess how certain processes should be maintained e.g., how to build a continuity plan to ensure the organization's existence. Meanwhile, S3 explains that defining the *how* depends primarily on what type of organization and business it is as well as its technical environment.

> "*To complement how we shall do, it is important to get support from people who are specialists in our technical systems, who know how to achieve security in the systems we have*" (S3).

S9 explains that it is not enough to just rely on ISO/IEC 27001 to be able to work effectively with information security. People with the right knowledge and skills must address issues that concern information security with the support of the standard, depending on the ambition level in the organization.

> "*Many people think that it is just a matter of purchasing the standard and any person within the organization can conduct this work. It doesn't work that way, the person must have competence in the various areas of information security to be able to navigate the work depending on the ambition level that the organization has set for information security"* (S9).

S9 further emphasizes that the challenge of building the processes and structures in an ISMS is not due to the standard, it is whether the people who perform this work have sufficient work experience or a suitable academic degree.

To fulfill the objective the stakeholders experience that the standard has a high level of output legitimacy and organizations can ensure to cover necessary aspects of information security. On the other hand, employees' work experience and education are of greater importance to be able to fulfill the following objective appropriately. They need to have the understanding and

knowledge of what measures need to be taken in relation to the standard of their specific organization. However, the output legitimacy decreases when there is no well-defined *how,* and stakeholders experience that there are aspects that are missing.

5.3 Objective #2: To achieve an acceptable level of security

Several stakeholders (S6-S10), experience that it is important to achieve an acceptable level of security by basing it on business risks. S6 mentions that a challenge is to determine which level of security they want to be; where information security is most needed; how to handle risks and to which degree.

> "*A challenge I have, from the board, is to decide what level of information security we want to achieve. Where can we take benefits from information and IT security the most? At what level do we manage risks?*" (S6).

S10 explains that their level of security is usually higher than their clients because of supply chain risks since they have to consider their security level as well as their clients. S8 argues that organizations shall not only rely on ISO/IEC 27001 because they primarily need to base their information security work on risks. On the other hand, the stakeholder further explains that certification could help to mitigate the risk of losing important business deals.

> *"The purpose must be that we need to achieve an acceptable level of security, for what we do with our information. I can have my ideas about how it should be but I have to base it on the organization's risk appetite"* (S8).

This is also confirmed by S7, who explains that besides risking losing important business deals, it is at least as important to achieving an acceptable level of security internally. By achieving an appropriate level of security it was also a question of cost. Thus, if the cost is acceptable to mitigate the risk. The risk level that an organization is willing to take was determined by upper management. To achieve the security level set by upper management, the stakeholders mentioned that enough money and resources were allocated. S10 mentions that it is good that ISO/IEC 27001 is based on analysis and risks, which essentially is used to implement something related to information security in the organization or get a budget. Furthermore, to effectively manage information security it is also a question of priority which was stated to be a consequence of goal conflicts and working with it iteratively. S6 refers to the domains that exist in the standard and it is important to work iteratively with those questions that exist in those domains to be better in the long run. S9 further explains that it is important that the information security work is conducted with the support of the entire ISO/IEC 27000 standard series, to be able to work effectively. The standard users need to have an understanding of the connection between ISO/IEC 27001 and the other standards in the series. In other words, the other standards in the series can be seen as complementary parts to the security measures presented in ISO/IEC 27001.

To ensure that the organization has an acceptable level of security it is common to test and measure the number of times an incident has occurred; how well a message is received; awareness in the organization etc. However, S10 experiences it is difficult to take support from ISO/IEC 27001 to effectively conduct these measurements. On the other hand, S9 explains once again that it is possible to take support from other standards in the series such as ISO/IEC 27008 which describes how one can assess the different security measures. Meanwhile, several stakeholders agree that a certification does not tell how well an

organization is in managing its information security work and these measured values do not exist in the certification, it only says whether you have done it or not. Therefore, it was necessary to supplement with a Soc2 audit which is additional costs and time to conduct.

> "*We supplement this with a Soc2 audit where we get an extra audit that says you have 27001, these are your basic controls, how you work with this, how effective you are with this, and how secure more or less you are in your delivery*" (S10).

The stakeholders, in general, experience that the standard has a high level of output legitimacy to have the ability to fulfill the following objective. Especially when the standard is complemented with other standards in the ISO/IEC 27000 series. The stakeholders believe that the certification can also reduce the risk of losing business deals and make employees aware of the importance of information security. However, in some cases, the stakeholders state that it is necessary to complement with other certifications or take support from other frameworks for support, which in turn decreases the output legitimacy of the standard.

5.4 Objective #3: To build information security culture and awareness

Building an information security culture and awareness within the organization and among the employees was a common objective in all interviews conducted. Several stakeholders stated that the ISO/IEC 27001 is not enough to support when it comes to information security culture and awareness, as only one of the 114 controls of the standard covers this issue. This could be experienced as difficult to work effectively when it comes to increasing information security awareness among the organization's employees. S6 explains that the standard is not good support when it comes to developing an information security culture, therefore it may be necessary to use other standards or frameworks to build both technical culture and security awareness. S5 further explains that the standard does not cover security measures regarding culture and awareness sufficiently:

> "*I don't think that ISO 27001 covers security culture and awareness in the same way as ISO 27005, which is a standard that focuses more on security awareness and competence development. These parts are a big problem, considering that most incidents are due to human factors and there is no sufficient support for those aspects in ISO 27001"* (S5).

The stakeholders further emphasized on other factors not directly related to the standard when trying to achieve this objective. To effectively develop a culture and increased awareness, the support of a strong management commitment was important. However, stakeholders such as S3, and S4 experience that they lack this form of commitment from the management. This is because the management either prioritizes other organizational issues and objectives or that they lack sufficient knowledge in information security. Unlike S8, which receives good support from the management and has no problems with them not being responsive when it comes to information security. On the other hand, S7 explained that if upper management decides that the organization shall work according to ISO/IEC 27001, it can reduce discussions regarding information security with for example system developers as they can experience it as unnecessary. Therefore, several stakeholders believe that it is important in building trust between employees and management to increase information security awareness within the entire organization. Even though the chosen frameworks can be considered inappropriate. To encourage the employees to work with the chosen standards and frameworks, S2 believes that it is important to build empathy and understanding for

employees:

> "*To get down to the pillar of information and cybersecurity it is important to show empathy and understanding for employees. Because many experience that the chosen frameworks or standards are not suitable or work effectively for the organization. Therefore, it is important to cooperate and do it in an agile way that suits the business needs*" (S2).

Therefore, stakeholders experience that the output legitimacy of the standard is low for working with information security culture and awareness. Primarily, due to the fact, the standard does not cover necessary security measures concerning those aspects of information security, which can make it difficult to fulfill the following objective. There are also internal and external factors that make this more difficult.

5.5 Objective #4: To comply with laws and regulations

Complying with laws and regulations is an important objective for the stakeholders. S3 explains that the financial sector is strictly regulated, and it is required to comply with national and international laws and regulations that are set against the business.

> "*The financial sector is strictly regulated, and we must comply with the requirements placed on the business from a regulatory perspective. As we are strictly regulated, audits are performed continuously, to check that we in fact, live up to the regulations*" (S3).

Conversely, new laws and regulations make this task more difficult. S1 explains that ISO/IEC 27001 does not guide standard users on how to comply with laws or regulations. But through a systematic approach, it is easier to comply with them. However, S6 believes that it can be difficult for a standard to be comprehensive and state how to comply with laws and regulations. For instance, S7 experiences a lack of appropriate security controls when it comes to the implementation and compliance of the GDPR in ISO/IEC 27001, but at the same time, the laws and regulations are available for organizations to comply with them.

S7 and S9 mention that the standard sets requirements for organizations to continuously monitor laws and regulations that are linked to their unique business and information security. This is because the laws are constantly evolving and therefore it is important to have an insight into how they develop. S7 means by monitoring the laws and regulations it is possible to identify changes and how the organization complies with them based on the requirements set in the standard. Therefore, to keep the organization's ISMS adapted according to the expectations set on them, the stakeholders spend a lot of time continuously monitoring the development of the laws and the requirements set on the organization from a regulatory perspective. S2 also states that by complying with laws organizations can further increase their security posture.

> "*By complying with standard or regulatory requirements such as GDPR or PCI DSS, we can further use it as a stepping stone to further increase and improve organizations' security posture*" (S2).

ISO/IEC 27001 has a decent level of output legitimacy by offering a systematic approach to achieve the objective. However, it is also questioned since the standard does not guide the stakeholders on how they will have the ability to comply with laws and regulations.

5.6 Objective #5: To build trust and relationships about information security

All stakeholders (S1-S10) agree that building trust among employees in information security is an important aspect of their various organizations. The stakeholders' experience, this can be challenging to build, considering that many employees in organizations lack the right knowledge and skills in information security. However, S6 believes that the ISO/IEC 27001 standard has a suitable basis to jointly create an understanding of information security.

> "*Although not everyone in the organization understands all details of the standard, I think it's a good reference framework that can be used to communicate with others and jointly achieve what needs to be achieved"* (S6).

S2 states that it is important to create good communication between the various departments and business areas when it comes to information security. The stakeholder has the responsibility to bridge this gap between the various departments, where frameworks such as ISO/IEC 27001 can be good support for being able to create this overlap.

In addition to building trust within the organization and among the employees, S7 explains that it is at least as important to build trust with their clients. The stakeholder believes that by being ISO/IEC 27001 certified or that the organization complies with the standard, it is possible to create trust with the client about how the supplier works with and ensures information security. However, S10 explains that many clients experience that the standard has lost its value and is not considered as powerful today. S5 further explains that as a consultant when collaboration is initiated with a client, it can be challenging to build with them despite an ISO/IEC 27001 certification.

> "*When you talk about information security, it's a lot of sensitive information, even if you sign a confidentiality agreement. It can take a while before the client learns to trust you and let our consultants do things for them*" (S5).

The output legitimacy of the ISO/IEC 27001 standard can be seen in different ways to fulfill the following objective. To build trust among the organization's employees regarding information security, the standard can be used effectively by stakeholders to primarily communicate about information security. Furthermore, it is a good reference framework to be able to discuss objectives and requirements with other employees with a similar language. However, the output legitimacy of ISO/IEC is not considered high when it comes to building trust and relationships between clients and suppliers. Since certification is not considered sufficient by the clients.

5.7 Objective #6: To achieve clients' information security requirements

Several stakeholders (S1-S2, S5 - S8, S10) point out that one of the most important objectives is to ensure compliance with clients' information security requirements. Stakeholders such as S5, S6, and S8 state that an ISO/IEC 27001 certification is considered an appropriate basis for providing how the organization's information security work is conducted. However, S1 and S7 point out that although the organization is certified according to ISO/IEC 27001, there

are still clients who annually ask them to answer questions on how they deal with their information security requirements.

> "*Many of our large clients demand that we are 27001 certified, or that we should at least be compliant. We annually get a list of 200 - 300 questions, which we must answer. If we hadn't performed the work that we have done and which we still do, we wouldn't have the ability to answer these questions in a good and dignified way*" (S7).

S7 further explains that the reason why clients ask the supplier to answer similar questions as the organization had to answer when applying for a certification, is mainly due to the client assessing the supplier's competence level when it comes to information security. Thus, the client has the opportunity, once again, to evaluate the supplier and if the client has sufficient resources to be able to collaborate with a new supplier. S1 experiences this process as time-consuming and explains it as follows:

> "*We have to work with a lot of administrative tasks when we need to answer so many questions. Especially, when a client has 300 questions about how we deal with information security. This is time-consuming and it is not enough to just refer to our certification to make the clients satisfied. It's a challenge, which takes a lot of time. We had hoped to avoid such issues when we became certified, but we didn't"* (S1).

S7 further explains that although it is a time-consuming process to have to answer several questions even if the organization is certified according to ISO/IEC 27001, this is another opportunity to explain and prove to the client that information security is important for the supplier. However, S10 states that certification makes it more effective when it comes to business deals rather than having to explain everything. S8 further mentions that through certification the organization can indicate that they are ensuring their information security work. Meanwhile, S2 states that the ISO/IEC 27001 sets the scope and requirements that organizations need to comply with, but it is also important to ask oneself whether a certification provides a good insight into if the entire organization complies with the standard.

S10 further explains that an ISO/IEC 27001 results in the organization achieving legitimacy for external parties. However, the certification has decreased in value as there are other certifications available in the market. On the other hand, S1 explains that it is still a good idea to have an ISMS based on ISO/IEC 27001 as it is a sort of best practice. Although the clients can require the supplier to be certified towards other standards that are more industry-developed such as NIST, TISAX, or CVA.

In summary, stakeholders experience that an ISO/IEC 27001 certification can in some cases be a good foundation for clients when collaboration is initiated with a supplier. However, stakeholders experience that in many cases the standard or a certification is not an effective solution for proving to clients that they have ensured information security. Mainly because several stakeholders experience that the certification has lost its value but also that many clients require compliance or certification according to other standards. Considering that stakeholders need support from other resources and frameworks to work effectively, the output legitimacy of ISO/IEC 27001 is considered as low when it comes to this objective.

5.8 Objective #7: To identify and maintain threats, risks, and vulnerabilities

All stakeholders (S1-S10) agree that an important aspect of information security is to continuously work on identifying, managing, and monitoring information security threats, risks, and vulnerabilities. Considering technological development, S4 points out that organizations discuss risks, information security, and threats with a different focus today to be able to ensure and implement appropriate security measures. S9 further explains that organizations have the responsibility, according to ISO/IEC 27001, to continuously work against risks and incidents to improve their information security work.

> "*The organizations have the obligation and a requirement from ISO 27001 to constantly work and improve their information security work"* (S9).

In addition to this, S8 explains that it is important to work risk-based when it comes to information security, where organizations identify in which areas the risk is highest to implement all necessary security measures.

> "*Staring blindly at the standard is not good. Because not all controls in the standard need to be implemented. Therefore, it's important to base the work on risks and based on those, have the most appropriate measures in place*" (S8).

S1 experience that ISO/IEC 27001 presents, on a general level, security measures that are related to risk management. The stakeholder further explains that the organizational requirements for risk mitigation have changed overtime. For instance, the stakeholder mentions that today more organizations are using cloud services and experience that the standard is insufficient support for how to mitigate risks against cloud services. This is also confirmed by S6, who mentions that it is important to know that the standard is not comprehensive in all aspects of information security, especially when it comes to risk management. At the same time, S2 and S3 state that ISO/IEC 27001 consists of security measures that can be used for risk assessment. However, there are no appropriate measures that can support stakeholders in monitoring the implemented measures.

> "*Many times, organizations comply with the standard, but they forget the continuous risk management process and the monitoring of which controls have been implemented. The standard also does not contribute to any support either*" (S2).

To counter this challenge, S7 explains that they continuously conduct a vulnerability audit with support of a technical tool, which scans the organization's applications to identify vulnerabilities that have occurred. Furthermore, S7 states that they also train employees in terms of risk management and identification.

Although several stakeholders experience insufficient support from ISO/IEC 27001 to work with the following objective, S9 and S10 believe that the ISO/IEC 27001 is good support to be able to work risk-based. For instance, S10 states that by using the standard as a checklist, it is possible to achieve the effects that need to be fulfilled.

To be able to identify information security risks, threats, and vulnerabilities, the opinions are divided among the stakeholders when it comes to the output legitimacy and capacity of ISO/IEC 27001. Stakeholders such as S1, S6, and S7 experience that the standard lacks guidelines for being able to work effectively with risk management. While stakeholders such as S2, S3, S9, and S10 believe that the output legitimacy of ISO/IEC 27001 is high, where the

standard includes clear information security measures and requirements on what organizations need to consider when pursuing this objective.

5.9 Objective #8: To ensure technical security

All stakeholders (S1-S10) strive to ensure technical security. However, a challenge that several of the stakeholders experience when it comes to the output legitimacy of the ISO/IEC 27001 standard is that it does not have clear guidelines for new technical solutions. Therefore, it is difficult to deal with these issues effectively and find support from ISO/IEC 27001, as the technical environment is changing faster than the standard. For instance, S1 explains that the standard does not mention anything about ransomware or phishing and how it can be prevented. Furthermore, S2 explains that there are several gaps in the standard:

> "*If I look at specific controls in the standard there are actually gaps. Some of the gaps are session controls, session terminations, security, and privacy attributes - there's none, information sharing is very lacking there, data mining protection, and event logging. The list is quite long*" (S2).

S8 further mentions that there are no technical measures for the management of cloud services; ensuring security in the use of IT, OT, and IoT; how organizations can ensure and minimize their vulnerabilities in their APIs.

> "*We have a lot of APIs, and organizations, in general, need to ensure the protection of their APIs, and this isn't addressed in the standard of how we need to do it. I think it's difficult for the standard to keep up with technological development"* (S8).

Meanwhile, S6 explains that the biggest mistake made in the industry is to view the ISO/IEC 27001 standard as a technical standard. Thus, the stakeholder believes that it is important to understand that the standard consists of administrative requirements that can help organizations tailor their information security work as needed.

> "*When it comes to technology, I think the standard is outdated, but it might be better to move away from the technology and let it live somewhere else and not mention any specific technology in ISO 27001*" (S6).

S7 explains that it is possible to take support from other standards that are more focused on system development and processes, which can provide more detailed insight into how the system development work should be conducted securely. This is confirmed by S3, S4, and S5, which state that it can be more appropriate to use standards such as CVA when it comes to securing cloud services but also to take support from other standards that are more technology-based.

In general, stakeholders experience that ISO/IEC 27001 has a low level of output legitimacy for ensuring technical security. As previously mentioned, several stakeholders experience that the standard lacks suitable guidelines and security measures to handle technical challenges effectively. Therefore, stakeholders believe that, to work effectively with this objective, it is necessary to implement and apply more technology-related standards.

6 Discussion

By incorporating the instrumental view of the stakeholder theory it was possible to identify eight information security objectives among the stakeholders. The view also made it possible to address the needs and interests concerning information security to maximize the effectiveness of ISO/IEC 27001 from a stakeholder view (Welcomer, 2002). Considering that the aim of the instrumental view is to identify the relationships or lack or relationships in the presence of stakeholder management and the achievement of the performance objectives (Cesar, 2019). In this case, there has been an interest in exploring the output legitimacy to achieve the identified information security objectives using the ISO/IEC 27001 standard.

A recent study by Andersson et al. (2022) studied the structures that affect the input and throughput legitimacy of ISO/IEC 27001. Meanwhile, this study complements by exploring the output legitimacy of the standard in relation to the identified information security objectives from a stakeholder view. Another study by Silva et al. (2016) explains when industry representatives are included during the standard development process, they are more likely to defend it accordingly. This study further confirms that industry representatives are more likely to comply with and rely on more industry-based standards such as TISAX (*See 5.7 Objective #6*). This in turn raises question regarding the output legitimacy of the ISO/IEC 27001 standard, as more resources are required to be able to work effectively with the information security objectives. However, the findings indicate that being certified with ISO/IEC 27001 makes this process easier and can reduce the number of questions asked by clients, and can make business deals go smoother.

Organizations usually implement ISO/IEC 27001 to ensure that there is a reviewable, consistent and repeatable way of dealing with information security issues and objectives. Furthermore, by complying with the standard the trust among internal and external stakeholders increases as the organizations can prove that the security is managed effectively (Ashenden, 2008). Compliance with an ISMS standard is an effective way of working with ISM. However, complying with an ISMS standard can not always be considered an easy task, as the requirements of a standard can be complex and difficult to understand (Susanto & Almunawar, 2015).

For the standard to have a high level of output legitimacy and for stakeholders to reach their objectives, it can be necessary to include relevant stakeholders in the standardization process. This will open the possibilities of influencing and addressing important objectives and security measures in the standard. In other words, by allowing stakeholders to participate in the standardization process, with openness, transparency, and the use of consensus for decision-making, the input and throughput legitimacy will increase (Andersson et al., 2022). This in turn will have an impact on the output legitimacy of the standard.

6.1 Implications for research

This study explores the output legitimacy of ISO/IEC 27001 based on eight information security objectives that were identified with support of the instrumental view of the stakeholder theory. The results section presents which stakeholders are striving to achieve which objective and their view on ISO/IEC 27001 capacity to fulfill the identified objectives effectively. What is possible to indicate is that all stakeholders agree that the ISO/IEC 27001 has a high problem-solving capacity and output legitimacy to maintain an ISMS. The predefined security measures in the standard enables the stakeholders to implement appropriate measures effectively. The standard offers a strategic and comprehensive approach

to information security. It also provides guidelines for how the management of business risks should be conducted in the implementation, establishment, operation, and monitoring process of an ISMS (Susanto & Shobairah, 2016). The standard explains how to maintain the CIA of an organization's information assets, by applying a risk management process while creating trust among stakeholders to manage the risks adequately (Aginsa et al., 2016). This is confirmed by the findings, where the stakeholders experience that the standard works as intended and has a high level of output legitimacy to maintain a management system for information security.

Meanwhile, the stakeholders experience there is insufficient guidance for ensuring technical security in the standard, which results that the output legitimacy of the standard is experienced as low. However, Kurnianto et al. (2018) emphasize that ISO/IEC 27001 presents technical security measures, but the standard is intended to focus on the implementation and management of an ISMS. Therefore, it is important not to consider ISO/IEC 27001 as a technical standard. On the other hand, it is about the whole process of increasing information security awareness and compliance (Kurnianto et al., 2018). Thus, ISM depends on technology, people, and processes (Ashenden, 2008; Nancylia et al., 2014). Culot et al. (2021) further point out that ISO/IEC 27001 is still treated as a technical standard within academia. Therefore, there is a need for changes in the increasingly interconnected world with new technical possibilities and challenges. At the same time, it is necessary to emphasize that Annex A of the ISO/IEC 27001 standard specifies and covers several technical measures such as operational security; logging and monitoring; management of technical vulnerabilities; security in development, and support processes, etc. (SIS, 2017). Meanwhile, the results also indicate, for the standard to have a high level of output legitimacy stakeholders with the right knowledge and skills must be working with information security. Because stakeholders with the right knowledge and skills will have the capacity to navigate the work regarding information security more adequately with the support of ISO/IEC 27001.

The opinions among the stakeholders are also divided when it comes to the security measures that concern risk management in ISO/IEC 27001. Some stakeholders experience that the standard does not cover the necessary measures to be able to work effectively with risk management and assessment. However, clause "*6.1 Actions to address risks and opportunities*" in ISO/IEC 27001 presents what organizations need to consider when working with information security risks. The clause guides stakeholders on what they need to proceed in a risk assessment and treatment (SIS, 2017). Furthermore, Carvalho and Marques (2019) explain that when stakeholders apply the standard, they will have the ability to evaluate and identify information security risks to later be able to implement the necessary security measures and procedures to preserve the CIA of information. Meanwhile, Alebrahim et al. (2014) state that the ISO/IEC 27001 standard consists of general concepts that can be used in risk management, but it does not specify which method stakeholders should use to identify threats and vulnerabilities which is an essential part of risk assessment.

Other aspects that decrease the output legitimacy of ISO/IEC 27001 is that the stakeholders experience that the standard provides insufficient guidance on how they should comply with laws and regulations. However, by having a systematic approach it is possible to comply with regulations such as GDPR. Similar indications are possible to identify in previous research, where organizations that comply with the standard have a better foundation for complying with GDPR (Lopes et al., 2019; Diamantopoulou et al., 2020). This further raises the question of whether it is stakeholders' interpretations and expertise in working with the standard or the

design that is behind it. Especially when the findings also indicated that people's experience in information security is lacking.

6.2 Implications for practitioners

The findings indicate that it is important to invest in the knowledge about the standard among standard users and stakeholders. Thus, it is important to not only focus on the standard development, but also on competence development regarding ISO/IEC 27001 and information security. Because if the standard users lack the right knowledge and skills regarding information security, it will be more difficult to navigate the work with the support of the standard. Considering that stakeholders experience that there are security measures that are lacking in the standard, although those aspects are stated in the standard. Therefore, it is important to increase the knowledge about the standard to reach a high level of output legitimacy. Above all, standard users need to understand that the ISO/IEC 27001 is not intended to function as a technical standard but as a standard for implementing, establishing, and operating an ISMS. In other words, if stakeholders understand the purpose of the standard and its structure, they will have the ability to use it more effectively.

Furthermore, this study justifies for practitioners that ISO/IEC 27001 does not describe *how* organizations should perform their information security work, but *what* they need to do to ensure that it is done appropriately. The standard presents 114 security measures that are suitable for implementation. However, each organization has a responsibility to tailor *how* these measures need to be implemented and established in the organization's ISMS.

7 Conclusion

The purpose of this study was to explore the output legitimacy of the ISO/IEC 27001 from a stakeholder view and its ability to achieve stakeholders' information security objectives. This was done by incorporating the instrumental view of the stakeholder theory. By considering the theory, eight information security objectives could be identified. Depending on this it was possible to explore the output legitimacy of the ISO/IEC 27001 and how the standard meets stakeholders desires.

According to the findings of the study, the output legitimacy of the ISO/IEC 27001 varies depending on which objective the stakeholders want to achieve. Considering the aim of the standard is to implement, establish, operate and monitor the ISMS, the stakeholders' experience that the standard has a high level of output legitimacy to maintain those aspects of an ISMS. Since it provides free rein for stakeholders to effectively tailor the information security work according to the information security needs and requirements, which exist within their unique businesses. The standard can also be used as a reference framework when organizations and stakeholders discuss information security with each other, which can result in effectively being able to build relationships and trust between all involved parties. In other words, ISO/IEC 27001 has the capacity to build the gaps that exist between different stakeholders and business units.

In relation to the objective "*To maintain an ISMS*", the output legitimacy of ISO/IEC 27001 is not considered as high when working with objectives concerning risk management and ensuring technical security. According to the standard, organizations need to continuously identify their risks, threats, and vulnerabilities. But several stakeholders experience that there is a lack of guidance in the standard on how to work and mitigate the risks, which decreases the output legitimacy of the standard. However, this raises the question of if the stakeholders have sufficient knowledge and understanding of the standard, as it covers several security measures about risk assessment and management. Furthermore, stakeholders need to understand that the standard is not intended to be a technical standard but to be the foundation for implementing, establishing, monitoring, and operating the ISMS of an organization. In other words, it is not only a matter of focusing on standard development, but also a competence development among standard users to increase the output legitimacy of ISO/IEC 27001.

In summary, to reach a high level of output legitimacy of ISO/IEC 27001, stakeholders and standard users must have the right knowledge and skills regarding the standard, but also about information security. Therefore, it is necessary within organizations to invest in the standard users and increase their awareness and knowledge of the standard and information security, to be able to navigate the work more easily and effectively and achieve the information security objectives with the support of the standard.

Limitations

This study has explored the output legitimacy of the ISO/IEC 27001 and how stakeholders can achieve their information security objectives by using this standard. However, the study was not free from limitations. One limitation is the small number of study participants. Thus, to have the ability to confirm the results one step further, more interviews would have been performed. Although saturation was achieved in the data collection phase, there are still aspects that need to be further explored and confirmed when it comes to the output legitimacy of ISO/IEC 27001. Considering this has been an explorative study, it has not covered the

output legitimacy of ISO/IEC 27001 from all possible stakeholder views who use the standard. To gain a more detailed insight into the output legitimacy of the standard, there is a need to interview all relevant standard users to cover more stakeholders' views and their experiences of the standard. In addition to this, this study only presents a few information security objectives that stakeholders are striving to achieve by using the ISO/IEC 27001, but it has not identified or covered a complete set of objectives. This is important to pay attention to, considering that the output legitimacy of the standard has not been explored in relation to other possible security objectives that stakeholders are striving to achieve.

However, the study provides a basic understanding of the output legitimacy of the standard about the most common information security objectives. Future research can use this study to further investigate the output legitimacy of ISO/IEC 27001 more extensively, by considering the limitations of this study.

Future research

Considering that there will be an updated version of ISO/IEC 27001, future research to explore the output legitimacy of the ISO/IEC 27001:2022 can be performed. This would create the opportunity for researchers to study the similarities and differences between the existing and future versions of the standard. If the output legitimacy of the forthcoming version of the standard differs among the stakeholders to be able to process the identified information security objectives.

Future research can also explore the output legitimacy of other information security standards. This will create the opportunity to study the similarities and differences between the different standards. This will create the opportunity to explore if other standards have a higher or lower output legitimacy to achieve stakeholder objectives.

References

Aginsa, A., Edward, I. Y. M., & Shalannanda, W. (2016, August). Enhanced information security management system framework design using ISO 27001 and zachman framework-A study case of XYZ company. In *2016 2nd International Conference on Wireless and Telematics (ICWT)* (pp. 62-66). IEEE.

Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information security management system. *International Journal of Computer Applications*, *158*(7), 29-33.

Alebrahim, A., Hatebur, D., & Goeke, L. (2014, August). Pattern-based and ISO 27001 compliant risk analysis for cloud systems. In *2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)* (pp. 42-47). IEEE.

Algheriani, N. M. S., Kirin, S., & Spasojevic Brkic, V. (2019). Risk model for integrated management system. *Tehnički vjesnik, 26*(6), 1833-1840.

Annarelli, A., Clemente, S., Nonino, F., & Palombi, G. (2021). Effectiveness and Adoption of NIST Managerial Practices for Cyber Resilience in Italy. In *Intelligent Computing* (pp. 818-832). Springer, Cham.

Andersson, A., Karlsson, F., & Hedström, K. (2020). Consensus versus warfare–unveiling discourses in de jure information security standard development. *computers & security*, *99*, 102035.

Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security–a structurational analysis. *Information & Management*, *59*(3), 103623.

Ashenden, D. (2008). Information Security management: A human challenge?. *Information security technical report*, *13*(4), 195-201.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: shaping an international information systems security standard. *MIS Quarterly,* 413-438.

Bailur, S. (2006). Using stakeholder theory to analyze telecenter projects. *Information Technologies & International Development*, *3*(3), pp-61.

Bakker, A. (2018). *OSSUM: a framework for determining the quality of Information Security Assessment Methodologies* (Master's thesis, University of Twente).

Beckers, K., Faßbender, S., Heisel, M., Küster, J. C., & Schmidt, H. (2012a, February). Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches. In *International Symposium on Engineering Secure Software and Systems* (pp. 14-21). Springer, Berlin, Heidelberg.

Beckers, Fassbender, S., Heisel, M., & Schmidt, H. (2012b). Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security

Management Systems Development and Documentation. 2012 Seventh International Conference on Availability, Reliability and Security, 242–248.

Beckers, K. (2015). Supporting ISO 27001 Compliant ISMS Establishment with Si. In *Pattern and Security Requirements* (pp. 109-137). Springer, Cham.

Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In *2008 Second International Conference on Emerging Security Information, Systems and Technologies* (pp. 224-231). IEEE.

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic approaches to a successful literature review* (Second edition.). Sage.

Botzem, S., & Dobusch, L. (2012). Standardization cycles: A process perspective on the formation and diffusion of transnational standards. *Organization Studies, 33*(5-6), 737-762.

Brugha, R., & Varvasovszky, Z. (2000). Stakeholder analysis: a review. *Health policy and planning*, *15*(3), 239-246.

Brunsson, N., Rasche, A., & Seidl, D. (2012). The dynamics of standardization: Three perspectives on standards in organization studies. *Organization studies*, *33*(5-6), 613-632.

Bryman, A. (2016). *Samhällsvetenskapliga metoder.* Malmö: Liber AB.

Bäckstrand, K. (2006). Multi-stakeholder partnerships for sustainable development: rethinking legitimacy, accountability and effectiveness. *European environment, 16*(5), 290-306.

Carvalho, C., & Marques, E. (2019, June). Adapting ISO 27001 to a Public Institution. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE

Castka, P. and Prajogo, D. (2013), The effect of pressure from secondary stakeholders on the internalization of ISO 14001. *Journal of Cleaner Production*, Vol. 47, pp. 245-252.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," Information Systems Research (16:1), pp 28-46.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385-400.

Cesar, S. (2019). Earning a social license to operate in mining: A case study from Peru. *Resources Policy*, *64*, 101482.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society*, *19*(3), 355-375.

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, 47(3), 79-86.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. TQM Journal, 33(7), 76–105.

Denscombe, M (2018). *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna* (Fjärde upplagan). Studentlitteratur.

De la Plaza Esteban, C., Visseren-Hamakers, I. J., & de Jong, W. (2014). The legitimacy of certification standards in climate change governance. *Sustainable Development, 22*(6), 420-432.

De Vries, H., Verheul, H., & Willemse, H. (2003, December). Stakeholder identification in IT standardization processes. In *Proceedings of the Workshop on Standard Making: A Critical Research Frontier for Information Systems. Seattle, WA* (pp. 12-14).

Dhillon, G. (2018) *Information Security: Text & Cases*. 2nd Edition. Prospect Press, Burlington, USA, 413 pages. ISBN: 9781943153251

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio organizational perspectives. *Information systems journal*, *11*(2), 127-153.

Dinu, V. (2017). Quality management and business excellence. Amfiteatru Economic Journal, 19(44), 5-7.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of management Review, 20*(1), 65-91.

Douvreleur, P. (2019). Challenges Faced by Legal Counsels in Big Data and Cybersecurity Activity. *Int'l. In-House Counsel J.*, *12*, 1.

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Zamani, E., & Maglaras, L. A. (2019). Real-time information security incident management: a case study using the IS-CHEC technique. *IEEE Access*, *7*, 142147-142175.

Fenz, S., & Neubauer, T. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002. Information & Computer Security.

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci*, *48*(2), 213-222.

Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Boston, MA: Pitman.

Freeman, R. E., Phillips, R., & Sisodia, R. (2020). Tensions in stakeholder theory. *Business & Society, 59*(2), 213-231.

Föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Myndigheten för samhällsskydd och beredskaps författningssamling. https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf

Galbreth, M.R., and Shor, M. 2010. "The Impact of Malicious Agents on the Enterprise Software Industry," MIS Quarterly (34:3), pp 595-A510.

Gao, Y. (2021, August). A Promising Application Prospect of Blockchain in Banking Industry from the Perspective of Stakeholder Theory. In *1st International Symposium on Innovative Management and Economics (ISIME 2021)* (pp. 161-165). Atlantis Press.

Hamdi, Z., Norman, A. A., Molok, N. N. A., & Hassandoust, F. (2019, December). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012103). IOP Publishing.

Heron, J. (9 July 2018) ISO 27001:2013 and ISO 27001:2017 what's the difference? *ISMS.online*. https://www.isms.online/iso-27001/iso-27001-2013-iso-27001-2017-whats-the-difference/

Holme, I. M., & Solvang, B. K. (1997) *Forskningsmetodik Om kvalitativa och kvantitativa metoder* Malmö: Holmbergs i Malmö AB

Hu, Q., Hart, P., and Cooke, D. (2007). "The Role of External and Internal Influences on Information Systems Security a Neo-Institutional Perspective," The Journal of Strategic Information Systems (16:2), pp 153-172.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221-232.

Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative market research: An international journal*.

ISO (2021). *The ISO survey of management system standard certifications 2020*. Retrieved 2022-01-17 from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO (n.d.). *ISO STANDARDS ARE INTERNATIONALLY AGREED BY EXPERTS*. Retrieved 2022-03-23 from https://www.iso.org/standards.html

Kallberg, J. (2012). The common criteria meets realpolitik: Trust, alliances, and potential betrayal. *IEEE Security & Privacy, 10*(4), 50-53.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*.

Kelly, M., Dowling, M., & Millar, M. (2018). The search for understanding: The role of paradigms. *Nurse Researcher*, *25*(4), 9-13.

Kica, E., & Bowman, D. M. (2012). Regulation by means of standardization: key legitimacy issues of health and safety nanotechnology standards. *Jurimetrics*, 11-56.

Kurnianto, A., Isnanto, R., & Widodo, A. P. (2018). Assessment of information security management system based on ISO/IEC 27001: 2013 on subdirectorate of data center and data recovery center in ministry of internal affairs. In *E3S Web of Conferences* (Vol. 31, p. 11013). EDP Sciences.

Makeri, Y. A. (2020). The Strategy Detection on Information Security in Corporate Organizations on Crucial Asset. *JOIV: International Journal on Informatics Visualization*, *4*(1), 35-39.

Mansell, S. F. (2013). *Capitalism, corporations and the social contract: A critique of stakeholder theory*. Cambridge University Press.

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. *arXiv preprint arXiv:1108.2150*.

MAXQDA (n.d.). *All-in-one Qualitative Analysis Software*. Retrieved 2022-04-04 from https://www.maxqda.com/qualitative-analysis-software?gclid=CjwKCAjw7IeUBhBbEiwADhiEMQeeIZgq6PVhF966s1tdtnoVBtVI9MmRX9rDO_o4R87yUW45PEvmYxoC32YQAvD_BwE

Mayntz, Renate (2010). Legitimacy and compliance in transnational governance. Working Paper 10/5. Cologne: Max Planck Institute for the Study of Societies.

Mena, S., & Palazzo, G. (2012). Input and output legitimacy of multi-stakeholder initiatives. Business Ethics Quarterly, 22(3), 527-556.

Mishra, A., & Dwivedi, Y. K. (2012). Stakeholder theory and applications in information systems. In *Information Systems Theory* (pp. 471-488). Springer, New York, NY.

Mitchell, R., Agle, B. and Wood, D. (1997), “Toward a theory of stakeholder identification and salience: defining the principle of who and what really counts”. *Academy of Management Review*, Vol. 22 No. 4, pp. 853-8.

Myers, M. D., & Avison, D. (Eds.). (2002). *Qualitative research in information systems: a reader*. Sage.

Myndigheten för samhällsskydd och beredskap (2018). *Security culture and information technology SECURIT* (MSB1222). https://rib.msb.se/filer/pdf/28479.pdf

Nancylia, M., Mudjtabar, E. K., Sutikno, S., & Rosmansyah, Y. (2014, October). The measurement design of information security management system. In *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-5). IEEE.

Niemimaa, E. (2016). Legitimising Information Security Policy during Policy Crafting: Exploring Legitimising Strategies.

Nyman, M., & Große, C. (2019). Are You Ready When It Counts? IT Consulting Firm's Information Security Incident Management. In *ICISSP* (pp. 26-37).

Oates, B. J. (2006). *Researching information systems and computing* . SAGE Publications.

Ojalainen, A. (2020). ISO 27001 information security management standard's implementation in software development environment: a case study.

Ording, L. G., Gao, S., & Chen, W. (2022). The influence of inputs in the information security policy development: an institutional perspective. *Transforming Government: People, Process and Policy*, (ahead-of-print).

Orozova, D., Kaloyanova, K., & Todorova, M. (2019). Introducing Information Security Concepts and Standards in Higher Education. *TEM Journal*, *8*(3), 1017.

Pavlov, G., & Karakaneva, J. (2011). Information security management system in organization. *Trakia Journal of Sciences, 9*(4), 20-25.

Piper, L. (20 January 2019). Ledn sys ISO 27001:2017 - att tänka på för en certifiering. *4Certifiering*. https://www.4certifiering.se/index.php/saekerhet-ledn-sys-iso-27001-2017

Proença, D., & Borbinha, J. (2018, July). Information security management systems-a maturity model based on ISO/IEC 27001. In *International Conference on Business Information Systems* (pp. 102-114). Springer, Cham.

Scharpf, F. W. (1999). *Governing in Europe: Effective and democratic?* Oxford/New York: Oxford University Press.

Schmidt, A. (2009, November). Conceptualizing Internet security governance. In *GigaNet: Global Internet Governance Academic Network, Annual Symposium*.

Schmidt, V. A. (2013). Democracy and legitimacy in the European Union revisited: Input, output and 'throughput'. *Political Studies*, *61*(1), 2-22.

Seltsikas, P., & Soyref, M. (2013). Information security: a stakeholder network perspective. In *ACIS 2013: Information systems: Transforming the Future: Proceedings of the 24th Australasian Conference on Information Systems* (pp. 1-11). RMIT University.

Sharma, N. K., & Dash, P. K. (2012). Effectiveness of ISO 27001, as an information security management system: an analytical study of financial aspects. *Far East Journal of Psychology and Business, 9*(3), 42-55.

Shojaie, B., Federrath, H., & Saberi, I. (2014, September). Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In *2014 Ninth International Conference on Availability, Reliability and Security* (pp. 259-264). IEEE.

Silva, L., Hsu, C., Backhouse, J., & McDonnell, A. (2016). Resistance and power in a security certification scheme: the case of c: cure. *Decision Support Systems, 92*, 68-78.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*.

Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

Stolorow, R. D., & Atwood, G. E. (1996). The intersubjective perspective. *Psychoanalytic review*, *83*(2), 181-194.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*, *2*(1), 67-75.

Susanto, H., & Almunawar, M. N. (2015). Managing compliance with an information security management standard. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1452-1463). IGI Global.

Susanto, A., & Shobariah, E. (2016, April). Assessment of ISMS based on standard ISO/IEC 27001: 2013 at DISKOMINFO Depok City. In *2016 4th International Conference on Cyber and IT Service Management* (pp. 1-6). IEEE.

Susanto, H., & Almunawar, M. N. (2018). *Information security management systems: A novel framework and software as a tool for compliance with information security standards*. Apple Academic Press.

Swedish Research Council (2017). Good Research Practice. Vetenskapsrådets rapportserie VR1710

Swedish Standards Institute. (2020). *Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Översikt och terminologi* (ISO/IEC 27000:2018). Svenska institutet för standarder. https://www-sis-se.db.ub.oru.se/produkter/terminologi-och-dokumentation/ordlistor/informationsteknik-ordlistor/ss-en-isoiec-2700020202/

Swedish Standards Institute. (2017). *Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav* (ISO/IEC 27001:2013 med Cor 1:2014 and Cor 2:2015). Svenska institutet för standarder. https://www-sis-se.db.ub.oru.se/produkter/terminologi-och-dokumentation/informationsvetenskap-publicering/dokument-for-administration-handel-och-industri/ssenisoiec270012017/

Tanadi, Y., Soeprajitno, R. R. W. N., Firmansah, G. L., & El Karima, T. (2021). ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology. *Riset Akuntansi dan Keuangan Indonesia*, *6*(2), 198-204.

Tanovic, A., Butkovic, A., Orucevic, F., & Mastorakis, N. (2014). The importance of introducing Information Security Management Systems for Service Providers.

Ţigănoaia, B. (2015). Some aspects regarding the information security management system within organizations–adopting the ISO/IEC 27001: 2013 standard. *Studies in Informatics and Control, 24*(2), 201-210.

Tjirare, D. J., & Shava, F. B. (2017, May). A gap analysis of the ISO/IEC 27000 standard implementation in Namibia. In *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-10). IEEE.

Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, 3(3), 128-135.

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

Uwizeyemungu, S., & Poba-Nzaou, P. (2015, February). Understanding information technology security standards diffusion: An institutional perspective. In *2015 International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 5-16). IEEE.

Verizon (2021). *Data Breach Investigations Report (DBIR) 2021.*

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Wagner, E., Mainardes, Alves, H., & Raposo, M. (2012). A model for stakeholder classification and stakeholder relationships. *Management Decision, 50*(10), 1861–1879.

Welcomer, S. A. (2002). Firm-stakeholder networks: Organizational response to external influence and organizational philosophy. *Business & Society*, *41*(2), 251-257.

Werle, R., & Iversen, E. J. (2006). Promoting legitimacy in technical standardization. *Science, Technology & Innovation Studies, 2*(1), 19-39.

Wiedenhöft, G., Luciano, E. M., & Testa, M. G. (2014). An indicators-Based Approach to Measuring Information Technology Governance Effectiveness: a Study with Brazilian Professionals. In ECIS.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Law and Governance*, *9*(2).

Appendices

Appendix A - Roles, responsibilities and organization type

Stakeholder	Role	Responsibility	Organisation no.	Organization type	Salience
S1	Information Security Manager	Ensure that the organization has an ISMS in operation and that all employees work in accordance with it. Furthermore, answer questions concerning information security from clients as well as setting requirements and follow up with the clients.	1	Computer programming	High Priority
S2	Consultant: Manager of two business units: ● Governance risk and compliance and ● Resilience and readiness	Currently working with risk assessment by using different risk management frameworks such as NIST, RMF but also ISO 27001, 27002, and PCI DSS.	2	Computer consulting business	Medium Priority
S3	CISO	Works with external and internal monitoring of the organization. That the organization complies with its information security objectives. The stakeholder has also the responsibility to train the personnel in information security and ensure appropriate technical security measures are implemented.	3	Lending activities	High Priority
S4	IT Manager	Ensures that the servers, clients, telephones, networks, and server rooms are in operation. Everything concerning the IT infrastructure and environment.	3	Lending activities	Medium Priority

S5	Consultant: Delivery Manager Cybersecurity & Law	Develops governing documents, policies, and instructions with the support of the ISO/IEC 27001 for various employees or IT personnel. Trains the personnel in information security.	4	Computer consulting business	Medium Priority
S6	CISO	Managing, leading, and developing new policies and guidelines that are group exceeding in information security for the organization.	5	Security business	High Priority
S7	Regional Manager/Information Security Officer/IT Manager	As regional manager, the stakeholder has the task of being responsible for the offers that the organization provides for its clients, i.e. process automation. As an information security manager, the stakeholder's task is to ensure that the organization complies with its ISO/IEC 27001 certification by continuously working according to the standard's various processes. As an IT manager, the stakeholder has a responsibility for the internal IT work in the organization.	6	Computer consulting business	High Priority
S8	Head of Security	Maintains the information security risks and how the organization manages its information assets by ensuring that only authorized people have access to confidential information and ensuring the integrity and availability of the information. Furthermore, the stakeholders continuously work with implementing accurate security measures for the organization.	7	Engineering company	High Priority
S9	Data Protection Officer	Implements and maintains the ISMS for the organization. Ensures that appropriate information security processes are implemented. Furthermore, the stakeholder has the responsibility for data protection in the organization's applications and how personal data is maintained and processed.	8	Investment and venture capital company	High priority
S10	Head of Security Governance/	The stakeholder has varying tasks and the work	9	Computer consulting	High Priority

	Head of Security Protection	depends primarily on what the threat and risk look like both internally and externally. Works continuously with reviews, monitoring the business, and ensuring that the implemented controls are used appropriately. Conducts information security awareness campaigns that address topical issues.		business	

Appendix B - Invitation letter

[*Translated from Swedish*]

Hi,
We are Yasmin Kamil and Sofia Lund who are studying the master's program in information security management at Örebro University. At the moment we are writing our master thesis in the field of information security.

The purpose of our master thesis is to investigate the effectiveness of the ISO 27001 standard after implementation and its problem-solving capacity. A part of the study is about conducting interviews with relevant stakeholders, to be able to investigate different stakeholders' perspectives on the international standard. Therefore, it would be appreciated if it is possible to have an interview with you between 7/3 - 6/5-2022. It is most likely possible to conduct the interview during a later time. If that's the case, we appreciate it if you contact us with dates that would be suitable as soon as possible. Participation is completely optional and you can withdraw your participation at any time without further justification.

The interview is estimated to take approximately one and a half hours. The interview will take place at a time and place jointly determined in advance. It is possible to conduct the interview either digitally or at your workplace during a time that suits you. If possible, we wish to be able to record the interviews to have it as a basis for transcription. Before conducting the interview, it is also possible to gain access to the interview questions.

The information you provide will be treated anonymously, so that no outside parties can identify you. Your information will only be processed by us who conduct the master thesis. The results will be presented in the form of a written thesis and an oral presentation. Once the thesis has been approved, it will be uploaded on the DiVA portal and the thesis will be available to the public. The recordings and transcripts of the interviews will be deleted when the thesis is approved. You will have the opportunity to take part in the thesis by receiving a copy.

During the interview, we will have a greater focus on the ISO 27001 certification and its relevance. A certification against ISO 27001 can, for example, be compared with a driving license. Thus, the certification does not present the number of times the organization has had a security incident and how well the organization actually manages security when it comes to their information assets.

We hereby ask if you want to participate in this study by replying to this email or contact us directly. If you have questions about the study, you are welcome to contact us.

Best regards,

Yasmin Kamil
Student
xxxxx@gmail.com
+46(0)70-XXX XX XX

Sofia Lund
Student
xxxxx@gmail.com
+46(0)73-XXX XX XX

Appendix C - Consent form

[*Translated from Swedish*]

Consent form for master thesis 2022

I have been informed about the purpose of the study in writing and agree to participate in interviews.

I have had the opportunity to get my questions answered regarding the interview before conducting the interview and I know who I can ask my questions to

I participate optionally in the study and can cancel my participation without giving further justification for the reason behind this by contacting one of the researchers for the study by e-mail or phone.

I give my consent to Yasmin Kamil and Sofia Lund to document, process and archive the information collected during the interviews. The data collected from the interview will be treated confidentially and anonymously as well as organizational affiliation linked to individual statements will not be published either.

By ticking the box, I confirm to participate in the study and agree that Örebro University processes my personal data in accordance with the The Swedish Data Protection Act.
(Name), (Email), (Place and date)

I hereby enter into (the yellow) and (our contact information) an agreement to participate in the study and agree that my data will be processed according to the information I have been assigned.

Appendix D - Interview guide

[*Translated from Swedish*]

Question(s)	***Comment***	***Source/Theory***
1. What is your role and what kind of tasks do you have that are related to information security? - *How would you describe your role when it comes to the work for an information security management system/information security?* 2. Why is it important to achieve / Why do you want to achieve it / Why do you need to achieve it? 3. How is it linked to information security? (How is information security important in your work?)	*The questions are asked in order to understand the key stakeholders' work tasks when it comes to information security and why it is important for the stakeholder to achieve these goals/tasks.* *By understanding each stakeholder's work tasks, it will be possible to identify themes, if they have any common tasks or if these tasks collide with others.*	Considering that a stakeholder can be defined in various ways (Freeman, 1984), there is therefore an interest to get a deeper understanding of the stakeholders involved in the study, to be able to define them appropriately. Furthermore, the questions are asked to understand how the stakeholders affect decisions or activities concerning information security within an organization (SIS, 2020). In other words, how the stakeholders have a direct and indirect influence within an organization that can have an impact on the policies, objectives and actions (Susanto et al., 2012).
4. What is important for you to be able to perform your work tasks effectively? - What goals do you want to achieve when it comes to information security work for a management system? - How, if in any way, does the standard support you in achieving these goals/objectives? (What opportunities do you face when using the standard?) - *(Opportunities can be related to "What support does the standard provide to be able to perform your tasks")*	*The question is asked to understand which resources the stakeholder needs to be able to perform his tasks effectively and correctly.* *The question is asked to understand and interpret what information security goal each stakeholder has based on their tasks. The question can help us to identify and find patterns between the goals and also be able to identify goals that are not related to other stakeholder's goals.* *The question is asked to understand if ISO 27001 contributes to opportunities in order for a stakeholder to conduct his work effectively.*	By considering the instrumental view of the stakeholder theory it can be possible to identify the relationships and lack of relationships between the fulfillment of the traditional business objectives and stakeholder management (Donaldson & Preston, 1995). Since there is an interest to explore the standard's problem-solving capacity and output legitimacy, it is important to gain an understanding of how the standard solves collective problems and meets stakeholders expectations (Maynz, 2010).

5. What are your challenges when it comes to your work tasks? - How, if in any way, does the standard prevent you from achieving these goals/objectives? - (What challenges do you face while using the standard?)	*The question is asked to be able to identify challenges that each stakeholder faces during the implementation of his work. This question can help us to identify patterns and differences between the various stakeholders' tasks.* *The question is asked to understand if ISO 27001 contributes to challenges for the stakeholder to be able to conduct his work effectively.*	Output legitimacy is generated from problem-solving capacities or expectations of standard adopters are met (Botzem & Dobusch, 2012). To achieve output legitimacy, it must be possible to solve problems collectively and successfully. The purpose from this perspective is "good governance" or in the case of standardization referring to "good" standards (Werle & Iversen, 2006). To achieve output legitimacy in standardization, it is necessary that the standard solves collective problems or meets stakeholders' expectations (Mayntz, 2010). Therefore, the higher the degree of acceptance of a standard, the higher its coordination ability will be, which is the core of output legitimacy. However, it is important to point out that what is gained in output legitimacy does not always result in a standard's overall and long-term stability, especially if it is a result of or reduces input legitimacy (Botzem & Dobush, 2012).
6. What is important for you to be able to carry out your work tasks effectively with the support of the standard?	*The question is asked to understand what is important that the standard presents from a stakeholder view in order for him to be able to conduct his work effectively and in a well functioning way.*	To solve organizational issues concerning information security, the organization needs to have deeper interactions and transactions with critical groups, otherwise it will result in failures (Bailur, 2006). In the context of implementation of standards, there are a variety of stakeholders to be involved in the process from senior management to employees (SIS, 2017).Output legitimacy is primarily about the standard's effectiveness and problem-solving capacity (Botzem and Dobusch, 2012).
7. What aspects do you experience are missing in ISO 27001 + 2 standards in relation to your work tasks, if any?	*The question is asked to investigate if there are any aspects that the standards have not considered in relation to the stakeholders daily work.*	To achieve output legitimacy in standardization, it is necessary that the standard solves collective problems or meets stakeholders expectations (Mayntz, 2010)". Therefore, if something is missing then they can see the

		standard as beneficial and in terms of "good" resulting in loss of legitimacy.
8. In relation to your tasks, what do you think is important that the standard contributes?	*The question is asked to investigate which aspects that the stakeholder thinks are important that the standard emphasizes in order for him to be able to conduct his tasks effectively.*	When it comes to the stakeholder theory, and the instrumental view of the theory, it is important to examine the relationships between the stakeholder management and the achievement of the organization's performance objectives (Mishra & Dwivedi, 2012). By understanding this it will be possible to understand the effectiveness and output legitimacy of the standard and how it can be associated with the perception of the results among a wider range of stakeholders (De La Plaza Esteban et al., 2014).
9. What does the standard contribute to between the different tasks? - What is the purpose of the tasks?	*The question is asked to investigate whether the standard contributes to any goal conflicts based on the different goals that each stakeholder has.*	As Donaldson and Preston (1995) mentions, the instrumental view of the stakeholder theory can help to identify the relationships and lack of relationships between the fulfillment of the traditional business objectives and stakeholder management. Therefore, it is of interest to investigate the standard's problem-solving capacity. Considering, to achieve output legitimacy in standardization it is important that the standard can solve collective problems and meet stakeholders expectations (Maynz, 2010).

Appendix E - Keywords and search terms

- ISO 27*** (27000, 27001, 27002)
- Information Security
- Information Security Management (ISM)
- Information Security Management System (ISMS)
- Standards
- Input legitimacy
- Output legitimacy
- Stakeholder theory
- Stakeholder