Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security management in ICT and non-ICT sector companies: A preventive innovation perspective

Mona Mirtsch[a,b,*], *Knut Blind*[b,c], *Claudia Koch*[a,b], *Gabriele Dudek*[a]

[a] *Bundesanstalt für Materialforschung und -prüfung (Federal Institute for Materials Research and-Testing — BAM), Berlin, Germany*

[b] *Technische Universität Berlin, Berlin, Germany*

[c] *Fraunhofer Institute of Systems and Innovation Research (ISI), Karlsruhe, Germany*

ARTICLE INFO

Article history:
Received 29 October 2020
Revised 18 June 2021
Accepted 21 June 2021
Available online 26 June 2021

Keywords:
Information Security
ISO/IEC 27001
Management system standard
Certification
Information security management system
Preventive innovation
Resource-based-view
Institutional theory

ABSTRACT

Despite the growing dependence of companies on information technology and the increasingly negative impact of security incidents worldwide, there is little research on the management of information security at the company level. This paper seeks to expand knowledge on the implementation of an information security management system based on the widely used international standard ISO/IEC 27001. We present motives, experienced impacts, and obstacles related to ISO/IEC 27001 implementation using data from a survey of 125 ISO/IEC 27001 certified companies in Germany. Since adoption rates vary between ICT and non-ICT sector companies, we highlight sector-related variations. We classify the adoption of this standard as a preventive organizational innovation and apply Structural Equation Modeling to unearth explanations for the comparatively low adoption of this management system standard among companies outside the ICT sector. We, therefore, derive recommendations for policymakers, standardization, and certification bodies to foster its diffusion.

1. Introduction

Companies increasingly rely on information and communication technology (ICT) to run their businesses, organize production, provide services or communicate internally and with customers (Eurostat 2020). With the accelerating digitalization and spread of the Internet of Things, it is not only ICT sector companies that have become increasingly vulnerable to cyber-attacks. For example, a study from Germany shows that 70% of the companies surveyed experienced digital attacks in 2019, compared to only 43% in 2017 (Berg and Niemeier, 2019). This study, furthermore, estimates the financial damage caused by production downtime or blackmail and loss of image at more than 100 billion Euros per year (Berg and Niemeier, 2019). As demonstrated, for instance, by the WannaCry ransomware attack (Mohurle and Patil, 2017), the Mirai botnet (Antonakakis et al., 2017), or the attack on Ukraine's power grid control system (Das and Gündüz, 2020), cyber-related threats affect businesses, individuals, and society alike.

* Corresponding author.
E-mail address: mona.mirtsch@bam.de (M. Mirtsch).

https://doi.org/10.1016/j.cose.2021.102383

Given these damages and the growing number of information security incidents in organizations worldwide (Accenture and Ponemon Institute 2019; Federal Office for Information Security (BSI), 2019, ENISA, 2019), information security and cybersecurity (on conceptual differences see Von Solms and Van Niekerk (2013)) are increasingly moving into the focus of policymakers. In the European Union, e.g., a Cybersecurity Strategy (European Commission, 2013), as well as several Directives and Regulations on related issues have been implemented in recent years. These explicitly highlight the vital role of standards and certifications in helping companies demonstrate compliance with information security requirements [1].

Against the backdrop of growing economic and regulatory pressures, companies increasingly need to take appropriate measures to protect their information assets and make this issue part of their strategic management (Saint-Germain, 2005; Peng, 2018). An information security management system (ISMS) aims to protect information assets and provides a systematic approach to managing risks. It, therefore, supports companies to meet their own information security objectives, as well as those of their customers, and to comply with legal information security-related requirements (ISO/IEC 27000:2018).

ISO/IEC 27001 as an international standard for such an ISMS "has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system" (ISO/IEC 27001:2013. ISO/IEC 27001 is referred to as the leading international standard for information security management (Susanto et al., 2011; Disterer, 2013; Culot et al., 2021). However, adoption of this standardized ISMS did not occur at the expected rate in its early years (Fomin et al., 2008; Tunçalp, 2014), and annual surveys by ISO itself of the number of valid certificates worldwide (ISO, 2020) indicate that this issue remains. ISO/IEC 27001 ranks third worldwide among the most frequently used management system standards, with 36,362 valid certificates at 68,930 sites[2], behind ISO 9001 for quality management (ranked first with nearly 900,000 valid certificates) and ISO 14001 for environmental management (ranked second with over 300,000 valid certificates) (ISO, 2020). In view of the rising relevance of information security, these absolute numbers show well the yet slow diffusion despite the high ranking. Sector data from the ISO survey of certified organizations worldwide (ISO, 2020) also reveal that ISO/IEC 27001 is adopted primarily by companies belonging to the ICT sector.

Given the growing relevance of information security, this development calls for a closer empirical exploration of the motives for adopting an ISMS according to ISO/IEC 27001, the impacts that can be realized, but also the obstacles. Previous studies on ISO/IEC 27001 have already analyzed these aspects. However, we aim to provide a more comprehensive view by analyzing the relationship between motives, realized impacts, and obstacles to the ISO/IEC 27001 adoption, as well as the overall benefit perceived by ISO/IEC 27001 certified companies. Therefore, by applying structural equation modeling, our study extends existing studies that have investigated each construct separately (van Wessel and de Vries, 2013; AbuSaad et al., 2011; Alshitri and Abanumy, 2014; Skopak and Sakanovic, 2016; Longras et al., 2018; Svoboda and Horalek, 2018) without statistically analyzing relationships. Previous studies on ISO/IEC 27001 adoption, furthermore, did not provide any empirically grounded answers to the prevalent question of the low level of adoption outside the ICT sector. Our study, therefore, addresses this research gap by explicitly differentiating between ICT and non-ICT sector companies in the analyses.

However, estimating structural equation models to address these objectives requires an accordant sufficient sample size (Hair et al., 2019) which is not trivial for several reasons: For one thing, it is difficult to gather information on a larger scale at the firm level because the adoption rate is still low. Another challenge is that companies are often unwilling to disclose their information security-related activities (Kotulic and Clark, 2004) and refuse to publish data on security-related events (Crossler et al., 2013). Indeed, the existing scientific studies on adopting ISO/IEC 27001 are characterized by small samples (maximum of 25) of certified companies (AbuSaad et al., 2011; Alshitri and Abanumy, 2014; Longras et al., 2018; Svoboda and Horalek, 2018). Therefore, from an empirical perspective, research on managing information security at the organizational level using ISO/IEC 27001 is scarce, mostly conceptual (Fomin et al., 2008; Barlette and Fomin, 2010; Tunçalp, 2014) or case-study based (van Wessel and de Vries, 2013). Accordingly, there is a need for research focusing on ISO/IEC 27001 certified firms, despite the still small number of certified firms available (Hsu et al., 2016; Culot et al., 2021).

To explore the adoption of ISO/IEC 27001 based on a large, comprehensive sample that allows for robust insights, we apply a novel, web-mining-based approach to compile our sample (Mirtsch et al., 2020a). With this, our study is the largest so far, with 125 ISO/IEC 27001 certified companies in Germany surveyed. This country is interesting to study as it, with 1,175 valid certificates, ranks sixth worldwide and third in the European Union (ISO, 2020).

Given the need for more research in information security management, which covers both empirical groundwork and theoretical development (Hsu et al., 2012; Culot et al., 2021), this paper draws on previous studies of information security management and research on other management system standards. Building on the classification of the implementa-

[1] Directive on the Safety of Network and Information Systems (NIS Directive (EU) 2016/1148) adopted in 2016, e.g., within Article 16 (Security requirements and incident notification) states that "digital service providers need to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems" taking into account "compliance with international standards."; The General EU Data Protection Regulation (GDPR - Regulation (EU) 2016/679) in force since May 2018, e.g., within Article 42 (Certification) encourages the "establishment of data protection certification mechanisms and of data protection seals and marks"; Cybersecurity Act (Regulation (EU) 2019/881) adopted in June 2019 states within Title III (European Cybersecurity Certification Framework) that a European cybersecurity certification scheme should include "references to the international, European or national standards applied in the evaluation […] (Article 54).

[2] defined as a permanent location where an organization carries out work or services

tion of ISO/IEC 27001 as an innovation (Hsu et al., 2012), this paper refers to the Resource-Based View (RBV) and institutional theory. It, furthermore, applies the concept of "preventive innovations" (Rogers, 1988; Rogers, 2002) and considers the adoption of ISO/IEC 27001 as an organizational innovation aimed at avoiding undesirable consequences in the future (Mirtsch et al., 2020b). This theoretical underpinning of our results helps, in particular, to gain a more profound understanding of the low adoption rate of ISO/IEC 27001 outside the ICT sector and to propose measures to promote the adoption of this management system standard.

The remainder of this paper is structured as follows. After we outline previous research on this management system standard, we present our conceptual model and derive hypotheses. In the following section, we present our methodology and the results of our company survey. Following the discussion, in which we also derive practical recommendations and contributions to theory, we conclude with limitations and promising avenues for future research.

2. Theoretical background

2.1. *Previous empirical studies on the adoption of ISO/IEC 27001*

Previous empirical studies specifically on ISO/IEC 27001 encounter on who adopts this standard (Mirtsch et al., 2020a); why (van Wessel and de Vries, 2013; AbuSaad et al., 2011; Alshitri and Abanumy, 2014; Skopak and Sakanovic, 2016; Longras et al., 2018; Svoboda and Horalek, 2018), and how companies benefit from its adoption, e.g., financially (Hsu et al., 2016; Tejay and Shoraka, 2011; Deane et al., 2019).

Mirtsch et al. (2020a) used Web Mining of German firm websites to identify ISO/IEC 27001 certified firms and then analyze antecedents for ISO/IEC 27001 certifications. They apply the Technology-Organization-Environment (TOE) framework of DePietro et al. (1990) and find that firm size, ICT sector affiliation, and product innovativeness drive ISO/IEC 27001 certification. Such certification, they note, is frequently coupled with certification of other management system standards such as ISO 9001, ISO 14001, and ISO 50001 (Mirtsch et al., 2020a).

Based upon the findings of six case studies from the U.K. and the Netherlands, van Wessel and de Vries (2013) revealed that companies adopt ISO/IEC 27001 and ISO/IEC 27002 for internal and external reasons. Certified firms benefit financially, e.g., through resulting new business opportunities, and non-financially, e.g., by realizing a reduced risk level for their company. The authors conclude that if companies provide essential services, the adoption of ISO/IEC 27001 and ISO/IEC 27002 also "contributes to a well-functioning society" (van Wessel and de Vries, 2013).

The few previous empirical studies that have surveyed firms that have adopted the standard focus mainly on the motives, impacts, and obstacles encountered by implementing ISO/IEC 27001. Table 1 provides an overview of the country, sample size, total valid certificates in these countries, and the different foci of these studies.

The results of these studies show that ISO/IEC 27001 certified firms are mainly driven, first, by prevention objectives, i.e., increasing information security and reducing the risk of security breaches, and second, by marketing objectives, such as achieving market access, enhancing corporate image, or increasing sales (AbuSaad et al., 2011; Longras et al., 2018). The firms surveyed encounter difficulties related to the time and cost efforts of certification and human resources (HR) obstacles as well as lack of top management support (Alshitri and Abanumy, 2014; Longras et al., 2018; Dionysiou et al., 2015). Recent company-level surveys increasingly link the adoption of ISO/IEC 27001 with ensuring compliance with regulations related to the General Data Protection Regulation (GDPR) (Longras et al., 2018) or national cybersecurity laws (Svoboda and Horalek, 2018), or more generally as a “ticket to the European market” (Dionysiou et al., 2015).

Tejay and Shoraka (2011) used an event-study approach to investigate stock market reactions following the announcement of ISO/IEC 27001 certification using a sample of 32 U.S. companies. However, they found no statistically significant effect and, therefore, concluded that firms did not gain significant financial value from obtaining ISO/IEC 27001 certification.

Similarly, Hsu et al., 2016 compared 25 ISO/IEC 27001 certified and control firms in Europe and the United States and found no empirical evidence that ISO/IEC 27001 certification has a positive effect on the stock market or in financial terms. Therefore, they conclude that ISO/IEC 27001, unlike ISO 9001, plays a defensive role to "prevent loss through management" and that ISO/IEC 27001 helps "meeting the requirement," instead of [gaining] a competitive advantage" Hsu et al., 2016.

In contrast to the two previously mentioned studies, Deane et al. (2019) found evidence of positive abnormal stock market reactions. Based on public announcements of ISO/IEC 27001 certification of 111 U.S. listed firms, this effect was even more pronounced for firms active in the manufacturing sector or providing financial services and firms having only recently been certified (Deane et al., 2019).

In the most theoretically and statistically advanced firm-level empirical study, Hsu et al. (2012) analyzed factors that impact the adoption (operationalized for their study as the intention to adopt) and assimilation (operationalized as practice being embedded in the organization) of information security management in organizations. From a theoretical perspective, Hsu et al. (2012) classify information security management as an administrative innovation and apply institutional theory. They surveyed 140 Korean information security managers using a partial least square (PLS) structural equation model (SEM). The authors find that economically based considerations and organizational capabilities moderate institutional pressures (emanating from regulators or peer firms) as determinants. They conclude with a recommendation for regulation as a coercive pressure, among other measures, as normative pressures are still less prevalent in information security management adoption decisions (Hsu et al., 2012).

The synthesis of our literature review shows that previous studies identify drivers for ISO/IEC 27001 certification in terms of firm characteristics and confirm that its adoption is mainly in the ICT sector (Mirtsch et al., 2020a). This is in line with data from the annual ISO (2020) survey. However, no reasons are given for the low level of adoption outside the ICT sector. Previous company-level studies focusing exclusively on ISO/IEC 27001 only provide an item list on constructs such as mo-

Table 1 – Previous surveys of ISO/IEC 27001 adoption.

Country	Sample (certified)	# cert. country	Focus of the study	Main research finding	Reference
Saudi-Arabia	8 (8)	13[3]	Motives, barriers, impact, lessons learned	Meeting customers' requirements no major motivation for certification	AbuSaad et al., 2011
Saudi-Arabia	34 (10)	46[3]	Barriers to implementation	HR management issues the biggest barrier for ISO/IEC 27001 implementation	Alshitri and Abanumy, 2014
Cyprus	152 (0)	2[3]	Reasons for non-adoption	Major reason for the non-adoption is that benefits cannot be quantified and measured in financial terms	Dionysiou et al., 2015
Bosnia and Herzegovina	20 (1)	10[3]	Familiarity with standard, planned adoption	Most surveyed firms are familiar with ISO/IEC 27001 and consider adopting it in the future, but adoption is still very low	Skopak and Sakanovic, 2016
Portugal	25 (25)	52[3]	Barriers, costs, co-occurrences with other standards	Despite high cost and time investment, respondents perceive ISO/IEC 27001 certification to increase firms' competitiveness	Longras et al., 2018
Czech Republic	33 (21)	463[4]	Motives, relation to national cybersecurity law	The relatively high adoption rate of ISO/IEC 27001 in the Czech Republic can be attributed to recently adopted national Cybersecurity law	Svoboda and Horalek, 2018

[3] At the time of the survey according to authors of the respective study
[4] According to ISO (2020) for the year 2017

tives, barriers, and benefits, which form the basis for our study. However, they are all characterized by very small sample sizes (with a maximum of 25 ISO/IEC 27001 certified organizations) that do not allow for multivariate statistical analysis, do not systematically build on each other, and are not theoretically grounded.

Summarizing the state of the art of research on ISO/IEC 27001 adoption, the need for a survey with a larger number of ISO/IEC 27001 certified companies becomes apparent. This allows multivariate analyses and broader generalization of the results, as well as differentiation in terms of sector affiliation (subgroups for ICT and non-ICT companies). Second, our literature review shows the need for a company-level survey of ISO/IEC 27001 adoption with a sound theoretical framing on which future studies could build, including a conceptualization of benefit beyond (immediate) financial gains.

2.2. *Theoretical framing*

To explore the adoption of the ISMS based on ISO/IEC 27001, we consider it as an organizational innovation and build on theories and frameworks from innovation research. The study by Hsu et al. (2012) paved the way for this by taking a major step in defining information security management as an administrative (as opposed to a technical) innovation. This is in line with Armbruster et al. (2008) and (Blind, 2019), who categorize the adoption of ISO management system standards such as ISO 9001 and ISO 14001 as organizational innovations. Similar to administrative innovations (Fernandes Rodrigues Alves et al., 2018), organizational innovations are defined as a "new organisational method in business practices, workplace organization or external relations" (OECD/Eurostat, 2005). We argue that this applies to ISO/IEC 27001, which encompasses technology, processes, and people (Siponen and Willison, 2009), and further refer to Nelson and Winter (1982), who emphasize the importance of routines to the success of companies.

Therefore, to analyze the motives and benefits of ISO/IEC 27001 adoption, we rely on two lines of theoretical underpinnings: innovation adoption theories (van Oorschot et al., 2018), and management theories for analyzing voluntary management system standards (Tuczek et al., 2018) with a focus on ISO/IEC 27001 (Culot et al., 2021).

Culot et al. (2021) build on the work of Nair and Prajogo (2009) and distinguish between functionalist and institutionalist, which we underpin with the theoretical views of the RBV and institutional theory. The latter helps explain why organizations become similar over time, a process also known as isomorphism (DiMaggio & Powell, 1983). In particular, organizations face institutional pressures that can be coercive, normative, and mimetic (Guler et al., 2002) in the context of institutional theory.

According to the RBV, firms strive to determine and make use of their strategic resources to gain 'sustained competitive advantage' (Barney, 1991). Routine procedures laid down in management system standards help companies build internal capabilities (Prajogo, 2011; Darnall, 2006), with information security becoming a strategic resource (Bakar et al., 2015), encompassing both tangible (e.g., related to technical investments) and intangible (e.g., in terms of employee awareness) aspects (Weishäupl et al., 2015).

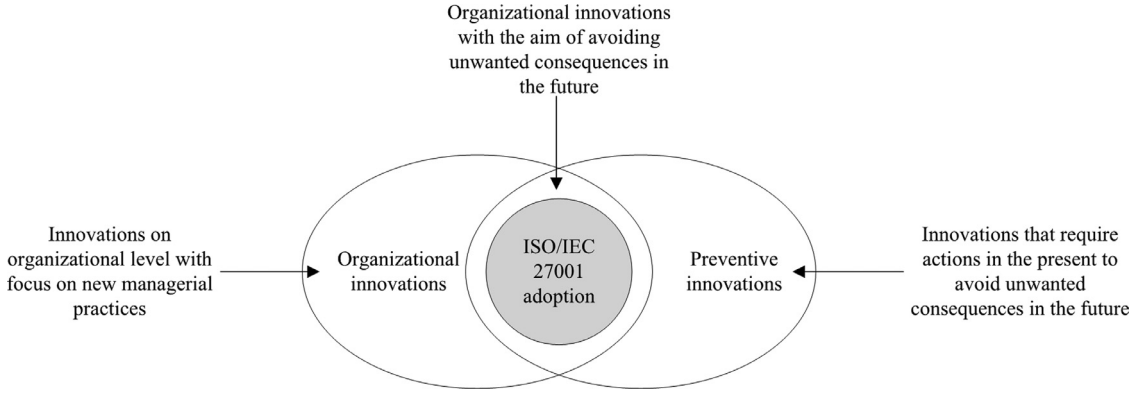

Fig. 1 – Adoption of ISO/IEC 27001 as preventive organizational innovation based on Rogers (2002)

However, we argue that neither institutional theory nor the RBV allow us to comprehensively explain why firms adopt a management system according to ISO/IEC 27001, whose financial benefits have not been evidenced in most previous studies (Hsu et al., 2016; Tejay and Shoraka, 2011). This underlines the need to view the adoption of ISO/IEC 27001 from a different perspective with a focus on the prevention aspect. To do so, we build on the work of Mirtsch et al., 2020b, who use the Diffusion of Innovation theory (DoI), considering a specific type of innovation that Rogers (1988) terms *preventive innovations*. These are defined as "new ideas that require action at one point in time in order to avoid unwanted consequences at some future time" (Rogers, 2002). Examples, according to Rogers (2003), include the use of automotive seat belts, health screening, vaccinations, quitting smoking, and prevention measures related to disasters such as hurricanes. The concept of preventive innovations has been applied primarily in the context of health studies (Overstreet et al., 2013), such as HIV protection (Bertrand, 2004), vaccinations (D'Souza et al., 2013), or cancer screening (Hahm et al., 2011).

According to Rogers (2003), the perceived relative advantage is the main predictor for the adoption rate of innovations. However, in the case of preventive innovations, the adopting unit benefits only later or maybe even not at all if the undesirable event does not occur. The rewards are, therefore, often intangible (Rogers, 2002). This type of innovation often diffuses more slowly than non-preventive innovations, also due to the **K**nowledge, **A**ttitude, and **P**ractice (KAP) gap: positive attitudes or values do not correlate with actual behavior, which may call for intervention to close this gap (Rogers, 2003). Rogers (2002) suggests several measures of how to increase the adoption of preventive innovations. These include emphasizing relative advantage, utilizing champions to promote adoption of this innovation, changing the norm of the system through peer support, and activating peer networks (Rogers, 2002).

We, therefore, follow Mirtsch et al., 2020b in classifying the adoption of ISO/IEC 27001 as a preventive innovation, as its adoption is not associated with immediate benefits but the potential return of its adoption (preventing something from happening) is rather uncertain. Therefore, we aim to specifically investigate the benefits associated with the prevention effects of ISO/IEC 27001 adoption as a preventive organizational innovation, as shown in Fig. 1.

2.3. *Conceptual model and hypotheses*

Our research aim is to explore why companies choose to adopt ISO/IEC 27001 (motives), the impacts they experience, the obstacles they encounter, and how these aspects relate to how adopting companies perceive the overall benefit of ISO/IEC 27001 adoption.

Ray et al. (2004) acknowledge, especially when applying the RBV for empirical studies, the main challenge lies in the choice of the dependent variable to measure competitive advantage, as overall firm performance can lead to misleading results, as this variable is oftentimes too aggregated and may neglect potentials of business activities that have not yet been fully realized (Ray et al., 2004). We argue this is especially true if the impact is not easily financially measurable, presumably due to its preventive nature (Hsu et al., 2016; Fomin et al., 2008). Therefore, we follow Ray et al. (2004), who propose to consider the effectiveness of business processes instead of firm performance and opt for overall benefit perception as the main dependent variable.

To investigate the experienced impacts on the overall benefit perception, we analyze the role of the initial motives, which we categorize as either functional or institutional following Culot et al. (2021). From a functionalist view, referring to RBV (Barney, 1991), companies can be motivated by achieving a higher level of information security (Susanto et al., 2012; van Wessel and de Vries, 2013; Culot et al., 2021) or increasing the efficiency in information security-related processes (Annarelli et al., 2020; Crowder, 2013; Abu Bakar et al., 2017; Culot et al., 2021). Firms may, therefore, adopt ISO/IEC 27001 to increase their internal capabilities, whereas information security may be considered a valuable resource for gaining sustained competitive advantage (Weishäupl et al., 2015).

From an institutional theory perspective, adopting firms might be motivated by regulatory pressures either exerted directly, e.g., in the case of energy providers in Germany which need to present a certificate that they implemented an ISMS according to ISO/IEC 27001 (Bundesnetzagentur, 2018) or to comply more efficiently with legal requirements, e.g., of the GDPR (Diamantopoulou et al., 2020). Second, companies may

strive to improve their image and be perceived as trustworthy partner (Culot et al., 2019; van Wessel and de Vries, 2013) or to gain market access (Ţigănoaia, 2015), such as in the case of public tenders requiring ISO/IEC 27001 certification (Culot et al., 2021). This can also be attributed to the signaling effect of certificates (Viscusi, 1978), which helps overcome information asymmetries, one cause for market failures, according to Akerlof (1978). Finally, firms may be subject to isomorphic pressures and strive to mimic competitors that already have ISO/IEC 27001 certification (Culot et al., 2021; Deane et al., 2019).

We expect that these motivations will likely differ in importance, which we aim to analyze, also considering sector-specific factors. We, furthermore, assume that there is a positive relationship between the initial motives and how the overall benefit of ISO/IEC 27001 implementation is perceived by adopting companies leading to the following hypothesis:

H1: *Initial motives to adopt ISO/IEC 27001 positively affect the benefit perception after implementation of ISO/IEC 27001.*

Regarding the experienced impacts of ISO/IEC 27001 adoption, Culot et al. (2021) differentiate between outcomes that are specific to the scope of the standard (related to risk prevention and higher business continuity) and other performance dimensions. In this sense, the adoption of ISO/IEC 27001 can lead to more efficient processes helping them to increase their information security level (Annarelli et al., 2020; van Wessel and de Vries, 2013). This may also lead to enhanced relationships with stakeholders (van Wessel and de Vries, 2013) or lower insurance costs (Susanto et al., 2012; Saint-Germain, 2005).

Previous studies on management systems have shown that experienced impacts are often related to initial motives (Terziovski and Power, 2007; Terziovski et al., 1997; Boiral and Roy, 2007; Nair and Prajogo, 2009). For instance, organizations that are functionally motivated are more likely to experience related internal impacts, whereas organizations that are institutionally motivated are more likely to achieve external impacts (Castka and Corbett, 2013). We argue that it is legitimate to also assume this relationship for the adoption of ISO/IEC 27001 and, therefore, hypothesize:

H2: *Initial motives to adopt ISO/IEC 27001 positively affect the corresponding experienced impacts after implementation of ISO/IEC 27001.*

Regardless of whether companies have functionalist or institutionalist motives, it is reasonable to assume that they adopt the management system only if the experienced impacts exceed the costs (Iatridis and Kesidou, 2018). Therefore, we argue that the overall benefit perception will depend on both the impacts experienced and the barriers encountered.

First, we expect that firms experience impacts from ISO/IEC 27001 adoption, which will affect their overall benefit perception. Second, organizations often face various difficulties when adopting an ISMS (Culot et al., 2021), which makes adoption more challenging and may even outweigh the benefits obtained (Lo and Chang, 2007). It is reasonable to suggest that companies that experience low impacts from ISO/IEC 27001 implementation may consider the adoption decision as a bad investment, which may even lead to the decision not to renew the certificate (Ferreira and Cândido, 2021). Obstacles in management system standard adoption in general often relate to economic resources, the complexity of the content of the standard, and organizational difficulties that include low employee motivation, lack of leadership, and resistance to change (Casadesu et al., 2001; Marimon and Casadesús, 2017). For ISO/IEC 27001 specifically, the high complexity of the standard related to the scope determination and the high number of controls are the main difficulty (Culot et al., 2021; Diesch et al., 2020). Low top management commitment (van Wessel and de Vries, 2013), need for support of external consultants, and time and cost investment can also be hurdles when implementing ISO/IEC 27001, affecting the overall benefit perception. Taking both aspects into account for the overall benefit perception of ISO/IEC 27001 adoption, we, therefore, hypothesize:

H3: *The experienced impacts of adopting ISO/IEC 27001 affect the overall benefit perception positively.*

and

H4: *Encountered obstacles affect the overall benefit perceived of ISO/IEC 27001 adoption negatively.*

Finally, we argue that besides these direct effects, there might be indirect effects that influence the overall benefit perception of ISO/IEC 27001 adoption. Therefore, we expect that experienced impacts might mediate motives when it comes to how companies evaluate the overall benefit of ISO/IEC 27001 adoption, leading to our following fifth hypothesis:

H5: *The effect of the initial motives on the perception of the overall benefits is mediated by the corresponding impacts experienced.*

Fig. 2 shows our conceptual model with the hypotheses.

3. Methodology

3.1. *Development of the questionnaire*

To get an overview of relevant aspects related to the adoption of ISO/IEC 27001 from a managerial perspective, we build on the limited previous empirical literature on ISO/IEC 27001. Following the advice of Marimon and Casadesús (2017) regarding research on those management system standards for which there is little empirical literature to date, we also borrow from the literature on other management system standards such as ISO 9001 for quality (Claver and Tari, 2008; Martinez-Costa et al., 2009; Nair and Prajogo, 2009), ISO 14001 for environmental (Alberti et al., 2000; Alvarez-Garcia and del RioRama, 2016; Bellesi et al., 2005; Murmura et al., 2018; Daddi et al., 2016), and ISO 50001 for energy management (Sinha et al., 2015). Through an in-depth literature review of various management system standards, we identified motives, obstacles encountered, and benefits that are the focus of management system adoption research (Castka and Corbett, 2013).

Afterwards, we conducted ten interviews with various stakeholders: seven companies certified to ISO/IEC 27001 from several sectors, ranging from the ICT sector to energy suppliers, two certification bodies, and one representative of the

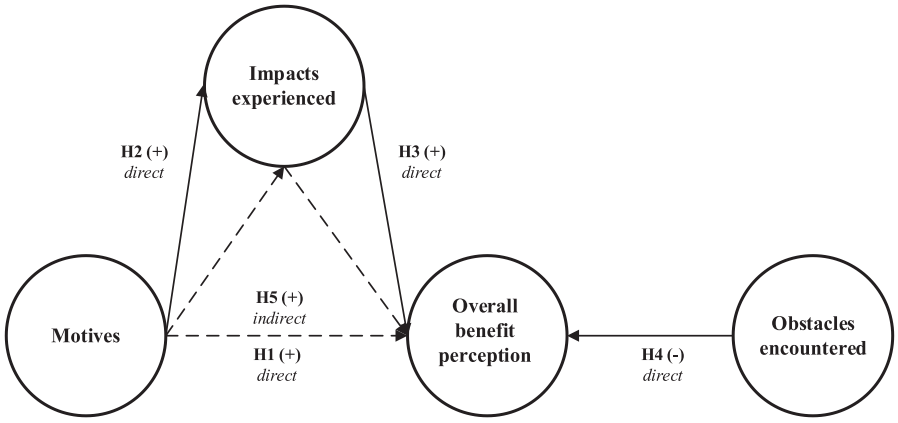

Fig. 2 – Conceptual model and research hypotheses.

Table 2 – Questionnaire sections.

Section	Content
1. Company data	Industry affiliation (NACE) Size (employees, sales) Innovativeness
2. Use of other management system standards	Adoption of other management system standards
3. Adoption of ISO/IEC 27001	Duration of ISO/IEC 27001 certification Scope of ISO/IEC 27001 certification Motives Experienced impacts Overall benefit perception Obstacles

German authority BSI (the Federal Office for Information Security). These interviews helped us validate whether our item list was adequate or whether we had overlooked important aspects.

Table A.1 in the annex depicts the relevant questions asked, items used within this study, and whether they were either derived from previous studies or our interviews. Table A.2 in the annex links the items with the theories we applied in our conceptual model (Section 2.3), including the short titles of the items which we use in the following. For example, in terms of institutional theory, we focus on coercive and mimetic forces but leave aside normative forces, as Hsu et al. (2012) revealed that they do not play a significant role in the adoption of information security management.

We conducted a pre-test with five ISO/IEC 27001 certified companies of different sizes and industries. For this, we used the cognitive technique of the "Think-Aloud Method" (Collins, 2003). The questions were designed with either yes/no responses or answers using a 5-point Likert scale, with 1 for "strongly disagree" and 5 for "strongly agree". Table 2 shows the different sections of the questionnaire that are relevant for this study.

3.2. *Survey*

We conducted a company-level survey and derived the sample building on the web-mining-based methodology of Kinne and Axenbeck (2018), which is used in Mirtsch et al. (2020a) to identify 806 German companies that either claim to be ISO/IEC 27001 certified on their firm websites or are listed in a publicly accessible certification database.

We contacted these 806 certified companies by phone between January and March 2020 to motivate the person responsible for information security to participate in the online survey. As a result, we were able to send 195 personalized links. We received 125 valid responses from ISO/IEC 27001 certified firms, which equals a response rate of 15.5% considering the 806 companies we contacted.

3.3. *Sample description*

Table 3 describes the sample in terms of further company characteristics as well as the scope of certification, the time period since initial certification, whether these companies are certified to another management system standard, and whether certification is legally required under the German IT Security Act. To be able to explore reasons for the low level of ISO/IEC 27001 adoption, particularly among companies outside the ICT sector, we distinguish between ICT and non-ICT sector companies.

ISO (2020) provides a sectoral breakdown for roughly one-third of all internationally valid ISO/IEC 27001 certificates, which is used to control our survey sample for possible sampling bias in terms of sector affiliation (Table 4). The comparison shows that the sector split of our German survey sample resembles the total global population to a great extent. German public utility firms (i.e., electricity, gas, and water supply) are over-represented compared to the overall population of ISO/IEC 27001 certificates. It is noteworthy, however, that German companies (such as energy suppliers) that fall under the European NIS Directive have to provide an ISO/IEC 27001 certificate as of 2018 (Bundesnetzagentur 2016).

Table 3 – Sample description and characteristics of ISO/IEC 27001 certified companies.

	All	ICT Sector	Non-ICT Sector		All	ICT Sector	Non-ICT Sector
Size (in # of employees)				*Certification scope*			
1-9	9	5	4	Full organization	54	32	22
10-49	43	32	11	IT	61	40	21
50-249	40	21	19	Other	10	1	9
250-499	11	7	4				
500-999	9	5	4	*Time since first certification*			
over 1000	13	3	10	1-3 years	56	30	26
				4-9 years	56	33	23
Turnover (in Mio €)				Over 10 years	13	10	3
0-2	18	8	10				
2-10	32	23	9	*Also certified to*			
10-50	25	15	10	ISO 9001	68	38	30
over 50	28	18	10	ISO 14001	12	4	8
No answer	22	9	13	ISO 50001	11	5	6
Innovative				*IT and Security Act*			
Yes	89	53	36	Required	17	4	13
No	36	20	16	Not required	108	69	39

Table 4 – Comparison of the survey sample with the total ISO/IEC 27001 population (ISO, 2020).

Sector affiliation	Survey sample (%) n=125	Total population with the sector (%) n=15,882
ICT	58.7%	53.9%
Scientific and other services	12.8%	12.6%
Electricity, gas, water supply	8.8%	1.5%
Financial services	4.8%	3.5%
Transportation and storage	4.0%	6.2%

3.4. *Statistical analysis*

Our statistical analysis comprises three steps.

Descriptive statistics on motives, experienced impacts, obstacles encountered, and perceived benefits are presented first. These are then analyzed to rank the variables according to their relevance and to test for their differences between ICT sector and non-ICT sector companies.

Second, we conduct an exploratory factor analysis using Stata version 15.0 (StataCorp., 2017) to reduce the number of items by determining the underlying latent factors for our following analysis. The number of factors is determined by scree plots (Cattell, 1966) and the Kaiser K1 rule (Kaiser, 1960). We also consider the variance of the proportions explained by the resultant number of factors and use the Kaiser-Meyer-Olkin (KMO) measure to assess sampling adequacy (Kaiser and Rice, 1974).

Third, we use exploratory path analysis to analyze the relationships between factors on motives, experienced impacts, and perceived benefits, including obstacles related to ISO/IEC 27001 adoption. Structural equation modeling (SEM) can be used to analyze relationships between observed and latent variables (Hair et al., 2019). We apply partial least squares (PLS)-SEM, originally developed by Wold (1966) and Lohmöller (1989), instead of covariance-based (CB)-SEM, because it does not impose distributional assumptions (such as normal distribution) on the data, is specific to exploratory research, and is applicable for smaller sample sizes (Hair Jr et al., 2017a, Hair et al., 2019). PLS-SEM combines elements of factor analysis with ordinary least squares (OLS) regression, and comprises a measurement (outer) and a structural (inner) model (Hair et al., 2019).

Applying SmartPLS Version 3 software (Ringle et al., 2015), we use the factors derived from the four exploratory factor analyses to set up a path model. To identify differences, we estimate the entire sample and the two subgroups, ICT sector, and non-ICT sector, separately. We highlight significant paths by performing a bootstrap resampling procedure with a resampling of 5,000 iterations with a significance level of 0.10 (as recommended in exploratory research), using the setting of the casewise deletion for missing values, as recommended by Hair Jr et al. (2017a). To identify a significant difference between the two subgroups (considering ICT sector affiliation as a moderating variable), we perform a multi-group analysis followed by a mediation analysis.

4. Results

4.1. *Ranking of motives, impacts, overall benefit perception, and obstacles*

Table 5 presents the results of the survey – with the mean values ranked by relevance, the standard deviation (SD), and the number of valid responses (Obs.), highlighting significant differences between the two subgroups.

The *motive* 'prevent incidents' is ranked highest by all organizations when adopting ISO/IEC 27001. This prioritization reflects the main objective of adopting ISO/IEC 27001, which

Table 5 – Motives, impacts, overall benefit perception, and obstacles.

	All			ICT Sector			Non-ICT Sector		
	Mean	SD	Obs.	Mean	SD	Obs.	Mean	SD	Obs.
Motives									
Prevent incidents	4.09	1.11	123	4.07	1.02	71	4.12	1.23	52
Demand from the customer* **	3.94	1.32	121	4.37	0.92	73	3.29	1.56	48
Improve internal processes	3.92	1.11	123	3.97	1.06	72	3.84	1.17	51
Increase legal certainty	3.91	1.24	121	3.81	1.30	69	4.04	1.15	52
Increase employee awareness	3.90	1.15	122	3.93	1.15	70	3.87	1.17	52
Promote domestic market access* **	3.69	1.40	117	4.09	1.09	69	3.13	1.59	48
Marketing/image reasons **	3.63	1.16	121	3.82	1.06	71	3.36	1.26	50
Meet top management objectives	3.10	1.44	118	3.21	1.38	70	2.94	1.52	48
Be (one of the) first to be certified	2.78	1.59	114	2.88	1.58	65	2.65	1.61	49
Competitors are certified*	2.65	1.35	118	2.83	1.26	69	2.41	1.44	49
Promote market access abroad*	2.46	1.48	112	2.68	1.49	66	2.13	1.42	46
Response to a specific incident	1.34	0.82	119	1.37	0.84	70	1.31	0.80	49
Experienced impacts									
Increased employee awareness	4.35	0.72	124	4.38	0.72	72	4.31	0.73	52
Increased information security	4.24	0.78	123	4.23	0.80	71	4.27	0.77	52
Reduced risk for incidents	4.03	0.88	120	3.97	0.94	71	4.12	0.78	49
Image improvement **	3.93	0.96	124	4.11	0.85	72	3.67	1.04	52
Higher legal certainty	3.69	1.13	118	3.62	1.07	68	3.78	1.22	50
Certificate-related sales increase* **	3.11	1.35	120	3.51	1.17	71	2.53	1.39	49
Reduced incident related internal costs*	2.56	1.15	118	2.71	1.13	70	2.33	1.15	48
Lower insurance premiums	1.84	0.99	96	1.85	0.98	54	1.83	1.01	42
Overall benefit perception									
Implementation is a good investment **	4.15	0.96	123	4.31	0.87	72	3.92	1.04	51
Additional cert. is a good investment	3.96	0.99	108	4.03	0.93	63	3.87	1.08	45
Obstacles									
High time investment	4.16	0.80	124	4.15	0.79	73	4.18	0.82	51
External consulting needed	3.80	1.32	119	3.66	1.40	70	4.00	1.19	49
High costs	3.55	0.96	120	3.60	0.87	70	3.48	1.07	50
Complexity of standard content	3.30	1.07	121	3.21	1.07	71	3.42	1.07	50
Lack of internal expertise	2.51	1.17	123	2.58	1.21	72	2.41	1.12	51
Difficult scope determination	2.47	1.25	123	2.47	1.23	72	2.47	1.29	51
Low employee motivation	2.35	0.97	123	2.30	0.90	71	2.42	1.07	52
Few consulting services available	2.19	1.07	113	2.23	1.11	64	2.12	1.03	49
Lack of top management commitment	1.70	1.03	123	1.67	1.07	72	1.75	0.98	51

Asterisks indicate the level of significance: * $p < 0.10$; ** $p < 0.05$; *** $p < 0.01$.

is to increase the company's information security. The high ranking of 'demand from the customer' by ICT sector companies and 'increase legal certainty', especially by non-ICT sector companies, also indicate institutional pressures arising from customers and government. Less relevant for both subgroups is an implementation in 'response to a specific incident'.

Comparing the motives of the ICT with those of the non-ICT sector companies, five significant differences are prevalent: The motives 'demand from the customer', 'promote market access' (domestic and abroad), 'competitors are certified', and 'marketing/image reasons' were rated higher by the representatives of the ICT sector companies than by those of non-ICT sector companies.

The highest-ranking *experienced impact* for the entire sample was 'increased employee awareness', followed by the other preventive impacts 'increased information security' for the company as well as 'reduced risk for incidents', which mirrors the motives surveyed. The three finance-related impacts ('certificate-related sales increase', 'reduced incident-related internal costs', and 'lower insurance premiums') ranked comparably low. Comparing the results of both subgroups, 'certificate-related sales increases', and 'image improvement' were rated higher by representatives of companies in the ICT sector than by companies outside the ICT sector.

Overall, the adoption of ISO/IEC 27001 is perceived as a good investment, while the additional certification is rated slightly lower. Moreover, ICT sector companies value the overall benefit of ISO/IEC 27001 implementations significantly higher than companies outside the ICT sector.

The highest-ranked *obstacles* to adopting ISO/IEC 27001 are time and high costs, as well as 'external consulting needed'. However, comparatively low scores for 'few consulting services available' are found. 'Lack of top management commitment' is rated lowest, as are difficulties in the HR area with 'low employee motivation'. It is worth noting that there are no significant differences in the obstacles encountered for companies within and outside the ICT sector.

4.2. *Results of the exploratory factor analyses*

In the following, we present the results of our four exploratory factor analyses.

Table 6 – Factor analysis results on motives.

Motive variables	Mean	SD	Factor 1 Prevention	Factor 2 Market access	Factor 3 Signaling
Increase legal certainty	3.90	1.24	**0.51**	-0.08	0.20
Improve internal processes	3.91	1.10	**0.87**	0.08	0.15
Increase employee awareness	3.89	1.15	**0.90**	0.03	-0.03
Meet top management objectives	3.10	1.43	**0.62**	0.12	0.30
Prevent incidents	4.08	1.11	**0.84**	0.01	0.02
Demand from the customer	3.95	1.32	-0.07	**0.84**	-0.09
Promote domestic market access	3.69	1.39	0.30	**0.74**	0.26
Promote market access abroad	2.44	1.48	-0.03	**0.74**	0.15
Be (one of the) first to be certified	2.78	1.58	-0.03	-0.02	**0.91**
Marketing/image reasons	3.62	1.16	0.27	0.28	**0.74**
Proportion of variance explained			*0.31*	*0.19*	*0.16*
Cum. proportion of variance explained			*0.31*	*0.50*	*0.66*

Table 7 – Factor analysis results on experienced impacts.

Experienced Impact variables	Mean	SD	Factor 1 Prevention-related impact	Factor 2 Market-related impact
Increased information security	4.24	0.78	**0.78**	-0.03
Increased employee awareness	4.35	0.72	**0.75**	0.29
Reduced risk for incidents	4.04	0.88	**0.76**	-0.06
Certificate-related sales increase	3.11	1.34	0.07	**0.82**
Image improvement	3.93	0.96	0.02	**0.86**
Proportion of variance explained			0.35	0.30
Cum. proportion of variance explained			0.35	0.65

Regarding the *motives* for adopting ISO/IEC 27001, following Kaiser's (1960) eigenvalue-greater-than-one rule and the Cattell (1966) scree plot, two items were dropped in the final model, namely 'competitors are certified' and in 'response to a specific incident'. Since both of these factors rank low (Table 5), we argue it is legitimate to drop them in the final model.

Therefore, three factors emerge from the first-factor analysis, which explain about 66% of the total variance, with a KMO value of 0.74. We coin the first factor *prevention* because the items that load the highest relate to preventing information security breaches and increasing the company's level of information security. We term the items that relate to meeting customer requirements and promoting market access (both domestic and abroad) as *market access* because they refer to criteria related to the ability to participate in the respective market. Finally, the items 'be (one of the) first to be certified' and 'marketing/image reasons', both of which load high on the third factor, we coin as *signaling* (Table 6).

In the same approach, regarding the *experienced impacts* of the adoption of ISO/IEC 27001, two items were dropped in the final model, namely 'reduced incident-related internal costs' and 'lower insurance premiums'. Since both ranked low (Table 5), we argue it was justified to drop them in the final model.

Thus, the second factor analysis on *experienced impacts* reveals two factors: First, the *prevention-related impact*, which includes items related to the core objective of this management system standard, namely, increasing the company's information security level, employees' awareness, and the reduced risk for incidents. Second, *market-related impact*, which includes items on (certificate-related) sales increase and image improvement (Table 7). These two factors explain 65% of the variance with a KMO value of 0.59, which is low but close to 0.60 as the minimum threshold for the KMO value.

The third factor analysis on the *overall benefit perception* comprises two items that explain 85% of the variance and includes both items on the overall perception of whether the adoption and the respective additional certification is a good investment for the adopting organization (Table 8).

Finally, from the fourth factor analysis on *obstacles* to the adoption of ISO/IEC 27001, three factors emerge that explain 59% of the variance with a KMO of 0.67. The first factor, *operational investment*, is linked to the time and cost required to invest, alongside the complexity of the standard content and the difficulties encountered in defining the scope of certification. The second factor, *human resources*, is related to difficulties associated with personnel, including low motivation, lack of top management commitment, and lack of qualified IT personnel. The third factor, *consulting need*, is an additional factor related to the need for consulting services and whether only a few consulting services are available on the market (Table 9). No items were omitted within the third and fourth factor

Table 8 – Factor analysis results on overall benefit perception.

Perceived benefit variables	Mean	SD	Factor 1 Overall benefit
Implementation is a good investment	4.15	0.95	0.92
Additional certification is a good investment	3.97	0.99	0.92
Proportion of variance explained			0.85
Cum. proportion of variance explained			0.85

Table 9 – Factor analysis results on obstacles.

Obstacles variables	Mean	SD	Factor 1 Operational investment	Factor 2 Human resources	Factor 3 Consulting need
High time investment	4.17	0.80	**0.64**	-0.01	0.21
Complexity of standard content	3.30	1.07	**0.71**	0.23	0.05
Difficult scope determination	2.48	1.25	**0.74**	0.28	-0.02
High costs	3.55	0.96	**0.68**	-0.21	0.34
Lack of top management commitment	1.69	1.03	0.06	**0.75**	0.02
Lack of internal expertise	2.52	1.17	0.08	**0.70**	0.42
Low employee motivation	2.34	0.98	0.11	**0.79**	-0.16
External consulting needed	3.81	1.32	0.09	0.11	**0.80**
Few consulting services available	2.20	1.08	0.17	-0.09	**0.70**
Proportion of variance explained			0.22	0.21	0.16
Cum. proportion of variance explained			0.22	0.43	0.59

analyses on overall benefit perception and obstacles encountered.

4.3. *Results of the structural equation modeling*

The factors that emerged from the factor analyses helped to set up the SEM model, whereas we only use reflective (instead of formative) indicators (Hair et al., 2019). After evaluating these, some items were excluded according to the recommendations of Hair Jr et al. (2017b) or extracted as single items following the evaluation of the separate factor analyses of both subgroups. 'Lack of top management commitment' was omitted from the HR obstacle factor due to its low loadings (below the threshold of 0.4) and 'high time investment' from the operational investment obstacle factor (due to the average variance extracted (AVE) value below 0.5). Including these two items as single items did not reveal significant path coefficients, so we dropped both items from the model completely. Taking into account that 'higher legal certainty' was not part of the preventive motive factor for non-ICT sector companies and considering content validity (Hair Jr et al., 2017a), this item was excluded from the first factor and the item 'legal compliance impact' was added as a single item due to the significant effect (path coefficient) within the final structural model.

Table 10 summarizes the evaluation of the measurement model. The results indicate adequate convergent reliability with its loadings, AVE above 0.5, internal consistency reliability with composite reliability values (CR) above 0.7, and discriminant validity with heterotrait-monotrait (HTMT) ratios below 0.9 following the guidelines on thresholds of Hair et al. (2019).

As shown in Table 11, the adjusted R^2 values for the complete sample of all endogenous variables reveal that the model explains 31.6% of the variance in preventive impact, 46% in the legal compliance impact, 47.1% in market impact, and 45.9% in overall benefit perception, with slight variations between the two subgroups.

Regarding the assessment of the structural model, the variance inflation factors (VIF) are all between 1 and 2 except for three motive items with values between 3 and 4, namely 'improve internal processes', 'increase employee awareness' and 'prevent incidents'. However, since they are below 5, indicating that there are no critical issues with multicollinearity, this is still acceptable (Hair Jr et al., 2017a). The VIF values are shown in the correlation matrix in Table A.3 in the Appendix.

The Standardized Root Mean Square Residual (SRMR) is 0.104, which is above the threshold specified for CB-SEM based models (<0.08); however, unlike CB-SEM based models, PLS-SEM models do not provide adequate model fit values (Hair et al., 2019).

The results of the structural model analysis are shown in Fig. 3, with significant paths highlighted by asterisks.

The results show that only 'legal compliance motives' have a significant and positive effect on the *overall benefit perception* with only partial support for our first hypothesis. Most *motives*, however, have a significant and positive effect on their related *impacts*. Therefore, our second hypothesis is mostly supported. The only exception is the case of non-ICT companies: The motive 'market access' has no significant effect on the experienced 'market impact'.

Table 10 – Assessment of the measurement model.

	Latent Variables	Indicators	Convergent validity		Internal consistency reliability	Discriminant validity
			Loadings	AVE	CR	HTMT<0.9
Motives	Preventive motives (PM)	Improve internal processes	0.923	0.743	0.919	Yes
		Increase employee awareness	0.724			
		Meet top management objectives	0.686			
		Prevent incidents	0.902			
	Legal compliance motives (LM)	Higher legal certainty	Single Item	1	1.000	N/A
	Market access motives (MAM)	Demand from the customer	0.791	0.622	0.831	Yes
		Promote domestic market access	0.847			
		Promote market access abroad	0.724			
	Signaling motives (SM)	Be (one of the) first to be certified	0.752	0.737	0.847	Yes
		Marketing/image reasons	0.953			
Impacts	Preventive impact (PI)	Increased information security	0.550	0.567	0.792	Yes
		Increased employee awareness	0.793			
		Reduced risk for incidents	0.878			
	Legal compliance impact (LI)	Higher legal certainty	Single Item	1	1.000	N/A
	Market impact (MI)	Certificate-related sales increase	0.853	0.737	0.831	Yes
		Image improvement	0.833			
Overall benefit perception	Overall benefit perception (BP)	Implementation is a good investment	0.901	0.797	0.887	Yes
		Additional certification is a good investment	0.884			
Obstacles	Operational investment obstacles (OIO)	High costs	0.671	0.599	0.816	Yes
		Complexity of standard content	0.840			
		Difficult scope determination	0.802			
	HR obstacles (HRO)	Lack of internal expertise	0.645	0.661	0.790	Yes
		Low employee motivation	0.951			
	Consulting need obstacles (CNO)	External consulting needed	0.703	0.664	0.795	Yes
		Few consulting services available	0.913			

Table 11 – R^2 adjusted values.

R^2 adjusted	Complete sample	ICT companies	Non-ICT companies
Preventive impact (PI)	0.316	0.362	0.279
Legal compliance impact (LI)	0.460	0.326	0.625
Market impact (MI)	0.471	0.362	0.445
Overall benefit perception (BP)	0.459	0.618	0.561

As far as the *overall benefit perception* is concerned regarding the *impacts*, only the 'preventive impacts' have a significant and positive effect – yet, only for ICT companies. Since the other experienced impact factors, i.e., 'legal compliance' and 'market impact', have no significant effect, our third hypothesis is only partially supported.

Regarding the influence of encountered *obstacles* on the *overall benefit perception* of ISO/IEC 27001, 'operational investment obstacles' have a significantly negative effect for both ICT and non-ICT sector companies. Since there is no significant effect of the other two observed obstacle factors, 'HR' and 'consulting need', our fourth hypothesis is again only partially supported.

Besides these direct effects, we have also analyzed *indirect effects* between the constructs: The results show that – while there was no direct effect of the preventive motives on the overall benefits perception as shown above – the preventive impacts may mediate the relationship between the preventive motives and the overall benefit perception. The result of the mediation analysis is shown in Figure 4.

The results reveal that there is full mediation taking place for ICT sector companies: There is no significant effect of preventive motives on the overall benefit perception, while preventive motives have a significant positive effect on the preventive impact, which in turn has a significant positive effect on the overall benefit perception. In contrast, no mediation

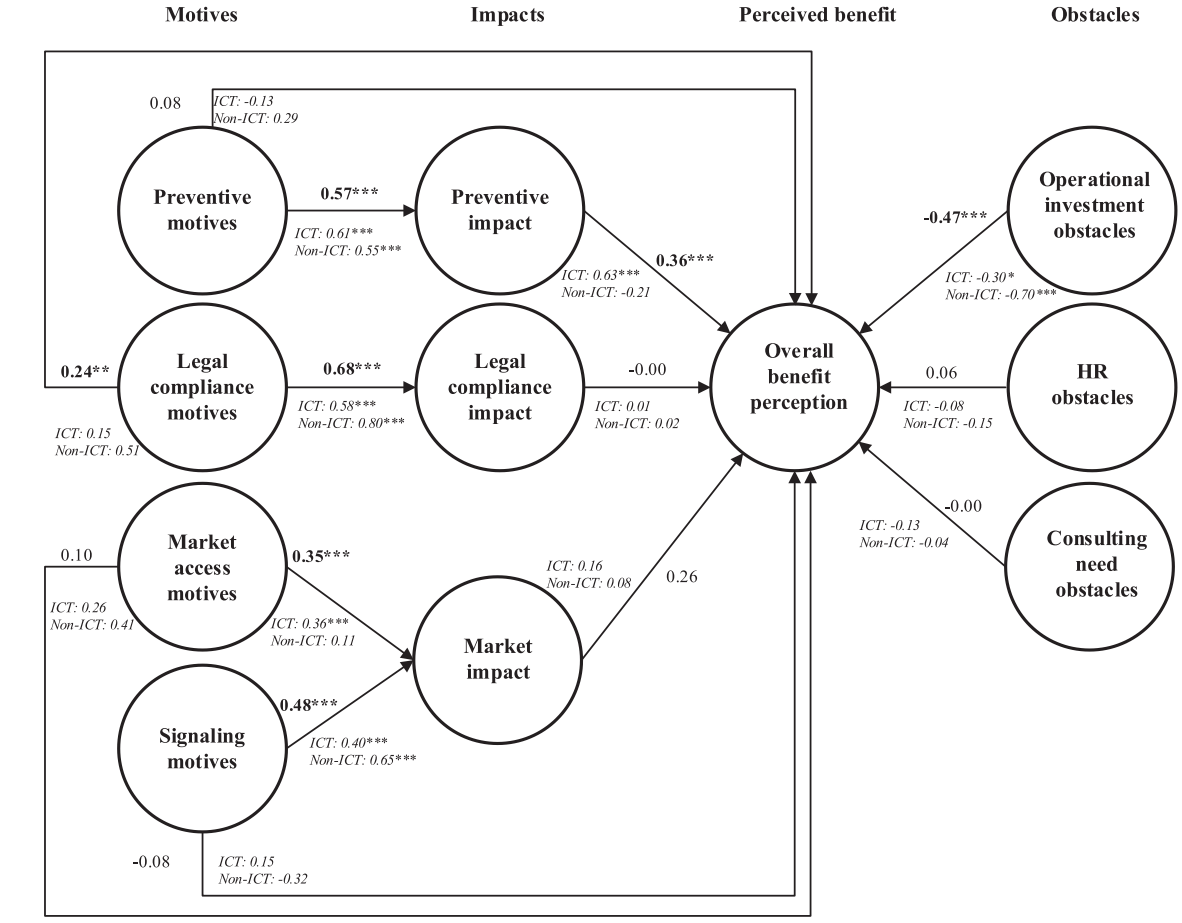

Fig. 3 – Results of the PLS-SEM with coefficients and p-values for the complete sample (n = 125) and subgroups ICT sector (n = 73) and Non-ICT sector companies (n = 52)

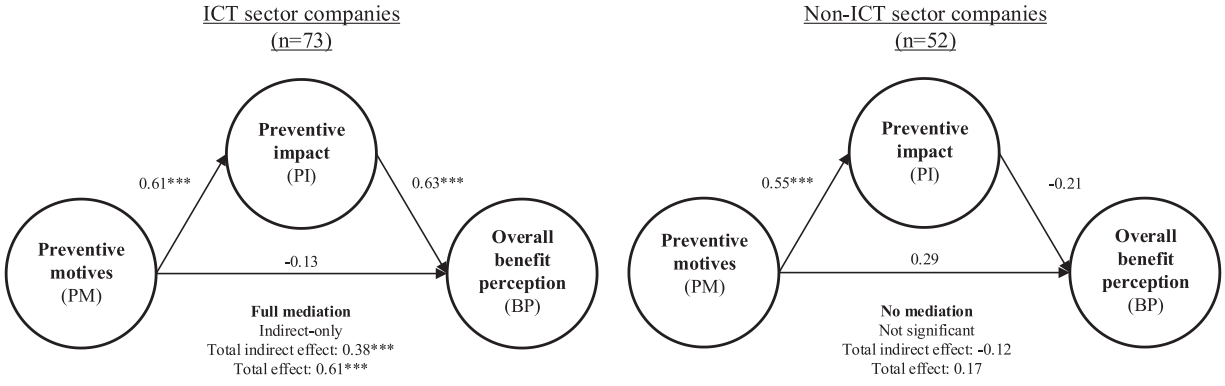

Fig. 4 – Results of the mediation analysis with coefficients and p-values.

takes place for non-ICT sector companies. Despite a significant positive effect of the preventive motives on the preventive impact, there is no significant effect for either the preventive motives or the preventive impact on the overall benefit perception (Figure 4).

This finding is supported by a multi-group analysis (Hair et al., 2019), which confirms a significant difference between ICT and non-ICT sector companies considering the path between preventive impact and overall benefit perception, with a coefficient difference of 0.81 (p-value<0.05). Therefore, our fifth hypothesis is only partially supported.

Table 12 summarizes the instances in which our hypotheses were supported, partially supported, or not supported.

Table 12 – Summary of findings.

			Full sample	ICT sector	Non-ICT sector
H1:	H1a	PM→BP	Not supported	Not supported	Not supported
Motives→	H1b	LM→BP	Supported	Not supported	Not supported
Benefit perception	H1c	MM→BP	Not supported	Not supported	Not supported
Partially supported	H1d	SM→BP	Not supported	Not supported	Not supported
H2:	H2a	PM→PI	Supported	Supported	Supported
Motives→ Impacts	H2b	LM→LI	Supported	Supported	Supported
Mostly supported	H2c	MM→MI	Supported	Supported	Not supported
	H2d	SM→MI	Supported	Supported	Supported
H3:	H3a	PI→BP	Supported	Supported	Not supported
Impacts→	H3b	LI→BP	Not supported	Not supported	Not supported
Benefit Perception	H3c	MI→BP	Not supported	Not supported	Not supported
Partially supported					
H4:	H4a	OIO→BP	Supported	Supported	Supported
Obstacles→	H4b	HRO→BP	Not supported	Not supported	Not supported
Benefit perception	H4c	CNO→BP	Not supported	Not supported	Not supported
Partially supported					
H5:	H5a	PM→PI→BP	Supported	Supported	Not supported
Motives→Impacts→Benefit perception	H5b	LM→LI→BP	Not supported	Not supported	Not supported
Partially supported	H5c	MM→MI→BP	Not supported	Not supported	Not supported
	H5d	SM→MI→BP	Not supported	Not supported	Not supported

PM = Preventive motives, LM=Legal motives, MM=Market access motives, SM=Signaling motives.
PI = Preventive impacts, LI=Legal impacts, MI=Market impacts, BP = Benefit perception.
OIO = Operational investment obstacles, HRO=HR obstacles, CNO = Consulting need obstacles.

5. Discussion and implications

5.1. *Discussion of the findings*

The findings of our study allow insights into companies' adoption of ISO/IEC 27001 by exploring their motives, experienced impacts, perceived overall benefits, and obstacles encountered during implementation, including their relationships.

As far as the *motives* are concerned, ISO/IEC 27001 certified organizations have various reasons for adopting this organizational innovation which differ in relevance. The main motive is to increase the company's information security level. This finding is consistent with other studies on management systems, according to which companies are mostly driven by achieving the core objectives of the management system, which in the case of ISO/IEC 27001 is to safeguard information security. However, when implementing management systems, companies are also driven by other reasons related to either economic or institutional motives (Castka and Corbett, 2013), though these often also depend on the sector affiliation. In the case of ISO 9001, for example, Singh et al. (2006) found that manufacturing firms are more economically driven in terms of reducing costs, while service providers are motivated by meeting external expectations, which can arise either from customers or government authorities. The findings of our study confirm such sector differences: ICT sector companies are significantly more motivated by customer requirements, gaining (especially domestic) market access and improving their image compared with ISO/IEC 27001 certified companies outside the ICT sector. This finding indicates that ICT companies also seek certification to yield institutional pressures and for signaling reasons.

Companies outside the ICT sector are apparently under less institutional pressure from customers and see less need for signaling. However, for this subgroup, in light of increasing regulation, ensuring legal compliance is a primary driver for ISO/IEC 27001 certifications. The analysis of the direct effects (H1) also shows that only this motive has a significant positive effect on the *overall benefit perception*, which is comparable high for non-ICT sector companies. This confirms the findings of previous studies on ISO/IEC 27001 that regulatory initiatives are increasingly triggering firms to adopt an ISMS (Longras et al., 2018; Svoboda and Horalek, 2018). In the case of Germany, this may be, on the one hand, the German IT Security Act, which represents the national transposition of the European NIS Directive. On the other hand, companies have to comply with the requirements of the General Data Protection Regulation (GDPR), where ISO/IEC 27001 helps to be GDPR compliant, as shown by Diamantopoulou et al. (2020). However, unlike for quality and environmental management, information security management seems not yet institutionalized, as our analyses indicate: In line with findings from (Uwizeyemungu and Poba-Nzaou, 2015), mimetic behavior, i.e., seeking certification because competitors are already certified, plays a minor role for both subgroups.

Our analysis shows a direct relationship between *motives* and the accordant *experienced impacts* of ISO/IEC 27001 certification (H2), confirming findings from previous management systems research (Terziovski and Power, 2007; Terziovski et al., 1997; Boiral and Roy, 2007; Nair and Prajogo, 2009). The actual major *impacts experienced* through the adoption

of ISO/IEC 27001 are related to prevention, particularly regarding the increased information security awareness among the companies' employees supporting our classification of ISO/IEC 27001 as preventive innovation. Most previous studies have not evidenced financial benefits from the ISMS adoption (Hsu et al., 2016, Tejay and Shoraka, 2011). Likewise, our analyses show that economic impacts in the form of increased sales or cost reductions are experienced less by the adopting companies – and even less so for companies outside the ICT sector. This is in contrast to most studies on ISO 9001 that show increased productivity or financial performance for adopters (Wiengarten et al., 2017).

Our study further explored the effects that the *experienced impacts* have on the *overall benefit perception* of ISO/IEC 27001 certification (H3). Out of the three impact categories – legal compliance, market impact, and preventive impact – only the latter has a significantly positive effect on the overall benefit perception. However, this is only the case for ICT sector companies.

Considering the RBV, safeguarding a firm's information security needs to be considered a strategic resource. Many of the ISO/IEC 27001 certified companies not only use ICT services but also offer them (Mirtsch et al., 2020a) and, therefore, safeguarding information security in terms of RBV is a valuable resource when providing data-related services to customers.

However, the fact that perceived legal compliance and market impacts do not positively impact the *overall benefit perception*, i.e., that our hypothesis H3 is only partially supported, can be attributed to the fact that these impacts were rated lower than the prevention-related impacts which ranked highest for certified companies.

To sum up, prevention is the focus of ISO/IEC 27001 implementation and certification, while other potential impacts take a back seat. This underlines the nature of an ISMS as preventive innovation, aiming to lower the probability of unwanted future events (Rogers, 2002). Such unwanted events (in the sense of security breaches) and accordant financial and market consequences, which are prevented by the ISMS and thus never occur (hence, e.g., money or customers are not lost due to successfully avoided incidents), make adopters unaware of such benefits.

As the benefits should exceed costs to motivate the implementation of ISO/IEC 27001, our analyses also encountered the *obstacles* faced and their impact on the overall benefit perception. The latter is indeed negatively affected by the necessary operational investment. This negative effect is even comparably greater for non-ICT than for ICT sector companies. In line with other management system standards, the adoption of and also the intended certification to ISO/IEC 27001 is a costly endeavor for companies. Unlike other management systems, however, this investment does not pay off immediately for companies certified to ISO/IEC 27001. Surprisingly, HR resources and necessary external consulting do not negatively impact the overall benefit perception (H5 only partially supported). Yet, this can be explained, again, by considering that the related items were not rated very high by the respondents in the first place. Thus, it seems that the need for knowledgeable and motivated personnel or external consultancy does not outweigh potential benefits.

5.2. *Practical implications*

The findings of our study provide possible explanations to the prevalent question as to why the adoption of ISO/IEC 27001 is so low among companies outside the ICT sector (Fomin et al., 2008; Tunçalp, 2014, Uwizeyemungu and Poba-Nzaou, 2015) and allow to derive practical implications.

Our results indicate a potential lack of immediate economic benefits from adopting ISO/IEC 27001, paired with a low level of institutional pressures arising from customers, especially for companies outside the ICT sector. Since companies of all sizes and sectors can fall victim to attacks (Berg and Niemeier, 2019), a potential need to actively promote the adoption of this management system standard becomes apparent, especially since information security constitutes a public good (Moore, 2010).

Following the recommendations of Rogers (2002) on how to promote the diffusion of preventive innovations, the results of this study, therefore, help to derive suitable measures to promote the adoption of ISO/IEC 27001.

First, regulators, standards developing organizations (SDOs), and certification bodies could raise the awareness of the benefits of ISO/IEC 27001, for example, through case studies of organizations that have successfully adopted this management system standard. This, on the one hand, could motivate companies to adopt this standard and, on the other hand, might cause stakeholders along the supply chain to appreciate the adoption of ISO/IEC 27001 by their partners. This, in turn, increases the market impact also outside the ICT sector, where our analyses still show low consciousness. Second, governmental agencies could actively address the relevant obstacles identified in our study to increase the overall perception of the benefits of adopting ISO/IEC 27001. Our results show that operational obstacles (comprising cost and complexity) have a significant negative effect on the benefit perception. Proposed measures could address the costs associated with the adoption of and certification against ISO/IEC 27001, for example, by providing incentives (as in the example of ISO 50001 for energy management, for which tax incentives are given (Sinha et al., 2015)).

In terms of how to deal with the standard complexity, companies could be encouraged to share best practices in the implementation of and intended certification to ISO/IEC 27001. In addition, SDOs could publish specific practical guidance documents to help, in particular, SMEs apply the ISO/IEC 27000 series, as proposed by the European Commission in its current rolling plan for ICT standardization (European Commission, 2021). These proposed measures could promote the adoption of ISO/IEC 27001, especially outside the ICT sector. From an institutional perspective, this could hopefully set off bandwagons (Uwizeyemungu and Poba-Nzaou, 2015), so these measures are only needed for a limited time.

Given the strong link between the motive of legal compliance and the overall perception of benefits, policymakers could also intervene in a regulatory manner by making the adoption of an ISMS in accordance with ISO/IEC 27001 mandatory. This is already the case in Germany for certain providers of critical infrastructures under the IT Security Act and could be extended to other groups of companies under the yet-to-

be-developed cybersecurity certification schemes under the EU Cybersecurity Act, following a risk-based approach. This might also change the perception of the preventive impacts and overall benefit perception (Culot et al., 2021).

5.3. *Theoretical implications*

As a contribution to theory, we first developed a conceptual framework and tested it empirically with items derived from a literature review and interviews. Our empirical study is based on a sample of ISO/IEC 27001 certified firms large enough to detect sector-specific differences and to generalize its findings. Therefore, our study enriches research on security management by following the call for access to corporate data and using actual behavior rather than intention data (Crossler et al., 2013) and second by providing an empirically grounded study rather than being "subjective-argumentative" (Siponen and Willison, 2007).

Following the call for studies with theoretical underpinnings (Culot et al., 2021), we, second, employ multiple theories to analyze the motives and benefits of ISO/IEC 27001 adoption. Building on the RBV, we highlight that information security management can be viewed as a valuable resource whose effectiveness should be measured beyond immediate financial gains or overall firm performance as the main dependent variable, in contrast to previous studies (Tejay and Shoraka, 2011; Hsu et al., 2016). Additionally, we employ institutional theory to highlight the role of external pressures where certificates can help signal compliance.

Third, the results of our research support the proposed classification of ISO/IEC 27001 as a preventive organizational innovation (Mirtsch et al., 2020b), which is characterized by the absence of immediate financial benefits but has the ability to prevent undesirable outcomes. This classification provides a possible explanation for the overall low level of adoption of this management system standard outside the ICT sector (Fomin et al., 2008). Our study, therefore, also contributes to the literature on innovation adoption by applying the concept of preventive innovation within a company-level survey of information security management.

6. Conclusion, limitations, and future research

Complementary to the advantages of digitalization, growing connectivity also entails risks to information security. The confidentiality, integrity, and availability of information is, therefore, an important asset that companies of all sizes and from all industries should safeguard. However, the adoption of ISO/IEC 27001 as the most popular international standard defining requirements for an information security management system is surprisingly low, for which there are (so far) few empirically grounded reasons. Therefore, we draw on institutional theory and the RBV. We, furthermore, argue that there is a legitimate need to consider the prevention focus as a distinctive feature of ISO/IEC 27001 compared to other management system standards previously analyzed. Therefore, this study analyzed the adoption of ISO/IEC 27001 through the lens of preventive organizational innovations.

The results of our study reveal that only preventive impacts and operational obstacles to investment significantly improve the overall benefit perception of ISO/IEC 27001 adoption. For the other experienced impacts arising from institutional pressures and economic considerations, we expect their importance to rise as stakeholders place more emphasis on companies taking active measures to safeguard information security. Due to this dynamic, we hope to motivate other researchers to replicate our study in the near future, especially in the face of institutional pressures increasingly arising from regulators.

Future studies could build on our study and enable a longitudinal perspective, particularly with regard to the influence of existing and future regulation, e.g., against the backdrop of the GDPR or the EU Cybersecurity Act. In addition, we recommend future research to complement the quantitative assessment with in-depth interviews and case studies to explore the findings in more detail. This will help shed light on why certain factors are not significant.

Our study is not without limitations, which may, however, provide promising avenues for future research. First, our study may suffer from memory bias, in which survey participants adapt their memory regarding their initial motives (which may have been years ago) to reflect the impact of the current management system, e.g., to avoid cognitive dissonance. Positive response bias has also been revealed in previous studies of management system standards (Manders, 2015), particularly when it comes to the question of who implemented a management system. Such bias could be reflected in the high overall score concerning the perceived overall benefits of adopting ISO/IEC 27001 and could also be triggered by very similar items, e.g., regarding motives and experienced impacts. Hence, future studies could preferably include a longitudinal perspective in which companies are surveyed both before adoption (on motives) and afterwards (on impacts), as well as the perspective of various people besides the person responsible for the management system in the company.

Second, our sector split (due to the sample size) does not allow for further sector differentiation, especially within the group of non-ICT sector companies. Future studies could deepen the sectorial analysis, e.g., by focusing on sectors in which information security is aimed at safeguarding personal data of customers (e.g., providers of financial services) as opposed to sectors in which ISO/IEC 27001 is implemented to safeguard internal production processes (e.g., in the context of Industry 4.0) also against the background of recent findings that positive abnormal returns differed between sectors (Deane et al., 2019).

Third, even though we deploy path analysis, our findings do not necessarily imply causality, and our model could be extended to include other aspects. As a suggestion, the impacts could be extended to matters of corporate social responsibility to provide a broader perspective on potential benefits of adoption and to strengthen the potentially important role of stakeholders beyond regulators and customers.

A final limitation is that our study was conducted in Germany, which has some regulatory peculiarities (e.g., the IT Security Act). Further research could, therefore, focus on countries with different regulatory and cultural settings, e.g., China or Japan, which rank first and second in terms of the number of valid ISO/IEC 27001 certificates (ISO, 2020).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Mona Mirtsch: Conceptualization, Methodology, Formal analysis, Writing - original draft, Writing - review & editing. **Knut Blind:** Conceptualization, Writing - review & editing. **Claudia Koch:** Writing - review & editing. **Gabriele Dudek:** Supervision.

Acknowledgments

This work was supported by the European Commission under Grant Agreement 778420—EURITO. We would like to thank our colleagues at BAM Dr. Tilman Denkler for help in developing the questionnaire, Michael Franke and Olaf Mätzner for IT support, Timo Kabierski for assistance with data analysis, Petra Keitzl for project management, and Susanne Stobbe for language editing. Finally, the authors acknowledge the valuable suggestions of the editor and three anonymous reviewers and thank them for their thoughtful comments and efforts to improve our manuscript.

Appendix

Overview of ISO/IEC 27001

The ISO/IEC 27001 standard is part of the ISO/IEC 27000 series of various standards on information security management published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This ISO/IEC 27000 family of standards comprises standards that address, for example, cloud security (ISO/IEC 27017 and ISO/IEC 27018), sector-specific applications such as telecommunications organizations (ISO/IEC 27011) or the energy utility industry (ISO/IEC 27019) or provide guidelines for cyber insurance (ISO/IEC 27102). The most recently published standard is ISO/IEC 27701 for privacy information management.

ISO/IEC 27001, which contains the general requirements for information security management systems, was first published in 2005 and is based on its predecessor British Standard (BS) 17799 (Disterer, 2013). It was replaced in 2013[3] by a revised version that is current today. Certification to standards from this family has so far only been possible to ISO/IEC 27001 (as in other families of standards, where usually only one standard is certifiable). However, sector-specific applications may be included if they do not conflict with ISO/IEC 27001 requirements.

ISO/IEC 27001 provides requirements for establishing, implementing, maintaining, and continually improving an ISMS that aims to preserve confidentiality, integrity, and availability of information. The standard defines this as follows:

- "Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity: Property of accuracy and completeness
- Availability: Property of being accessible and usable upon demand by an authorized entity" (ISO, 2013).

ISO/IEC 27001 comprises ten clauses, starting with three general ones on scope, normative references, and terms and definitions (referring to ISO/IEC 27000). It continues with the (4) context of the organization. Since ISO/IEC 27001 is "applicable to all organizations, regardless of type, size, or nature" (ISO/IEC 27001), its implementation must be tailored to its specific needs. The remaining clauses cover the aspects of Leadership (5), Planning (6), Support (7), Operation (8), Performance evaluation (9), and Improvement (10).

Although ISO/IEC 27001 follows the same high-level structure of other ISO management system standards, such as ISO 9001 and ISO 14001, there are some major differences. Besides pursuing various objectives (quality versus environmental protection versus information security), ISO/IEC 27001 is based on risk management principles and focuses on controls that organizations should select and implement (Disterer, 2013).

Annex A lists the applicable 35 control objectives and 114 controls derived from ISO/IEC 27002:2013 in the following 14 security control clauses:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

[3] For more information on the changes compared to the ISO/IEC 27001:2005 versions see ISO (2013), "New version of ISO/IEC 27001 to better tackle it security risks", available at: https://www.iso.org/news/2013/08/Ref1767.html (accessed 21 January 2021). The standard was last reviewed and confirmed in 2019, so the version ISO/IEC 27001:2013 (hereinafter referred to as ISO/IEC 27001) will remain to be the current version. According to a resolution of the 27th IAF General Assembly (https://www.iaf.nu/upFiles/Resolutions_IAF27_Approved.pdf), from 2015 all firms must comply with this version in order to become certified. Since a certificate is granted usually for three years, all currently ISO/IEC 27001 certified companies should be certified against ISO/IEC 27001:2013.

Table A.1 – Questionnaire items and references.

Indicators	Variable	Items based on:
Motives		
For what reasons has your company implemented the ISO/IEC 27001 standard or been certified according to ISO/IEC 27001?		
Please rate the extent to which the following reasons apply to your company (1 = Strongly disagree 5= Strongly agree)		
Demand from the customer	V1	AbuSaad et al., 2011
To promote domestic market access	V2	AbuSaad et al., 2011
To promote market access abroad	V3	AbuSaad et al., 2011
To increase legal certainty and/or to meet legal requirements	V4	Longras et al., 2018 Svoboda and Horalek, 2018
To improve internal company processes regarding information security	V5	AbuSaad et al., 2011 Svoboda and Horalek, 2018
To increase employee awareness of information security	V6	AbuSaad et al., 2011
Because competitors are also certified	V7*	Interview-derived
To be the first company (or one of the first) to be certified in my industry	V8	Interview-derived
For marketing and image reasons	V9	AbuSaad et al., 2011 Hsu et al., 2016
To meet the objectives of corporate management or top management (e.g., corporate target)	V10	AbuSaad et al., 2011
To prevent information security incidents	V11	Svoboda and Horalek, 2018
In response to a specific information security-related incident	V12*	Interview-derived
Experienced impacts		
What effect does the management system according to ISO/IEC 27001 have on your company?		
Please rate the extent to which the following effects apply to your company (1 = Strongly disagree 5= Strongly agree)		
Increased information security of the company (e.g., products or services less vulnerable to hacker attacks and higher business continuity)	V13	Barlette and Fomin, 2008 Longras et al., 2018
Increased employee awareness of information security	V14	AbuSaad et al., 2011
Lower insurance premiums	V15*	Saint-Germain, 2005 Fomin et al. 2008
Reduction of internal company costs caused by information security incidents	V16*	Saint-Germain, 2005
Reduction of the risk of information security incidents	V17	Svoboda and Horalek, 2018
Increase in sales through reference to the certificate (e.g., to customers or buyers)	V18	Interview-derived
Image improvement	V19	Interview-derived
Higher legal certainty	V20	Longras et al., 2018 Svoboda and Horalek, 2018
Overall benefit perception		
How much do you agree with the following statements?		
Please rate the extent to which you agree with the following statements? (1 = Strongly disagree 5= Strongly agree)		
All in all, the information security management system according to ISO/IEC 27001 is a good investment in terms of costs and benefits for our company.	V21	Longras et al., 2018
All in all, an additional ISO/IEC 27001 certification is a good investment in terms of cost-benefit for our company	V22	Longras et al., 2018
Obstacles		
What difficulties did your company face with the implementation of ISO/IEC 27001?		
Please comment on the extent to which the difficulties were or are applicable (1 = Strongly disagree 5= Strongly agree)		
High time investment	V23*	Barlette and Fomin, 2008 Alshitri and Abanumy, 2014
High costs	V24	Barlette and Fomin, 2008 Alshitri and Abanumy, 2014 Longras et al., 2018 Hsu et al., 2016
External consulting required for implementation	V25	Barlette and Fomin, 2008 Alshitri and Abanumy, 2014
Few consulting services available	V26	Interview derived
Lack of top management commitment	V27*	AbuSaad et al., 2011 Alshitri and Abanumy, 2014
In-house expertise insufficient (no suitably qualified employees available)	V28	Barlette and Fomin (2008) Alshitri and Abanumy, 2014 Longras et al., 2018
Low motivation and willingness of employees	V29	AbuSaad et al., 2011 Alshitri and Abanumy, 2014
Complexity of the standard content	V30	AbuSaad et al., 2011 Alshitri and Abanumy, 2014 Longras et al., 2018
Difficult determination of the scope	V31	Longras et al., 2018

Note: * depicts exclusion from PLS-SEM model.

Table A.2 – Management theories used and questionnaire items.

Management theory	Short description	Variables*
Resource-based view	From the perspective of the Resource-Based View (RBV), companies strive for sustained competitive advantage, which derives from the resources and capabilities a company controls. These should be valuable, rare, imperfectly imitable, and not substitutable. These resources and capabilities can be both tangible and intangible assets and also include a company's management skills, its organizational processes and routines, and the knowledge and information it controls. (Barney, 1991; Barney et al., 2001)	*Motives* Improve internal processes (V5) Increase employee awareness (V6) Be (one of the) first to be certified (V8) Meet top management objectives (V10) Prevent incidents (V11) Response to a specific incident (V12) *Impacts experienced* Increased information security (V13) Increased employee awareness (V14) Lower insurance premiums (V15) Reduced incident-related internal costs (V16) Reduced risk for incidents (V17) Certificate-related sales increase (V18) *Obstacles* High time investment (V23) High costs (V24) External consulting needed (V25) Few consulting services available (V26) Lack of top management commitment (V27) Lack of internal expertise (V28) Low employee motivation (V29) Complexity of standard content (V30) Difficult scope determination (V31) *Overall benefit perception* Implementation is a good investment (V21) Additional certification is a good investment (V22)
Institutional theory	Institutional theory is concerned with the influence of institutions within society that exert formal and informal pressures, e.g., on organizations. These external pressures can be coercive (stemming, e.g., from political influence), mimetic (copying others also as a means of dealing with uncertainty), or normative (related to professionalization) and help explain why organizations become similar over time, also known as isomorphism. (DiMaggio and Powell, 1983; Meyer and Rowan, 1977)	*Motives* Coercive: Demand from the customer (V1) Promote domestic market access (V2) Promote market access abroad (V3) Marketing/image reasons (V9) Increase legal certainty (V4) Mimetic Competitors are certified (V7) *Impacts experienced* Higher legal certainty (V20) Image improvement (V19)
Diffusion of Innovations theory	The Diffusion of Innovations (DoI) theory addresses why, how and what rate innovations spread among a social system (Rogers, 1962). As a specific form of innovation preventive innovations aim to lower the probability of unwanted future events. Since this might affect the persuasion phase negatively, these are oftentimes characterized by lower adoption rates than incremental innovations (Rogers, 2002).	*Motives* Improve internal processes (V5) Increase employee awareness (V6) Prevent incidents (V11) Response to a specific incident (V12) *Impacts experienced* Increased information security (V13) Increased employee awareness (V14) Reduced risk for incidents (V17)

Note: * depicts short titles used within the article.

Table A.3 – Correlation matrix with VIF values.

		Motives												Experienced Impacts								Overall Benefit Perception		Obstacles								
	VIF	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21	V22	V23	V24	V25	V26	V27	V28	V29	V30	V31
V1	1.43	1																														
V2	1.38	0.45	1																													
V3	1.31	0.38	0.44	1																												
V4	1.00	-0.11	0.18	0.08	1																											
V5	**3.89**	-0.02	0	0.07	0.36	1																										
V6	**3.49**	0.00	0.20	0	0.42	**0.76**	1																									
V7	N/A	0.19	0.38	-0.01	0	0.23	0.21	1																								
V8	1.36	0.05	0.17	0.05	0.10	0	0.00	0.01	1																							
V9	1.36	0.17	0	0.24	0.19	0.33	0.25	0	**0.52**	1																						
V10	1.43	0.04	0.34	0	0.35	0.49	0.46	0.20	0	0.27	1																					
V11	**3.05**	0.00	0.24	-0.06	0	**0.66**	**0.71**	0.25	0.03	0	0.40	1																				
V12	N/A	0.09	0.14	0.18	0.19	0	0.18	0.12	0.09	0.13	0	0.12	1																			
V13	1.20	0.08	0	-0.16	-0.05	0.24	0.22	0	0.17	0.01	0.09	0.24	0	1																		
V14	1.33	0.18	0.24	0	0.15	0.35	0.41	0.09	0	0.15	0.21	0.33	0.05	0	1																	
V15	N/A	0.28	0.10	0.08	0	0.08	0.11	0.30	0.07	0	0.21	0.13	0.06	0.14	0	1																
V16	N/A	-0.01	0.01	-0.15	0.13	0	0.30	0.21	0.03	0.13	0	0.32	0.16	0.33	0.14	0	1															
V17	1.30	-0.01	0	-0.08	0.17	0.44	0.50	0	0.01	0.06	0.28	**0.51**	0	0.34	0.30	0.01	0.28	1														
V18	1.22	0.43	**0.53**	0	0.05	0.10	0.08	0.27	0	0.43	0.15	0.13	0.09	0	0.17	0.29	0.07	0.08	1													
V19	1.22	0.15	0.31	0.18	0	0.31	0.24	0.23	0.29	**1**	0.19	0.20	0.09	0.10	0	-0.06	0.11	0.02	0.45	1												
V20	1.00	-0.06	0.11	0.13	**0.65**	0	0.26	0.17	0.26	0.26	0	0.21	0.09	0.03	0.15	0	0.15	0.20	0.20	0.38	1											
V21	1.55	0.12	0	0.14	0.16	0.32	0.28	0	0.06	0.09	0.25	0.26	0	0.33	0.30	0.24	0.29	0	0.34	0.13	0.21	1										
V22	1.55	0.02	0.21	0	0.17	0.34	0.34	0.28	0	0.19	0.34	0.45	-0.10	0	0.21	0.21	0.30	0.47	0	0.20	0.24	**0.71**	1								
V23	N/A	0.02	0.08	-0.17	0	0.08	0.04	-0.11	0.04	0	-0.05	0.13	0.04	0.16	0	-0.15	-0.06	-0.01	0.03	0	-0.14	-0.18	-0.12	1								
V24	1.12	0.14	0.16	-0.05	0.13	0	0.04	-0.09	0.14	0.06	0	0.04	0.06	0.10	0.12	0	-0.12	-0.10	0.02	0.13	0	-0.33	-0.26	0.48	1							
V25	1.14	0.06	0	0.10	-0.04	-0.19	-0.16	0	0.01	-0.01	-0.10	-0.14	0	0.07	-0.05	-0.02	-0.07	0	-0.06	0.01	0.04	-0.17	0	0.09	0.26	1						
V26	1.14	0.07	0.02	0	-0.01	-0.06	-0.01	0.02	0	0.01	-0.02	0.01	0.25	0	-0.04	-0.01	-0.08	-0.11	0	0.03	0.01	-0.18	-0.17	0	0.26	0.30	1					
V27	N/A	0.15	0.07	0.04	0	0.03	0.00	0.00	-0.10	0	-0.12	0.02	0.03	-0.01	0	0.19	0.12	-0.02	0.02	0	-0.16	0.03	-0.01	0.15	0	-0.03	0.07	1				
V28	1.17	0.22	0.01	0.07	-0.14	0	-0.09	0.06	-0.10	0.09	0	-0.01	0.02	0.09	-0.10	0	0.07	-0.10	0.07	-0.04	0	-0.05	-0.04	0.08	0.06	0	0.14	0.40	1			
V29	1.17	0.20	0	0.12	-0.07	-0.12	-0.15	0	-0.04	0.02	-0.18	-0.16	0	-0.23	-0.27	0.05	-0.16	0	-0.05	-0.14	-0.16	-0.18	0	0.05	-0.02	0.02	0.01	0	0.36	1		
V30	1.62	0.11	0.04	0	0.02	0.02	-0.05	0.07	0	0.08	0.01	0.00	0.04	0	-0.11	-0.14	-0.06	0.08	0	0.11	0.09	-0.31	-0.19	0	0.31	0.20	0.14	0.10	0	0.21	1	
V31	1.67	0.12	0.08	0.01	0	-0.02	-0.05	0.13	0.15	0	-0.06	0.06	0.07	-0.08	0	-0.06	0.02	-0.03	0.12	0	0.17	-0.28	-0.16	0.21	0	0.16	0.11	0.18	0.38	0	**0.52**	1

Note: N/A at VIF values depicts exclusion from the PLS-SEM model.

Not all of the controls defined in Annex A need to be applied by organizations to comply with ISO/IEC 27001, and organizations may also choose to design controls. However, organizations must prepare a Statement of Applicability (SoA) indicating and justifying which controls are included and which are not (ISO/IEC 27001).

REFERENCES

Abu Bakar Z, Yaacob NA, Udin ZM, Hanaysha JR, Loon LK. The adoption of business continuity management best practices among malaysian organizations. Adv. Sci. Lett. 2017;23(9):8484–91.

AbuSaad, B., Saeed, F.A., Alghathbar, K. and Khan, B., 2011. "Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned", in *Proceedings of the 9th Australian Information Security Management Conference*,Perth Western Australia, pp. 1-9.

Accenture and Ponemon Institute (2019), "The cost of cybercrime", available at https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (accessed 01.11.2019).

Akerlof GA. "The market for "lemons": quality uncertainty and the market mechanism". In: Diamond P, Rothschild M, editors. In: Uncertainty in Economics. Academic Press; 1978. p. 235–51.

Alberti M, Caini L, Calabrese A, Rossi D. Evaluation of the costs and benefits of an environmental management system. Int. J. Prod. Res. 2000;38(17):4455–66.

Alvarez-Garcia J, del RioRama MD. Sustainability and EMAS: impact of motivations and barriers on the perceived benefits from the adoption of standards. Sustainability 2016;8(10):1057.

Annarelli A, Nonino F, Palombi G. Understanding the management of cyber resilient systems. Comput. Ind. Eng. 2020;149.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L. and Kallitsis, M., 2017. "Understanding the Mirai Botnet", in *Proceedings of the 26th USENIX Security Symposium (USENIX Security 17)*, USENIX Association, Vancouver , BC, pp. 1093-1110.

Alshitri, K.I. and Abanumy, A.N., 2014. "Exploring the Reasons Behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia", in *Proceedings of the 2014 International Conference on Information Science and Applications (ICISA)*, IEEE, Seoul, South Korea, pp. 1-4.

Armbruster H, Bikfalvi A, Kinkel S, Lay G. Organizational innovation: The challenge of measuring non-technical innovation in large-scale surveys. Technovation 2008;28(10):644–57.

Bakar ZA, Yaacob NA, Udin ZM. The effect of business continuity management factors on organizational performance: a conceptual framework. Int. J. Econ. Financ. Issues 2015;5:128–34 No. Special Issue.

Barlette Y, Fomin VV. Exploring the Suitability of IS Security Management Standards for SMEs. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008); 2008. p. 308. doi:10.1109/HICSS.2008.167.

Barlette Y, Fomin VV. The adoption of information security management standards: A literature review. In: Information Resources Management: Concepts, Methodologies, Tools and Applications. IGI Global; 2010. p. 69–90.

Barney J. Firm resources and sustained competitive advantage. J. Manag. 1991;17(1):99–120.

Barney J, Wright M, Ketchen Jr DJ. The resource-based view of the firm: Ten years after 1991. J. Manag. 2001;27(6):625–41.

Bellesi F, Lehrer D, Tal A. Comparative advantage: The impact of ISO 14001 environmental certification on exports. Environ. Sci. Technol. 2005;39(7):1943–53.

Berg, A. and Niemeier, M. (2019), "Wirtschaftsschutz in der digitalen Welt", available at https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf (accessed 06.01.2021).

Bertrand JT. Diffusion of innovations and HIV/AIDS. J. Health Commun. 2004;9(S1):113–21.

Boiral O, Roy M-J. ISO 9000: integration rationales and organizational impacts. Int. J. Operat. Prod. Manage. 2007;27(2):226–47.

Blind, K., 2019. Certifications based on International Management System Standards as Innovation Indicators: An Explorative

Feasibility Analysis, in *Proceedings of the EURAS 2019 Conference: Standards for a Bio-Based Economy*, Rome, Italy, pp. 51-69.
Bundesnetzagentur (2016), "Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den ITSicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006", available at https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/Konformitaetsbewertungsprogramm.pdf?__blob=publicationFile&v=1 (accessed 10 August 2020).
Bundesnetzagentur (2018), "IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz", available at https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf;jsessionid=B7B3F268790093AC5A473CEAECBDA6FF?__blob=publicationFile&v=4 (accessed 10.08.2020).
Casadesu M, Gime G, Heras I. Benefits of ISO 9000 implementation in Spanish industry. Eur. Bus. Rev. 2001;13(6):327–36.
Castka P, Corbett CJ. Management systems standards: diffusion, impact and governance of ISO 9000, ISO 14000, and other management standards. Found. Trends® Technol. Inf. Operat. Manage. 2013;7(3–4):161–379.
Cattell RB. The scree test for the number of factors. Multivar. Behav. Res. 1966;1(2):245–76.
Claver E, Tari JJ. The individual effects of total quality management on customers, people and society results and quality performance in SMEs. Qual. Reliab. Eng. Int. 2008;24(2):199–211.
Collins D. Pretesting survey instruments: an overview of cognitive methods. Qual. Life Res. 2003;12(3):229–38.
Crossler R, Johnston A, Lowry P, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput. Sec. 2013;32:90–101.
Crowder M. Quality standards: integration within a bereavement environment. TQM J. 2013.
Culot G, Fattori F, Podrecca M, Sartor M. Addressing industry 4.0 cybersecurity challenges. IEEE Eng. Manage. Rev. 2019;47(3):79–86.
Culot G, Nassimbeni G, Podrecca M, Sartor M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. TQM J. 2021;33(7):76–105.
D'Souza C, Mort GS, Zyngier S, Robinson P, Schlotterlein M. Preventive innovation: an australian case study on HPV vaccination. Health Mark. Q. 2013;30(3):206–20.
Daddi T, Testa F, Frey M, Iraldo F. Exploring the link between institutional pressures and environmental management systems effectiveness: an empirical study. J. Environ. Manage. 2016;183:647–56.
Darnall N. Why firms mandate ISO 14001 certification. Bus. Soc. 2006;45(3):354–81.
Das R, Gündüz MZ. Analysis of cyber-attacks in IoT-based critical infrastructures. Int. J. Inf. Sec. Sci. 2020;8(4):122–33.
Deane JK, Goldberg DM, Rakes TR, Rees LP. The effect of information security certification announcements on the market value of the firm. Inf. Technol. Manage. 2019;20(3):107–21.
DePietro R, Wiarda E, Fleischer M. The context for change: organization, technology and environment. In: Tornatzky LG, Fleischer M, Chakrabarti A, editors. In: The processes of technological innovation. MA: Lexington Books; 1990. p. 151–75.
Diamantopoulou V, Tsohou A, Karyda M. From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls. Inf. Comput. Sec. 2020;28(4):645–62.
Diesch R, Pfaff M, Krcmar H. A comprehensive model of information security factors for decision-makers. Comput. Sec. 2020;92.
DiMaggio P, Powell WW. The iron cage revisited: Collective rationality and institutional isomorphism in organizational fields. Am. Sociol. Rev. 1983;48(2):147–60.
Dionysiou I, Kokkinaki A, Magirou S, Iacovou T. Adoption of ISO 27001 in cyprus enterprises: current state and challenges. In: Standards and Standardization: Concepts, Methodologies, Tools, and Applications. IGI Global; 2015. p. 994–1017.
Disterer G. ISO/IEC 27000, 27001 and 27002 for information security management. J. Inf. Sec. 2013;4(2):92–100.
ENISA (2019), "ENISA threat landscape report 2018", available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 (accessed 12.01.2021).
European Commission (2013), "Cybersecurity strategy of the european union: an open, safe and secure cyberspace", available at http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed 05.03.2018).
European Commission (2021), "Rolling plan for ICT standardisation 2021;" available at https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2021 (accessed 19.04.2021).
Eurostat (2020), "Community survey on ICT usage and e-commerce in enterprises", available at https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises#Access_and_use_of_the_internet (accessed 14.6.2021).
Federal Office for Information Security (BSI) (2019), "The State of IT Security in Germany in 2019", available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf;jsessionid=06117C749F55DD2F21912222B9E3352F.2_cid503?__blob=publicationFile&v=3 (accessed 14.06.2021).
Fernandes Rodrigues Alves M, Vasconcelos Ribeiro Galina S, Dobelin S. Literature on organizational innovation: past and future. Innov. Manage. Rev. 2018;15(1):2–19.
Ferreira LM, Cândido CJ. Factors influencing firm propensity for ISO 9001 withdrawal: evidence on decertification tendency and antecedents. Int. J. Prod. Econ. 2021;233.
Fomin, V.V., de Vries, H.J. and Barlette, Y., 2008. ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption, in *Proceedings of the third European conference on Management of Technology (EuroMOT)*, Nice, France, pp. 1-13.
Guler I, Guillén MF, Macpherson JM. Global competition, institutions, and the diffusion of organizational practices: The international spread of ISO 9000 quality certificates. Adm. Sci. Q. 2002;47(2):207–32.
Hahm M-I, Park E-C, Choi KS, Lee H-Y, Park J-H, Park S. Inequalities in adoption of cancer screening from a diffusion of innovation perspective: Identification of late adopters. Cancer Epidemiol. 2011;35(1):90–6.
Hair JF, Risher JJ, Sarstedt M, Ringle CM. When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. 2019;31(1):2–24.
Hair Jr JF, Hult GTM, Ringle C, Sarstedt M. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks, CA: Sage; 2017a.
Hair Jr JF, Sarstedt M, Ringle CM, Gudergan SP. Advanced Issues in Partial Least Squares Structural Equation Modeling. Thousands Oaks, CA: Sage; 2017b.
Hsu C, Lee J-N, Straub DW. Institutional influences on information systems security innovations. Inf. Syst. Res. 2012;23(3-part-2):918–39.

Hsu C, Wang T, Lu A. In: The Impact of ISO 27001 Certification on Firm Performance. Hawaii, USA: IEEE; 2016. p. 4842–8.
Iatridis K, Kesidou E. What drives the quality of certifiable management system standards implementation? Insights from the ISO 9001 Standard". In: Heras-Saizarbitoria I, editor. In: ISO 9001, ISO 14001, and New Management Standards. Cham, Switzerland: Springer; 2018. p. 17–38.
ISO. In: Information Technology – Security Techniques – Information Security Management Systems – Requirements. ISO/IEC 27001:2013 (en); 2013.
ISO (2020), "The ISO Survey of Management System Standard Certifications 2019", available at https://www.iso.org/the-iso-survey.html (accessed 4 September 2020).
Kaiser HF. The application of electronic computers to factor analysis. Educ. Psychol. Measur. 1960;20(1):141–51.
Kaiser HF, Rice J. Little jiffy, mark IV. Edu. Psychol. Measur. 1974;34(1):111–17.
Kinne J, Axenbeck J. Web mining of firm websites: a framework for web scraping and a pilot study for Germany. In: ZEW Discussion Paper 18-033. Mannheim: ZEW – Leibniz Centre for European Economic Research; 2018. p. 1–35.
Kotulic AG, Clark JG. Why there aren't more information security research studies. Inf. Manage. 2004;41(5):597–607.
Lo LK, Chang DS. The difference in the perceived benefits between firms that maintain ISO certification and those that do not. Int. J. Prod. Res. 2007;45(8):1881–97.
Lohmöller J-B. Latent Variable Path Modeling with Partial Least Squares. Heidelberg: Physica-Verlag; 1989.
Longras A, Pereira T, Cameiro P, Pinto P. In: On the Track of ISO/IEC 27001: 2013 Implementation Difficulties in Portuguese Organizations. IEEE; 2018. p. 886–90.
Manders, B. (2015), *Implementation and Impact of ISO 9001*,(No. EPS-2014-337-LIS). Erasmus Research Institute of Management – ERIM Ph.D. Series, Rotterdam.
Marimon F, Casadesús M. Reasons to adopt ISO 50001 energy management system. Sustainability 2017;9(10):1740.
Martinez-Costa M, Choi TY, Martinez JA, Martinez-Lorente AR. ISO 9000/1994, ISO 9001/2000 and TQM: The performance debate revisited. J. Oper. Manage. 2009;27(6):495–511.
Meyer JW, Rowan, B. Institutionalized organizations: formal structure as myth and ceremony. Am. J. Sociol. 1977;83(2):340-363.
Mirtsch M, Kinne J, Blind K. Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis". IEEE Trans. Eng. Manage. 2020a;68(1):87–100.
Mirtsch, M., Pohlisch, J. and Blind, K., 2020b. Exploring the international diffusion of the information security management system standard ISO/IEC 27001: exploring the role of culture, in *Proceedings of the 28th European Conference on Information Systems (ECIS2020)* A Virtual AIS Conference.
Mohurle S, Patil M. A brief study of wannacry threat: Ransomware attack 2017. Int. J. Adv. Res. Comput. Sci. 2017;8(5):1938–40.
Moore T. The economics of cybersecurity: principles and policy options. Int. J. Crit. Infrastruct. Prot. 2010;3(3):103–17.
Murmura F, Liberatore L, Bravi L, Casolani N. Evaluation of Italian companies' perception about ISO 14001 and eco management and audit scheme III: motivations, benefits and barriers. J. Cleaner Prod. 2018;174:691–700.
Nair A, Prajogo D. Internalisation of ISO 9000 standards: the antecedent role of functionalist and institutionalist drivers and performance implications. Int. J. Prod. Res. 2009;47(16):4545–68.
Nelson RR, Winter SG. An Evolutionary Theory of Economic Change. Harvard University Press; 1982.
OECD/Eurostat. Oslo Manual, The Measurement of Scientific and Technological Activities. Paris: OECD Publishing; 2005.
Overstreet RE, Cegielski C, Hall D. Predictors of the intent to adopt preventive innovations: a meta-analysis. J. Appl. Soc. Psychol. 2013;43(5):936–46.
Peng S-y. Private" Cybersecurity Standards? cyberspace governance, multistakeholderism, and the (Ir) relevance of the TBT Regime. Cornell Int. Law J. 2018;51(2):445–69.
Prajogo D. The roles of firms' motives in affecting the outcomes of ISO 9000 adoption. Int. J. Operat. Prod. Manage. 2011;31(1):78–100.
Ray G, Barney JB, Muhanna WA. Capabilities, business processes, and competitive advantage: choosing the dependent variable in empirical tests of the resource-based view. Strateg. Manage. J. 2004;25(1):23–37.
Ringle, C.M., Wende, S. and Becker, J.-M. (2015), "SmartPLS 3", in *Boenningstedt: SmartPLS GmbH*.
Rogers EM. Diffusion of Innovations. Free Press of Glencoe; 1962.
Rogers EM. Breakthrough: Emerging New Thinking. In: Gromyko A, Hellmann M, editors. Diffusion of the idea of beyond war. New York: Walker; 1988.
Rogers EM. Diffusion of preventive innovations. Addict. Behav. 2002;27(6):989–93.
Rogers EM. Diffusion of Innovations. New York, NY: Free Press; 2003.
Saint-Germain R. Information security management best practice based on ISO/IEC 17799. Inf. Manage. J. 2005;39(4):60–6.
Singh PJ, Feng M, Smith A. ISO 9000 series of standards: comparison of manufacturing and service organisations. Int. J. Qual. Reliab. Manage. 2006;23(2):122–42.
Sinha M, Karcher P, Jochem R. Success factors and organizational approaches for the implementation of energy management systems according to ISO 50001. TQM J. 2015.
Siponen M, Willison R. In: A critical assessment of IS security research between 1990–2004. , Switzerland: Gallen; 2007. p. 1551–9.
Siponen M, Willison R. Information security management standards: problems and solutions. Inf. Manage. 2009;46(5):267–70.
Skopak A, Sakanovic S. Adoption of Standard for Information Security ISO/IEC 27001 in Bosnia and Herzegovina, in. Proceedings of the International Conference on Economic and Social Studies (ICESoS) - Regional Economic Development - Entrepreneurship and InnovationSarajevo, Bosnia and Herzegovina 2016:35–42.
StataCorp. In: StataCorp LLC. Stata statistical software: release 15. TX: College Station; 2017.
Susanto H, Almunawar MN, Tuan YC. Information security management system standards: a comparative study of the big five. Int. J. Electr. Comput. Sci. IJECS-IJENS 2011;11(5):23–9.
Susanto H, Almunawar MN, Tuan YC. Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. Int. J. Eng. Technol. 2012;2(1):67–75.
Svoboda T, Horalek J. Analysis of the information security management in Czech Republic. Adv. Sci. Lett. 2018;24(11):8562–6.
Tejay GP, Shoraka B. Reducing cyber harassment through de jure standards: a study on the lack of the information security management standard adoption in the USA. Int. J. Manage. Dec. Mak. 2011;11(5-6):324–43.
Terziovski M, Power D. Increasing ISO 9000 certification benefits: a continuous improvement approach. Int. J. Qual. Reliab. Manage. 2007.
Terziovski M, Samson D, Dow D. The business value of quality management systems certification. Evidence from Australia and New Zealand. J. Oper. Manage. 1997;15(1):1–18.
Ţigănoaia B. Some aspects regarding the information security management system within organizations–adopting the

ISO/IEC 27001: 2013 standard". Stud. Inform. Control 2015;24(2):201–10.
Tuczek F, Castka P, Wakolbinger T. A review of management theories in the context of quality, environmental and social responsibility voluntary standards. J. Cleaner Prod. 2018;176:399–416.
Tunçalp D. Diffusion and adoption of information security management standards across countries and industries. J. Glob. Inf. Technol. Manage. 2014;17(4):221–7.
Uwizeyemungu, S. and Poba-Nzaou, P., 2015. Understanding information technology security standards diffusion: An institutional perspective, in Proceedings of the 2015 International Conference on Information Systems Security and Privacy (ICISSP), pp. 5-16.
van Oorschot J, Hofman E, Halman JIM. A bibliometric review of the innovation adoption. Technol. Forecast Soc. Change 2018;134:1–21.
van Wessel R, de Vries HJ. Business impact of international standards for information security management. Lessons from case companies. J. ICT Stand. 2013;1:25–40.
Viscusi WK. A note on" lemons" markets with quality certification. Bell J. Econ. 1978;9:277–9.
Von Solms R, Van Niekerk J. From information security to cyber security. Comput. Sec. 2013;38:97–102.
Weishäupl, E., Yasasin, E. and Schryen, G., 2015. A multi-theoretical literature review on information security investments using the resource-based view and the organizational learning theory, in Proceedings of the 36th International Conference on Information Systems (ICIS), Forth Worth, Texas, USA.
Wiengarten F, Humphreys P, Onofrei G, Fynes B. The adoption of multiple certification standards: perceived performance implications of quality, environmental and health & safety certifications. Prod. Plan. Control 2017;28(2):131–41.
Wold H. Estimation of principal components and related models by iterative least squares. In: Krishnajah PR, editor. In: Multivariate analysis. New York: Academic Press; 1966. p. 391–420.

Mona Mirtsch is a researcher at the Division S.2 Accreditation and Conformity Assessment at the Bundesanstalt für Materialforschung und -prüfung (Federal Institute for Materials Research and Testing—BAM), Berlin, Germany, dealing with questions of quality infrastructure. She holds a Doctoral degree in innovation economics from the Technische Universität Berlin in the field of information security management, standards and certification. She holds a master's degree from the San Diego State University and a Diploma from the European University Viadrina Frankfurt, both in Business administration.

Knut Blind is a Professor for Innovation Economics at Technische Universität Berlin, Germany, and Coordinator of Innovation & Regulation at Fraunhofer Institute for Systems and Innovation Research ISI. His habilitation from the faculty of Economics at Kassel University concerned the economic aspects of standardization. He holds a Doctoral degree in economics from Freiburg University and a master's degree in Economics at the University of Freiburg. His research focus is on analyzing the connection between regulation and innovation. He was elected a member of the German Academy of Science and Engineering (acatech) in 2017 due to his scientific achievements.

Claudia Koch is a researcher at the Division S.2 Accreditation and Conformity Assessment at the Bundesanstalt für Materialforschung und -prüfung (Federal Institute for Materials Research and Testing—BAM), Berlin, Germany, dealing with questions of quality infrastructure. She holds a Doctoral degree in innovation economics from the Technische Universität Berlin in the field of standardization in the Industrial Internet of Things. She holds a Diploma in Business administration and a master's degree in Business law and economic law (LL.M.oec.) from Martin-Luther Universität Halle-Wittenberg.

Gabriele Dudek is head of the Division 2.6 Testing and Evaluation of Explosives and Pyrotechnic at the Bundesanstalt für Materialforschung und -prüfung (Federal Institute for Materials Research and Testing—BAM), Berlin, Germany. She holds a Doctoral degree in natural sciences from the Humboldt University Berlin and holds a master's degree from the Technische Universität Berlin in chemistry. She has over 15 years' experience in standard setting on general requirements for bodies performing conformity assessment, such as certification, and their accreditation.