Information Systems and e-Business Management (2023) 21:699–722
https://doi.org/10.1007/s10257-023-00646-y

ORIGINAL ARTICLE

Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden

Yasmin Kamil[1] · **Sofia Lund**[1] · **M Sirajul Islam**[1,2]

Received: 19 January 2023 / Revised: 3 June 2023 / Accepted: 17 July 2023 / Published online: 21 August 2023

Abstract

Organizations use the ISO/IEC 27001 standard to establish an information security management system (ISMS). This standard outlines specific security measures and requirements that organizations can implement to effectively manage their information assets. However, the effectiveness of the standard's problem-solving capabilities has raised some questions. Consequently, there is a continuous development of new governance methods that demand fresh approaches to validate security operations and measures. In light of this, research is being conducted to examine the application and impact of ISO/IEC 27001, as well as to analyze the challenges and knowledge gaps through theoretical perspectives. By employing stakeholder theory, the focus shifts towards integrating business and social issues and exploring how non-business pressures can influence stakeholder motivations in implementing standards. Additionally, it investigates the impact of these standards on an organization's reputation, performance, and operations. Therefore, the objective of this study is to investigate the output legitimacy of ISO/IEC 27001 from the perspective of stakeholder expectations. To accomplish this, an interview-based study was conducted, involving relevant stakeholders engaged in information security management within private organizations in Sweden. The findings reveal eight key information security objectives. The results indicate that the level of output legitimacy of the standard varies across these objectives, ranging from high to medium to low. To achieve a high level of output legitimacy for ISO/IEC 27001, stakeholders must understand that the standard is not solely a technical document. Furthermore, stakeholders need to possess the appropriate knowledge and skills in information security to effectively navigate their work while leveraging the support provided by the standard.

Keywords ISO/IEC 27001 · Output legitimacy · Stakeholder theory · Information security standard · Private organizations · Sweden

Extended author information available on the last page of the article

1 Introduction

To ensure information security within organizations, it is advisable to establish an information security management system (ISMS) that facilitates the control and secure management of information (Nancylia et al. 2014). The implementation of an ISMS encompasses strategies and policies aimed at preserving the confidentiality, integrity, and availability (CIA) of critical business information assets (Fonseca-Herrera et al. 2021). Moreover, an ISMS empowers organizations to enhance the effectiveness of managing their information assets (Susanto et al. 2011). This standard defines security requirements and measures that can be integrated into an ISMS, providing organizations with the necessary framework to manage their information assets (Al-Dhahri et al. 2017). The standard offers support for implementing, establishing, operating, and improving the organization's ISMS, which can be tailored to meet specific organizational needs (Orozova et al. 2019). While ISO/IEC 27001 provides an overview of security measures, ISO/IEC 27002 offers detailed guidelines, focusing on technical and formal security measures. Failure to adopt a suitable ISMS for operations and information systems can compromise the ability to ensure business continuity (Santos-Olmo et al. 2016). By adhering to standards such as the ISO/IEC 27000 series, organizations can establish a robust ISMS framework. This series of standards provides requirements that assist in safeguarding an organization's information assets effectively (Hamdi et al. 2019).

Implementing the ISO/IEC 27000 series ensures that the organization has a suitable ISMS in place. Organizations should leverage information security standards to implement suitable security measures (Tjurare & Shava, 2017). However, selecting and implementing an appropriate ISMS standard can pose challenges (Susanto and Almunawar 2018). Conversely, organizations must demonstrate their commitment to secure business practices by adopting authoritative guidelines (Siponen & Wilson, 2009). It is important because business partners may require proof of information asset protection. Thus, there should be available evidence showcasing adequate protection measures (Von Solms 1999).

Furthermore, organizations primarily embrace information security standards for market assurance and governance (Shojaie et al. 2014). These standards are regarded as necessary and influential tools today, given the rising threats of cybercrime, hacktivism, and foreign governments targeting valuable organizational assets (Andersson et al. 2020). In other words, safeguarding organizations' information assets is crucial, particularly in interconnected business environments, to mitigate the impact of security incidents and ensure business continuity (Proença & Borbina, 2018). By obtaining ISO/IEC 27001 certification, organizations can demonstrate that they have achieved an acceptable level of security, fostering customer confidence (Disterer 2013). Additionally, the standard not only guides organizations in implementing a management system but also aims to enhance their legitimacy and credibility (Douvreleur 2019).

Legitimacy can be categorized into three domains: input, throughput, and output legitimacy (Scharpf 1999; Schmidt 2013). To attain output legitimacy through ISO/IEC 27001, the standard must effectively address collective problem-solving (Werle and Iversen 2006). However, the effectiveness of ISO/IEC 27001 in terms of informa-

tion security, and therefore its output legitimacy, can be questioned (Uwizeyemungu and Poba-Nzaou 2015). Hence, security managers should design and adapt security practices based on stakeholders' values to avoid doubts regarding output legitimacy (Topa and Karyda 2019).

Output legitimacy pertains to the problem-solving capacity and effectiveness of policies or standards (Bäckstrand 2006). It is crucial for standards to address collective problems and meet stakeholders' expectations (Mayntz 2010). Hence, an organization's foundational documents and policies must effectively align with stakeholders' values (Schmidt 2013). Specifically, the effectiveness of ISO/IEC 27001 in resolving issues and meeting stakeholders' expectations becomes significant (Mena and Palazzo 2012). Conducting a stakeholder analysis is essential to gather and analyze information about stakeholders, understanding their perspectives, and identifying factors that can influence decision-making (Brugha & Varvasovzky, 2000). As new governance approaches emerge, there is a need for new methods to legitimize security operations and measures (Schmidt 2009). In this regard, engaging relevant stakeholders can enhance output legitimacy (Christou 2018). Scholars like Culot et al. (2021) propose conducting theory-based research to examine the effects and application of ISO/IEC 27001. By applying stakeholder theory, the integration of business and social issues can be explored, considering how non-business pressures impact stakeholders' motivations during standard implementation and influence an organization's reputation and operations (Castka and Prajogo 2013). The stakeholder theory emphasizes building relationships and creating value for stakeholders, underscoring the importance of organizations addressing stakeholder interests to enhance performance (Gao 2021). Moreover, by considering the stakeholder theory, attention can be given to stakeholders' interests concerning an organization's information security objectives (Yaokumah & Brown, 2014).

Given the above justifications and considering the expectations in information security management, the objective of this study is to examine the output legitimacy of ISO/IEC 27001 based on the perspectives of various stakeholders. The research question is formulated as follows: "*What are the viewpoints of different stakeholders in information security management regarding the output legitimacy of ISO/IEC 27001 in achieving their information security objectives*?" To address this research question, an interview-based study was conducted with stakeholders employed in private organizations in Sweden. The organizations included in the study were either ISO/IEC 27001 certified or implemented the standard to uphold their information security practices. This study is particularly relevant to stakeholders working in private organizations who are interested in exploring the output legitimacy of ISO/IEC 27001, both at a national and international level. The findings can provide stakeholders with valuable insights into the effectiveness of the standard and its ability to address common information security issues that are relevant to multiple stakeholders. Additionally, the study aims to contribute to the academic understanding of the output legitimacy of the standard from a stakeholder perspective, offering a deeper insight into its implications.

2 Related research

2.1 Information Security Management System (ISMS) standards

Standards can be regarded as repositories of best practices derived from expert knowledge in a particular field (ISO, n.d.). They encompass a set of requirements that products or systems should meet, offering solutions to recurring challenges (Tofan 2011). In the realm of information security, there exist several recommended standards that organizations can adopt to ensure the safeguarding of their information assets (Bakker 2018). For instance, ISMS standards enable organizations to methodically document, establish, and consistently manage procedures aimed at ensuring the security and reliability of their information assets. These standards serve as the foundation for achieving the CIA (Confidentiality, Integrity, and Availability) of vital business assets, which is the fundamental objective of information security (Rezakhani et al. 2011). Notable examples of ISMS standards include ISO/IEC 27001, BS 7799, and NIST SP800 (Tofan 2011; Susanto and Almunawar 2018).

The ISO/IEC 27001 standard has gained significant international recognition and adoption. It is jointly developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (Tofan 2011). The initial version of ISO/IEC 27001 was published in 2005 as an evolution of the BS 7799 standard (Shojaie et al. 2014). The most recent international version of the standard was released in 2013, with notable changes such as alignment with the structure of other standards like ISO/IEC 9001 and 14,001. Additionally, the requirement for documented procedures and records was replaced with documented information, and certain requirements were revised or removed (Ţigănoaia 2015). ISO/IEC 27001 specifies requirements for establishing, implementing, maintaining, and improving an information security management system within an organizational framework. These requirements are generic and applicable to organizations of any size, type, or nature. However, the standard provides guidelines rather than mandating specific actions (Swedish Standards Institute [SIS], 2017). The ISO/IEC 27000 series is based on risk management and includes 114 security measures. ISO/IEC 27001 sets forth the requirements for an ISMS to achieve certification, outlining seven key elements: establishment, implementation, operation, monitoring, review, maintenance, and improvement of the system. It is intended to be used in conjunction with ISO/IEC 27002. While the standard presents a structured set of information security measures, organizations are free to implement additional effective measures as long as they align with ISO/IEC 27001 (Tofan 2011). The standard covers best practices and security measures related to areas such as security policy, governance, asset management, human resources security, physical and environmental security, communication and operations management, development and maintenance, information security incident management, business continuity management, and compliance (Tofan 2011; SIS, 2017).

In Sweden, the current version of the standard is SS-ISO/IEC 27001:2017, which is applicable as a national standard (SIS, 2017). However, no significant changes were made compared to the 2013 version, and it was intended to seek approval by CEN/CENELEC for the EN designation (Heron 2018). The modifications in the 2017

version are minimal, with two Corrigendum/Amendments addressing Clause 6.1.3 and Annex A Clause 8.1 (Piper 2019). These changes include recognizing information itself as an asset that can be part of the inventory and presenting the Statement of Applicability (SoA) in bullet form, highlighting four elements (Heron 2018). The SoA document specifies the number of security measures, the names of the controls, and the results of control implementation (Tanovic et al. 2014).

2.2 Output legitimacy

Scharpf (1999) and Schmidt (2013) have identified three distinct domains of legitimacy: input legitimacy, throughput legitimacy, and output legitimacy. Input legitimacy emphasizes the significance of participation and consensus in decision-making, with choices being deemed legitimate when they align with the will of the people (Scharpf 1999). This domain emphasizes stakeholder involvement, ensuring that all participants have equal opportunities to contribute to the establishment of standards (Kica & Bowman, 2012). Throughput legitimacy centers on the decision-making process itself and its quality. It examines factors such as effectiveness, accountability, transparency, inclusiveness, and openness (Scharpf 1999). It necessitates the presence of mechanisms and transparency to guarantee responsiveness to stakeholders (Kica & Bowman, 2012). On the other hand, output legitimacy focuses on the effectiveness of problem-solving through the implementation of laws or standards (Scharpf 1999). This aspect of legitimacy assesses the outcomes of the decision-making process and evaluates whether they effectively address stakeholder issues (Kica & Bowman, 2012).

The operationalization of output legitimacy has traditionally been centered around the concept of effectiveness, which can be understood as the institutional performance in terms of results. In this regard, output legitimacy is closely linked to how a wider range of stakeholders perceives the outcomes (De La Plaza Esteban et al., 2014). When implementing standards, various stakeholders, ranging from senior management to employees, need to be involved in the process (SIS, 2017). Botzem and Dobusch (2012) further elaborate that output legitimacy primarily revolves around the effectiveness and problem-solving capabilities of the standard, making it a crucial aspect of its dissemination. Consequently, the dissemination of rules becomes essential for establishing a sustainable standardization regime, as a high level of standard application contributes to output legitimacy. In this context, output legitimacy pertains to the relevance of the content outlined in documents and can also be measured by observing behavioral changes among actors associated with ISO/IEC 27001.

As mentioned, output legitimacy in standardization is derived from the standard's ability to effectively solve problems or meet the expectations of its adopters (Botzem and Dobusch 2012). Achieving output legitimacy necessitates collective and conscious actions from relevant stakeholders to successfully address specific issues (Tofan 2011). The ultimate goal, from this perspective, is to establish "good governance," where the focus in standardization is on developing "good" standards rather than distinguishing between different standards adopted by organizations, as long as they prove beneficial (Werle and Iversen 2006). Richardson and Eberlein (2011) propose that a technically sound standard can be recognized as "good" if experts in

the field acknowledge its ability to resolve technical problems or facilitate future developments. In this context, output legitimacy primarily revolves around the standard itself, contrasting with the input legitimacy that emphasizes the standardization process. As stakeholders' expectations are expected to be met through output legitimacy in standardization (Mayntz 2010), a higher degree of acceptance for a standard enhances its coordination capacity. However, it is important to note that gaining output legitimacy does not always guarantee the overall and long-term stability of a standard, particularly if it comes at the expense of or diminishes input legitimacy (Botzem and Dobusch 2012).

Some studies have investigated the legitimacy of information security standards, including works by Backhouse et al. (2006), Kallberg (2012), Silva et al. (2016), Aldya et al. (2019), Lopes et al. (2019), Diamantopoulu et al. (2020), and Andersson et al. (2022). Backhouse et al. (2006) and Silva et al. (2016) emphasize the importance of involving industry representatives in the development of standards to ensure legitimacy and credibility. When participants feel a sense of ownership over the standard, they are more likely to defend and support it. Andersson et al. (2022) conducted a recent study that identified the structures influencing the input and throughput legitimacy of information security standards. Kallberg (2012) highlights the significance of building alliances and trust when establishing and maintaining standards. Various groups, such as NATO, the EU, the African Union, and the Union of South American Nations, have demonstrated the advantages of collaboration in this regard. However, the aspect of output legitimacy, which relates to problem-solving capacity and effectiveness, has received limited attention in the literature.

2.3 Definition and classification of stakeholder

One of the widely used definitions of an organizational stakeholder is provided by Mansell (2013), who defines stakeholders as "any group or individual who can affect or is affected by the achievement of an organization's objectives" (p. 30). However, stakeholders can be defined in different ways, encompassing both narrow and broader perspectives. Freeman (1984) introduces the concept of stakeholders having a "stake" in the organization, emphasizing the importance of considering their perspectives. Stakeholders can be categorized into primary groups or secondary/instrumental groups based on the breadth of the definition (Freeman 1984). Considering how organizations incorporate their information security mechanisms into their processes when working with information security standards is also crucial (AlKalbani et al., 2017). This integration plays a significant role in gaining legitimacy, as it is a vital component for organizations, enabling growth, resource acquisition, strategic transformation, and sustainability (Niemimaa, 2016).

In order to further classify stakeholders, there have been various proposals that consider their levels of importance. One widely used model is the stakeholder salience model developed by Mitchell et al. (1997). This model has made a significant contribution to stakeholder theory by highlighting that not all stakeholders have equal importance, as certain stakeholders may be more crucial in specific issues (Wagner et al. 2012). The stakeholder salience model suggests that stakeholders can be assessed based on three criteria: power, legitimacy, and urgency. By comparing stakeholders

against these criteria, their salience can be determined and they can be categorized as having high, medium, or low priority (Seltsikas and Soyref 2013). In this particular study, the focus is placed on stakeholders involved in the implementation and maintenance of an ISMS in accordance with ISO/IEC 27001. It is important to note that this study limits the analysis to these specific stakeholders.

Building on the identification of stakeholder groups in information security processes proposed by Seltsikas and Soyref (2013), it is possible to further identify stakeholders relevant to ISO/IEC 27001. Consistent with stakeholder theory, the ISO/IEC 27000:2018 standard provides a definition of a stakeholder as "*a person or organization 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) elaborate that stakeholders can be organizations, groups, or individuals who have a direct or indirect interest in an organization, and can both influence and be influenced by its policies, objectives, and actions.

ISO/IEC 27001 serves as a framework for identifying and describing stakeholders' functional and non-functional requirements in information security, as discussed by Beckers et al. (2012a). The standard refers to stakeholders as "interested parties" who have the opportunity to express security problems and objectives during the implementation of an Information Security Management System (ISMS) (Beckers et al. 2012b). Sharma and Dash (2012) emphasize the importance of conducting thorough business analyses to support the adoption of ISO/IEC 27001. This involves listing primary business objectives and achieving consensus among stakeholders. Key stakeholders play a crucial role in this process. As previously mentioned, identifying the information security objectives of key stakeholders requires investigating those with power, urgency, and legitimacy in the realm of information security (Seltsikas and Soyref 2013). According to the methodological support provided by the Management System for Business Security (MSBS), stakeholders such as Chief Information Security Officers (CISOs), IT managers, information security officers, and data protection officers are considered relevant to the information security work within an organization. These stakeholders are identified as having the power, urgency, and legitimacy to influence and shape how information security practices are conducted within the organization. Therefore, it is crucial to consider the perspectives of these stakeholders in the study to explore the output legitimacy of ISO/IEC 27001 from a stakeholder viewpoint, taking into account the information security objectives they aim to achieve. By understanding their views, the study can provide insights into the effectiveness and relevance of ISO/IEC 27001 in meeting the information security goals of these key stakeholders.

3 Methodology

Overall. this study employs a qualitative research approach to investigate the output legitimacy of ISO/IEC 27001 from the perspective of relevant stakeholders and their expectations. Qualitative research allows for in-depth data collection and analysis within the specific contexts of the participants (Bryman, 2016). It focuses on providing detailed descriptions and understanding how reality is socially constructed.

Additionally, qualitative research aims to apply existing theories to specific examples (Eisenhardt and Graebner 2007). To conduct informed interviews, the researchers studied the concept of output legitimacy in relation to the ISO/IEC 27001 standard and the instrumental view of stakeholder theory. The instrumental view was particularly relevant for formulating questions that explore the stakeholders' information security objectives and how the standard can effectively help achieve them. Given the research objective, interpretive interviews were deemed appropriate. These interviews allow for exploration and interpretation of the level of output legitimacy of ISO/IEC 27001 from a stakeholder perspective. Interpretive interviews are commonly used in research to gain insights and understanding of a phenomenon through the perspectives of individuals and their priorities within the specific context being studied (Myers and Avison 2002).

3.1 Selection of respondents

The respondents for this study were selected based on the guidelines provided by the Swedish Civil Contingencies Agency (MSB). The selection criteria focused on individuals who held positions of power, urgency, and legitimacy in relation to information security within their respective organizations. The appendix provided in the study (available on bit.ly/27001-iso-iec) outlines the details of the respondents who participated in the research. These participants were employed in nine private organizations in Sweden, representing various industries such as software development, computer consulting, financial lending, security, engineering, and investment and venture capital businesses. The choice of these organizations was driven by the intention to explore the output legitimacy of ISO/IEC 27001 across different sectors. By including organizations from diverse industries, the study aimed to identify similarities and differences in how the standard contributes to the achievement of information security objectives across various organizational contexts. Public organizations were excluded from the study as they are mandated to adopt and implement ISO/IEC 27001 according to the guidelines provided by the Swedish Civil Contingencies Agency (MSB, 2020).

3.2 Conducting the interviews

The study used a combination of online and physical interviews to gather data from the respondents. Due to the remote location of some participants in relation to the researchers, online collaboration tools such as Microsoft Teams and Zoom were utilized to conduct interviews with them. The interviews followed a semi-structured approach, where an interview guide was used as a framework to address pertinent questions related to the research purpose. Appendix B (available on bit.ly/27001-iso-iec) provides details of the interview questions used in the study, along with an explanation of why these questions were asked, supported by existing research. The use of semi-structured interviews allowed for flexibility and the exploration of in-depth insights from the participants in relation to the output legitimacy of ISO/IEC 27001.

3.3 Interview analysis

The audio recordings of the interviews were transcribed, and a deductive analysis approach was employed. Deductive analysis involves using an existing theory to investigate its applicability in specific instances (Hyde 2000). In this study, the instrumental view of stakeholder theory was used as the theoretical framework to identify the information security objectives of the stakeholders and examine the relationships between stakeholder management and the organization's performance objectives. To facilitate the analysis of the transcribed data, the computer-assisted qualitative analysis tool MAXQDA was utilized. MAXQDA is a software tool commonly used in academic, business, and scientific institutions for the analysis of text and multimedia data. By utilizing MAXQDA, the researchers were able to organize, code, and analyze the textual data efficiently, aiding in the interpretation of the findings and the identification of patterns and themes related to the output legitimacy of ISO/IEC 27001 from a stakeholder perspective.

4 Results

This section presents the results obtained from the analysis of the data. It begins by introducing the information security objectives identified by different stakeholder groups, all working towards their achievement with the aid of the standard. Subsequently, each information security objective is presented in greater detail, providing a comprehensive understanding.

4.1 Stakeholder groups and information security objectives

In this section, we outline the prevailing information security objectives pursued by different stakeholder groups. It serves as a framework for organizing the results section. Table 1's first column presents the objectives that will be elaborated upon subsequently. The second column specifies the stakeholder groups actively working towards each specific objective. The third column displays anonymized codes assigned to the stakeholders. For further details regarding the stakeholders' roles, responsibilities, and the types of organizations they represent, please refer to Appendix A (accessible at bit.ly/27001-iso-iec).

4.1.1 Objective #1: to maintain a well-defined ISMS

All stakeholders (S1-S10), unanimously agreed that the ISO/IEC 27001 standard provided a solid foundation for establishing a qualitative, efficient, and secure operational environment with an ISMS in place. The standard serves as a comprehensive framework for systematically addressing information security concerns. It empowers stakeholders to establish a robust groundwork for information security by incorporating various security measures and requirements that facilitate the development of processes such as information classification. However, S1 expressed that there were

Table 1 Overview of the identified information security objectives various stakeholder groups strive to achieve

Objec.	Stakeholder groups	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

certain aspects currently absent from the standard, which could enhance their ability to perform their tasks even more effectively. S1 elaborated on this matter as follows::

> "*If the standard were non-existent, we would likely have fallen short in implementing 20% of the current security requirements. However, if the standard were augmented with an additional 20% of the security measures we currently lack, it would attain perfection."* (S1, Software development company).

S2 held the view that ISO/IEC 27001 served as a comprehensive framework that outlined the necessary requirements for organizations to achieve success in their information security efforts. However, it is ultimately the organization's responsibility to determine the level of scope they wish to apply the standard, whether it encompasses the entire organization or specific business units. Nevertheless, several stakeholders, including S1, S2, S6, and S7, encountered a perceived lack of specific guidance in the standard regarding "how" the implementation processes take place. As a result, stakeholders found themselves in the position of defining their own security measures based on their unique business needs, industry best practices, and the expectations set forth by clients and upper management. Defining the "how" within a standard poses challenges due to its intended applicability across various organizational contexts. It is worth noting, however, that S1 believed that explicitly defining the implementation process would greatly facilitate and enhance the overall legitimacy of the standard,

particularly when it comes to implementing technical measures. S7 explained that certain circumstances may arise where it became challenging to determine how specific processes should be maintained, such as developing a continuity plan to ensure the organization's continued existence. On the other hand, S3 clarified that the definition of the "how" primarily depends on the organization's type, nature of business, and the technical environment it operates within.

> *"In order to effectively determine how we should proceed, it is crucial to seek support from individuals who specialize in our technical systems and possess the knowledge of achieving security within those systems."* (S3, Financial lending company).

To achieve the objective, stakeholders perceived that the standard holds a significant level of output legitimacy, enabling organizations to address essential aspects of information security. However, the effectiveness of fulfilling this objective relies heavily on the work experience and education of employees. It is crucial for them to possess a thorough understanding and knowledge of the specific security measures required by their organization, aligned with the standard. Nevertheless, the output legitimacy diminishes when there is a lack of well-defined implementation guidelines or a clear "how." Stakeholders observed that certain crucial aspects were missing, thereby hindering the optimal attainment of the objective.

4.1.2 Objective #2: to achieve an acceptable level of security

Several stakeholders (S6-S10) emphasized the significance of attaining an acceptable level of security that was aligned with business risks. S6 acknowledged the challenge of determining the desired security level, identifying areas where information security was most crucial, and establishing appropriate measures for risk management.

> *"One challenge I face from the board, is to determine the desired level of information security we aim to achieve. Where can we derive the greatest benefits from information and IT security? And at what level should we effectively manage risks?"* (S6, Security company).

S10 elaborated that their security level was typically higher than that of their clients due to the presence of supply chain risks. They must consider not only their own security level but also that of their clients. In contrast, S8 argued that organizations should not solely rely on ISO/IEC 27001 but rather prioritize basing their information security efforts on risks. However, the stakeholder also acknowledged that certification could assist in mitigating the risk of losing significant business opportunities.

> *"The objective is to attain an acceptable level of security for the organization's information. While I may have personal opinions on how it should be achieved, ultimately, it must be aligned with the organization's risk appetite".* (S8, Engineering company).

In order to ensure that the organization maintains an acceptable level of security, it is customary to conduct testing and measurements, such as tracking the frequency of incidents, evaluating message reception, and assessing organizational awareness. However, S10 found it challenging to utilize ISO/IEC 27001 effectively for these measurement purposes. On the other hand, S9 suggested that support can be sought from other standards within the series, such as ISO/IEC 27008, which guides on assessing various security measures. Meanwhile, multiple stakeholders concurred that certification alone did not indicate how well an organization manages its information security efforts, and those measured values were not included in the certification process. The certification merely confirmed whether the required actions had been implemented or not. Consequently, supplementing with a Soc2 audit became necessary, despite the additional costs and time it entails.

> *"We complement this by conducting a Soc2 audit, which provides an additional assessment that not only verifies adherence to ISO/IEC 27001 and the basic controls but also evaluates how effectively the organization works with these controls and gauges the level of security in its operations."* (S10, Computer consulting company).

The stakeholders, overall, found that the standard possesses a high level of output legitimacy, enabling it to effectively accomplish the following objectives, particularly when combined with other standards in the ISO/IEC 27000 series. They believed that certification can mitigate the risk of losing business opportunities and raised employees' awareness regarding the significance of information security. However, in certain instances, stakeholders highlighted the need to supplement the standard with additional certifications or seek support from other frameworks, which may diminish its output legitimacy.

4.1.3 Objective #3: to build an information security culture and awareness

Building an information security culture and promoting awareness among employees emerged as a common objectives in all the interviews conducted. Multiple stakeholders expressed the view that ISO/IEC 27001 is insufficient in supporting the development of information security culture and awareness. They highlighted that out of the 114 controls in the standard, only one specifically addressed this issue. Consequently, effectively enhancing information security awareness within the organization can be challenging. S6 elaborated on the inadequacy of the standard in supporting the development of an information security culture, suggesting the need to utilize other standards or frameworks to foster both technical culture and security awareness. Additionally, S5 emphasized that the standard didn't adequately encompass security measures concerning culture and awareness:

> *"In my opinion, ISO 27001 does not comprehensively address security culture and awareness in the same manner as ISO 27005. The latter standard places more emphasis on security awareness and competence development. These aspects pose significant challenges, given that most incidents are attributed to*

human factors. ISO 27001 lacks sufficient support in addressing these specific areas." (S5, Computer consulting company).

The stakeholders highlighted additional factors that play a crucial role in achieving the objective of developing a strong information security culture and increased awareness. They emphasized the importance of strong management commitment for effective implementation. However, stakeholders like S3 and S4 reported a lack of such commitment from management. This could be due to management prioritizing other organizational issues and objectives, or lacking sufficient knowledge of information security. In contrast, S8 expressed satisfaction with the support received from management and did not face responsiveness issues concerning information security. On the other hand, S7 explained that if upper management decides to adopt ISO/IEC 27001, it can reduce discussions about information security with system developers, as they may perceive it as unnecessary. Therefore, multiple stakeholders believe that building trust between employees and management is crucial for enhancing information security awareness across the entire organization.

4.1.4 Objective #4: to comply with laws and regulations

Compliance with laws and regulations is a significant objective for the stakeholders. S3 specifically highlighted that the financial sector operates under strict regulations, requiring adherence to national and international laws and regulations that were applicable to their business operations.

"*In the financial sector, strict regulations are in place, and it is imperative for businesses to comply with these regulatory requirements. Continuous audits are conducted to ensure that the organization is adhering to the regulations effectively.*" (S3, Financial lending company).

On the contrary, the introduction of new laws and regulations adds complexity to the task of compliance. S1 pointed out that ISO/IEC 27001 did not provide explicit guidance on complying with specific laws or regulations. However, through a systematic approach, it became easier to align with these requirements. S6 believed that it can be challenging for a standard to be all-encompassing and provide detailed instructions on complying with every law and regulation. For instance, S7 highlighted the lack of adequate security controls in ISO/IEC 27001 for implementing and complying with the General Data Protection Regulation (GDPR). However, organizations had access to the laws and regulations themselves, which they must follow to ensure compliance.

Both S7 and S9 emphasized that ISO/IEC 27001 established requirements for organizations to continually monitor laws and regulations that were relevant to their specific business and information security. This was crucial due to the ever-evolving nature of laws and regulations, requiring organizations to stay informed about their development. S7 highlighted that by monitoring these changes, organizations can identify any modifications and assess their compliance based on the requirements outlined in the standard. Consequently, stakeholders invested significant time in continuously monitoring legal developments and the regulatory expectations placed on

their organization's Information Security Management System (ISMS). S2 further pointed out that compliance with laws not only ensured adherence but also contributed to enhancing an organization's overall security posture.

4.1.5 Objective #5: to build trust and relationships about information security

All stakeholders (S1-S10) unanimously agreed that establishing trust among employees regarding information security was a critical aspect within their respective organizations. They acknowledged that building such trust can be challenging, particularly due to the lack of appropriate knowledge and skills in information security among many employees. Nevertheless, S6 expressed the belief that the ISO/IEC 27001 standard provided a suitable foundation for collectively fostering an understanding of information security.

> "*While not everyone within the organization may grasp all the intricacies of the standard, it is considered a valuable reference framework that enables effective communication and collaboration towards shared objectives."* (S6, Security company).

S2 emphasized the significance of establishing effective communication channels among different departments and business areas concerning information security. The stakeholder recognized their responsibility in bridging the gap between these diverse units. Frameworks like ISO/IEC 27001 can serve as a valuable support in fostering collaboration and facilitating the necessary overlap between departments to promote a cohesive approach to information security.

The output legitimacy of the ISO/IEC 27001 standard serves different purposes in fulfilling the objective of building trust among the organization's employees in information security. Stakeholders found the standard effective in communication and using a common language when discussing information security objectives and requirements. It served as a valuable reference framework in these internal interactions. However, the output legitimacy of ISO/IEC 27001 was not perceived as high in terms of building trust and relationships between clients and suppliers. Certification alone did not deem sufficient by clients, indicating that additional measures may be necessary to establish trust in these external relationships.

4.1.6 Objective #6: to achieve clients' information security requirements

Several stakeholders (S1-S2, S5-S8, S10) highlighted the crucial objective of ensuring compliance with clients' information security requirements. S5, S6, and S8 expressed that an ISO/IEC 27001 certification serves as a suitable foundation for demonstrating how the organization conducts its information security practices. However, S1 and S7 noted that even though the organization holds ISO/IEC 27001 certification, they still encountered clients who annually requested detailed information on how they addressed their specific information security requirements. This implies that the certification alone may not fully satisfy certain clients' information security expectations, necessitating additional explanations and responses from the organization.

> "*Many of our big clients require us to have ISO/IEC 27001 certification, or at the very least, compliance with its standards. Annually, we receive a list of 200–300 questions from these clients, which we must respond to. Without the diligent efforts we have invested, we would not possess the capability to address these questions in a good and dignified manner*". (S7, Computer consulting company).

S7 provided additional insight into the rationale behind clients requesting suppliers to answer similar questions as those encountered during the certification process. The primary reason was for the client to assess the supplier's competence in information security. It served as an opportunity for the client to evaluate the supplier's capabilities and determine if they possessed the necessary resources to engage in a collaborative partnership. However, S1 found this process to be time-consuming and described it as follows:

> *"We are faced with numerous administrative tasks when we are required to answer an extensive set of questions, particularly when a client presents us with a list of 300 inquiries concerning our information security practices. This process is time-consuming and cannot be solely resolved by referring to our certification. It presents a challenge that demands a significant investment of time. We had anticipated that obtaining certification would alleviate such issues, but unfortunately, this has not been the case."* (S1, Software development company).

In summary, stakeholders acknowledged that ISO/IEC 27001 certification can serve as a valuable foundation in certain cases when initiating collaboration with clients as a supplier. However, they also expressed that, in many instances, the standard or certification alone was not sufficient to demonstrate their commitment to information security. This was primarily due to the perceived devaluation of the certification by some stakeholders and the fact that many clients now require compliance or certification according to alternative standards. As stakeholders required additional support from other resources and frameworks to effectively address information security, the output legitimacy of ISO/IEC 27001 was considered relatively low in achieving this specific objective.

4.1.7 Objective #7: to identify and maintain threats, risks, and vulnerabilities

All stakeholders (S1-S10) unanimously recognized the significance of continuously identifying, managing and monitoring information security threats, risks, and vulnerabilities. Given the rapid pace of technological advancements, S4 highlighted that organizations now engage in discussions around risks, information security, and threats with a distinct focus. This enabled them to ensure the implementation of appropriate security measures to mitigate potential risks. Furthermore, S9 emphasized that organizations had a responsibility, as outlined in ISO/IEC 27001, to proactively address risks and incidents, with the aim of enhancing their information

security practices. This reinforced the need for a continuous and proactive approach to maintaining and improving information security within organizations.

> *"The organizations are obligated and required by ISO/IEC 27001 to continuously work on and enhance their information security practices."* (S9, Investment and venture capital company).

In addition, S8 highlighted the importance of adopting a risk-based approach to information security. Organizations needed to identify areas where the risks were most significant and prioritized the implementation of appropriate security measures accordingly. By focusing resources on areas with higher risks, organizations can effectively mitigate potential threats and safeguard their information assets.

> *"It is not advisable to blindly adhere to the standard without considering the specific context of the organization. Therefore, it is crucial to align the information security efforts with the identified risks and implement the most suitable and effective measures accordingly."* (S8, Engineering company).

S1 observed that ISO/IEC 27001 provided security measures at a general level that were related to risk management. However, the stakeholder highlighted that the requirements for risk mitigation had evolved over time. With the increasing use of cloud services, S1 found the standard to be inadequate in guiding how to effectively address risks associated with cloud services. This sentiment was echoed by S6, who emphasized that the standard didn't cover all aspects of information security comprehensively, particularly in the realm of risk management. On the other hand, S2 and S3 noted that ISO/IEC 27001 included security measures that can be utilized for risk assessment purposes. However, the stakeholders pointed out the absence of appropriate measures to support stakeholders in monitoring the implementation and effectiveness of these measures. This gap in monitoring capabilities posed a challenge for stakeholders in ensuring ongoing effectiveness and improvement in their information security practices.

The stakeholders held differing views regarding the output legitimacy and effectiveness of ISO/IEC 27001 in addressing information security risks, threats, and vulnerabilities. S1, S6, and S7 expressed concerns about the standard's lack of comprehensive guidelines for effective risk management. They believed that ISO/IEC 27001 did not provide sufficient support in this area. On the other hand, stakeholders such as S2, S3, S9, and S10 had a more positive assessment of the standard's output legitimacy. They believed that ISO/IEC 27001 was a high-quality framework that included clear measures and requirements for organizations to consider when addressing information security risks. These stakeholders perceived the standard as providing valuable guidance in identifying and managing information security risks. Overall, there was a divergence of opinions among the stakeholders regarding the extent to which ISO/IEC 27001 adequately addresses the complexities of information security risk management.

4.1.8 Objective #8: to ensure technical security

All stakeholders (S1-S10) were unified in their efforts to ensure technical security within their organizations. However, they faced challenges regarding the output legitimacy of the ISO/IEC 27001 standard when it came to addressing new technical solutions. Many stakeholders found that the standard lacked clear guidelines in this area, making it difficult to effectively handle those emerging issues. They expressed that the technical environment was evolving at a faster pace than the standard, and as a result, ISO/IEC 27001 may not provide adequate support. For example, S1 highlighted that the standard did not address specific topics such as ransomware or phishing and their prevention measures. Similarly, S2 identified several gaps within the standard's coverage of technical security. These observations indicate that while ISO/IEC 27001 provides a general framework for information security management, it may not keep up with the rapid pace of technological advancements and emerging threats. As a result, stakeholders may need to supplement the standard with additional resources and frameworks to effectively address new technical challenges and ensure comprehensive technical security measures.

> *"When examining the individual controls outlined in the standard, it becomes evident that there are certain areas that lack adequate coverage. These gaps include session controls, session terminations, security and privacy attributes, absence of information-sharing provisions, insufficient data mining protection, and inadequate event logging. The list of deficiencies is rather extensive."* (S2, Computer consulting company).

S8 also highlighted the absence of technical measures for effectively managing cloud services. The stakeholder (S8) pointed out the lack of provisions for ensuring security in the utilization of IT, OT, and IoT systems, as well as the inadequate guidance on how organizations can safeguard and minimize vulnerabilities in their APIs.

> *"The current standard fails to address the crucial aspect of API protection, which is of significant concern for organizations, considering the prevalence of APIs in today's landscape. In my opinion, this highlights the challenge faced by the standard in keeping pace with rapid technological advancements."* (S8, Engineering company).

In contrast, S6 clarified that a common mistake within the industry was regarding the ISO/IEC 27001 standard purely as a technical standard. Instead, it emphasized the significance of recognizing that the standard encompasses administrative requirements that can assist organizations in customizing their information security practices according to their specific needs. This understanding highlights the importance of approaching the standard from a broader perspective.

In general, stakeholders had expressed concerns regarding the limited effectiveness of ISO/IEC 27001 in ensuring technical security. As mentioned earlier, many stakeholders felt that the standard lacked appropriate guidelines and security measures to adequately address technical challenges. Consequently, stakeholders believed that

to achieve effective outcomes in this regard, it was essential to implement and apply additional standards that could specifically address technology-related aspects. This suggests a need for a more comprehensive framework that can better address the dynamic nature of technical security requirements.

5 Discussion

This study focuses on investigating the output legitimacy of ISO/IEC 27001, based on eight identified information security objectives derived from the instrumental view of stakeholder theory. The results section examines the stakeholders' perspectives on which objectives they strive to achieve and their perception of ISO/IEC 27001's effectiveness in fulfilling these objectives. Overall, the study reveals a unanimous agreement among stakeholders that ISO/IEC 27001 possesses a high problem-solving capacity and output legitimacy in maintaining an ISMS. The predefined security measures outlined in the standard enable stakeholders to implement appropriate measures effectively. ISO/IEC 27001 provides a strategic and comprehensive approach to information security, offering guidelines for managing business risks throughout the implementation, establishment, operation, and monitoring phases of an ISMS (Susanto & Shobairah, 2016). The standard also emphasizes the importance of maintaining CIA of an organization's information assets through the application of a risk management process, thereby fostering trust among stakeholders in effectively managing risks (Aginsa et al. 2016). The findings of the study confirm the stakeholders' experiences, demonstrating that the standard operates as intended and possesses a high level of output legitimacy in maintaining an information security management system.

The application of the instrumental view of stakeholder theory proved valuable in identifying eight common information security objectives shared among stakeholders. By utilizing this perspective, the study effectively addressed the needs and interests related to information security, aiming to maximize the effectiveness of ISO/IEC 27001 from a stakeholder viewpoint (Welcomer 2002). The instrumental view seeks to uncover the relationships, or lack thereof, between stakeholder management and the achievement of performance objectives. In this particular study, the focus was on exploring the output legitimacy to fulfil the identified information security objectives utilizing the ISO/IEC 27001 standard. By adopting this perspective, the study aimed to gain insights into how well the standard aligned with stakeholder expectations and needs, and how it contributed to achieving the specified information security objectives.

Organizations commonly adopt ISO/IEC 27001 as a means to establish a systematic and reliable approach to addressing information security concerns and achieving specific objectives. By implementing this standard, organizations strive to ensure that their processes and practices for information security are consistently reviewed, maintained, and reproducible. Additionally, compliance with ISO/IEC 27001 enhances trust among both internal and external stakeholders, as organizations can provide evidence of effective security management (Ashenden, 2008). Nevertheless, it is important to note that achieving compliance with an ISMS standard is not always

a straightforward task. The requirements outlined in the standard can be intricate and challenging to comprehend. Organizations may face complexities in understanding and implementing the standards, requiring significant effort and expertise to navigate the intricacies successfully.

There appears to be a divergence of opinions among stakeholders regarding the adequacy of security measures related to risk management in ISO/IEC 27001. Some stakeholders expressed the view that the standard lacks the necessary measures to effectively address risk management and assessment. However, it is worth noting that clause 6.1 of ISO/IEC 27001, titled "*Actions to address risks and opportunities*", outlines the considerations organizations should take when working with information security risks. This clause guides stakeholders on how to proceed with risk assessment and treatment (SIS, 2017). Carvalho and Marques (2019) explain that by adhering to the standard, stakeholders gain the ability to evaluate and identify information security risks, enabling them to implement the appropriate security measures and procedures to safeguard the confidentiality, integrity, and availability of information. However, Alebrahim et al. (2014) state that while the ISO/IEC 27001 standard encompasses general concepts applicable to risk management, it does not specify the particular method stakeholders should utilize to identify threats and vulnerabilities—an essential aspect of risk assessment. Overall, there is a divergence in stakeholders' perspectives regarding the extent to which ISO/IEC 27001 addresses risk management measures. While the standard guides addressing risks and opportunities, stakeholders may require additional methods or approaches to effectively identify and assess risks in their specific organizational contexts.

Furthermore, stakeholders' perceived lack of guidance on compliance with laws and regulations decreases the output legitimacy of ISO/IEC 27001. Specifically, stakeholders feel that the standard does not provide sufficient direction on how to effectively adhere to legal requirements. However, by adopting a systematic approach provided by the standard, organizations can establish a framework to ensure compliance with regulations such as the General Data Protection Regulation (GDPR). Previous research supports this notion, showing that organizations compliant with ISO/IEC 27001 are better positioned to meet GDPR requirements (Lopes et al. 2019; Diamantopoulou et al. 2020). This raises the question of whether the interpretation and expertise of stakeholders in working with the standard, or the design of the standard itself, contribute to these perceptions. Additionally, the findings also indicate that there is a lack of experience among individuals in the field of information security. It is important to consider these factors when examining the challenges faced by stakeholders and the potential impact on the output legitimacy of ISO/IEC 27001.

6 Conclusion

The purpose of this study was to examine the output legitimacy of ISO/IEC 27001 from the perspective of stakeholders and assess its effectiveness in fulfilling their information security objectives. To achieve this, the study employed the instrumental view of stakeholder theory as a framework. By identifying and considering the eight information security objectives shared among stakeholders, the study aimed to

analyze the output legitimacy of ISO/IEC 27001 and evaluate how well the standard aligns with stakeholders' expectations.

The findings of the study indicate that the output legitimacy of ISO/IEC 27001 varies depending on the specific objectives that stakeholders aim to achieve. The standard demonstrates a high level of output legitimacy in relation to implementing, establishing, operating, and monitoring an ISMS. Stakeholders perceive that ISO/IEC 27001 effectively addresses these aspects of an ISMS and provides a solid foundation for maintaining information security within their organizations. One key strength of ISO/IEC 27001, as reported by stakeholders, is its flexibility and adaptability to meet the unique information security needs and requirements of different businesses. Moreover, ISO/IEC 27001 serves as a valuable reference framework for discussions and collaborations between organizations and stakeholders. By adhering to the standard, stakeholders can establish common ground and foster relationships based on trust and shared understanding of information security practices. In this way, ISO/IEC 27001 helps bridge gaps and enhance communication among different stakeholders and business units.

In conclusion, achieving a high level of output legitimacy for ISO/IEC 27001 requires stakeholders and users of the standard to possess the necessary knowledge and skills in both the standard itself and information security. It is crucial for organizations to invest in the training and development of their personnel to enhance their awareness and understanding of the standard, as well as information security principles. By increasing the knowledge and skills of standard users, organizations can empower their stakeholders to navigate their information security work more effectively and efficiently. This investment in education and awareness can contribute to better utilization of the standard and improved alignment with information security objectives. By fostering a knowledgeable and skilled workforce, organizations can enhance their ability to achieve their information security objectives with the support of the standard.

6.1 Limitations & future research

Given the adopted research approach and data collection scope, techniques and analysis, this study acknowledges certain limitations and highlights avenues for future research. It acknowledges that the identified information security objectives may not represent a complete set, as the research approach and data collection scope have inherent limitations. It is important to recognize that there may be additional security objectives that stakeholders strive to achieve but were not captured in this study. The study also notes the small size of the interviewed participant sample, suggesting that conducting more interviews could further strengthen the results. Increasing the sample size would provide a broader perspective and enhance the validity and generalizability of the findings. Future research is encouraged to build upon this study and explore the output legitimacy of ISO/IEC 27001 more extensively, taking into account the limitations of the current research. Additionally, as ISO/IEC 27001 is periodically updated, future studies can investigate the output legitimacy of the ISO/IEC 27001:2022 version. This would provide an opportunity to examine the similari-

ties and differences between the existing and updated versions of the standard, shedding light on the evolving nature of information security practices.

Acknowledgements The authors would like to thank Professor Fredrik Karlsson for his guidance during the study.

Funding Open access funding provided by Örebro University.

Declarations The authors have no competing interests, including financial and non-financial, to declare that are relevant to the content of this article.

References

Aginsa A, Edward IYM, 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. Int J Comput Appl 158(7):29–33

Aldya AP, Sutikno S, Rosmansyah Y (2019) Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. In: IOP conference, materials science and engineering 550:1–11

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

AlKalbani A, Deng H, Kam B, Zhang X (2017) Information Security compliance in organizations: an institutional perspective. Data Info Manage 1(2):104–114

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. Inf Manag 59(3):103623

Backhouse J, Hsu CW, Silva L (2006) Circuits of power in creating de jure standards: shaping an international information systems security standard. MIS Q, 413–438

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

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

Beckers K, Faßbender S, Heisel M, Küster JC, 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. Springer, Berlin, Heidelberg, p 14–21

Beckers, Fassbender S, Heisel M, Schmidt H (2012b) Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation. In: 2012 seventh international conference on availability, reliability and security, p. 242–248

Botzem S, Dobusch L (2012) Standardization cycles: a process perspective on the formation and diffusion of transnational standards. Organ Stud 33(5–6):737–762
Brugha R, Varvasovszky Z (2000) Stakeholder analysis: a review. Health Policy Plann 15(3):239–246
Bryman A (2016) Social research methods, 5th edn. Oxford, p 373–374.
Castka P, Prajogo D (2013) The effect of pressure from secondary stakeholders on the internalization of ISO 14001. J Clean Prod 47:245–252
Christou G (2018) The challenges of cybercrime governance in the European Union. Eur Politics Soc 19(3):355–375
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 J 33(7):76–105
De la Plaza Esteban IJ, Visseren-Hamakers W, de Jong (2014) The legitimacy of certification standards in climate change governance. Sustain Develop 22:420–432
Diamantopoulou V, Kalloniatis C, Lyvas C, Maliatsos K, Gay M, Kanatas A, Lambrinoudakis C (2020) Aligning the concepts of risk, security and privacy towards the design of secure intelligent transport systems. Computer Security. Springer, Cham, pp 170–184
Disterer G (2013) ISO/IEC 27000, 27001 and 27002 for information security management
Douvreleur P (2019) Challenges faced by legal counsels in Big Data and Cybersecurity Activity. Int'l In-House Counsel J 12:1
Eisenhardt KM, Graebner ME (2007) Theory building from cases: Opportunities and challenges. Acad Manag J 50(1):25–32
Fonseca-Herrera OA, Rojas AE, 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 RE (1984) Strategic management: a stakeholder approach. Pitman, Boston, MA
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 AA, Molok NNA, 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 (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/
Hyde KF (2000) Recognising deductive processes in qualitative research. *Qualitative market research: An international journal*
ISO (n.d.) (2022) -03-23 from https://www.iso.org/standards.html
Kallberg J (2012) The common criteria meets realpolitik: Trust, alliances, and potential betrayal. IEEE Secur Priv 10(4):50–53
Kica E, Bowman DM (2012) Regulation by means of standardization: key legitimacy issues of health and safety nanotechnology standards. Jurimetrics 53(1):11–56
Lopes IM, Guarda T, Oliveira P (2019) Implementation of ISO 27001 standards as GDPR compliance facilitator. J Inform Syst Eng Manage 4(2):1–8
Mansell SF (2013) Capitalism, corporations and the social contract: a critique of stakeholder theory. Cambridge University Press
Mayntz R (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. Bus Ethics Q 22(3):527–556
Mitchell R, Agle B, Wood D (1997) Toward a theory of stakeholder identification and salience: defining the principle of who and what really counts. Acad Manage Rev 22(4):853–858
Myers MD, Avison D (eds) (2002) Qualitative research in information systems: a reader. Sage
Nancylia M, Mudjtabar EK, 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). IEEE, p 1–5
Niemimaa E (2016) Crafting an information security policy: insights from an ethnographic study. In: The 37th international conference on information systems (ICIS 2016)
Orozova D, Kaloyanova K, Todorova M (2019) Introducing Information Security Concepts and Standards in Higher Education. TEM J 8(3):1017
Piper L (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

Rezakhani A, Hajebi A, Mohammadi N (2011) Standardization of all information security management systems. Int J Comput Appl 18(8):4–8

Richardson AJ, Eberlein B (2011) Legitimating transnational standard-setting: the case of the International Accounting Standards Board. J Bus Ethics 98(2):217–245

Santos-Olmo A, Sánchez LE, Caballero I, Camacho S, Fernandez-Medina E (2016) The importance of the security culture in SMEs as regards the correct management of the security of their assets. Future Internet 8(3):30

Scharpf FW (1999) Governing in Europe: effective and democratic? Oxford University Press, Oxford/New York

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

Schmidt VA (2013) Democracy and legitimacy in the European Union revisited: Input, output and 'throughput'. Polit Stud 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 NK, Dash PK (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. Decis Support Syst 92:68–78

Siponen M, Willison R (2009) Information security management standards: problems and solutions. Inf Manag 46(5):267–270

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

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 MN, Tuan YC (2011) Information security management system standards: a comparative study of the big five. Int J Electr Comput Sci IJECSIJENS 11(5):23–29

Susanto H, Almunawar MN, Tuan YC (2012) Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. Int J Eng Technol 2(1):67–75

Swedish Civil Contingencies Agency - MSB (2020) Myndigheten för samhällsskydd och beredskaps författningssamling. Föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6

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/

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/

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. Stud Inf Control 24(2):201–210

Tjirare DJ, Shava FB (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 DC (2011) Information security standards. J Mob Embedded Distrib Syst 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

Von Solms R (1999) Information security management: why standards are important. Inform Manage Comput Secur.

Wagner E, Mainardes, Alves H, Raposo M (2012) A model for stakeholder classification and stakeholder relationships. Manag Decis 50(10):1861–1879

Welcomer SA (2002) Firm-stakeholder networks: organizational response to external influence and organizational philosophy. Bus Soc 41(2):251–257

Werle R, Iversen EJ (2006) Promoting legitimacy in technical standardization. Sci Technol Innov Stud 2(1):19–39

Yaokumah W, Brown S (2014) An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. J Law Govern 9(2):51–66

Authors and Affiliations

Yasmin Kamil[1] · Sofia Lund[1] · M Sirajul Islam[1,2]

✉ M Sirajul Islam
sirajul.islam@oru.se; sislam@alfaisal.edu

Yasmin Kamil
yasminakamil@gmail.com

Sofia Lund
sofia.v.lund@telia.com

[1] Örebro University School of Business, Örebro, Sweden

[2] Alfaisal University, Riyadh, Saudi Arabia