International Journal for Quality Research 17(3) 747–768
ISSN 1800-6450

Mona Mirtsch[1]

Article info:
Received 17.03.2022.
Accepted 10.07.2023.

UDC – 004.057.2
DOI – 10.24874/IJQR17.03-08

ADOPTION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD ISO/IEC 27001: A STUDY AMONG GERMAN ORGANIZATIONS

Abstract: *Against the backdrop of numerous security breaches and cyber-attacks, organizations need to take measures to secure their data and information. However, the well-known management system standard ISO/IEC 27001 for information security has shown a lower adoption rate – in terms of annual ISO survey data – than was previously expected by scholars and practitioners. Through the lens of Rogers' diffusion of innovation theory, we consider the adoption of ISO/IEC 27001 as a 'preventive innovation' and aim to identify factors that help gain a better understanding of its adoption. Therefore, we conducted a survey among German organizations on the use and impact of management system standards, explicitly distinguishing between organizations that implement ISO/IEC 27001 and those that are additionally certified against this standard. This study provides insights and contributes to an advanced understanding of motives, impacts, barriers, and useful measures to increase adoption of ISO/IEC 27001. Our findings may be useful to organizations considering the adoption of this management system standard, to certification bodies providing certification services, and to policymakers seeking means to improve information security in organizations.*

Keywords: *ISO/IEC 27001, Management system standard, Information security, QI-FoKuS, Certification*

1. Introduction

With the increasing digitalization of organizations, the role of digitally stored information and information security is also becoming increasingly important. Security breaches have become a global concern, with a value at risk arising from direct and indirect attacks worth USD 5.2 trillion between 2019 and 2023 (Accenture and Ponemon Institute, 2019). Despite the high risk, organizations might not take adequate measures to ensure information security, given the number and severity of security breaches.

Information security management assists organizations in preserving information security. The international management system (MS) standard ISO/IEC 27001 defines the requirements for the establishment, implementation, control, and continuous improvement of an information security MS. After implementing an MS standard, organizations may decide to additionally seek certification as a form of conformity assessment. Certification is defined as a third-party attestation that the

[1] Corresponding author: Mona Mirtsch
Email: mona.mirtsch@bam.de

requirements laid down in the standard have been met (ISO/IEC 17000). These certificates can help organizations signal their efforts to stakeholders, thus overcoming information asymmetries regarding safeguarding information security (Disterer, 2013; Saint-Germain, 2005).

The annual ISO Survey (ISO, 2019a) can serve as an indicator of the diffusion of this MS by taking into account the number of valid certificates against ISO/IEC 27001. Compared to other MS standards such as ISO 9001 for quality and ISO 14001 for environmental management, the number of ISO/IEC 27001 certificates for information security is lower than expected by scholars (Fomin, de Vries, & Barlette, 2008; Tunçalp, 2014). The reason for this may be found in the economics of cybersecurity, which is characterized by misaligned incentives, information asymmetries, and negative externalities (Anderson & Moore, 2006; Moore, 2010). In the case of ISO/IEC 27001, previous studies have, furthermore, shown that organizations neither benefit (directly) from its implementation (Fomin et al., 2008; Hsu, Wang, & Lu, 2016), even compared to other popular MS standards (Castka & Corbett, 2013). Furthermore, certification against this standard is often not demanded by relevant stakeholders, so ISO/IEC 27001 has not yet reached a legitimate status yet (Uwizeyemungu & Poba-Nzaou, 2015).

To overcome this market failure, certification against standards such as ISO/IEC 27001 has increasingly moved into the focus of policymakers in the European Union and other regions. For example, under the Directive on security of network and information systems (NIS Directive EU 2016/1148) and transposition into German law, German authorities require energy providers (as operators of essential services in critical infrastructures) to submit certificates to the competent authority (Bundesnetzagentur, 2018). Under the General Data Protection Regulation (EU GDPR), certificates are foreseen to demonstrate the compliance with legal requirements (Diamantopoulou, Tsohou, & Karyda, 2019; Lopes, Guarda, & Oliveira, 2019), and finally, the recently adopted Regulation on Information and Communication Technology Cybersecurity Certification Regulation (EU) 2019/881, the "Cybersecurity Act", sets up a European cybersecurity certification framework for ICT products, services, and processes, which will provide for mandatory certificates for specific areas from 2023.

However, firms do not have to seek external attestation through certification but can also make use of this MS standard by implementing it partially or fully. Nevertheless, most studies do not differentiate between the implementation of MS standards and a possible additional certification (Manders, 2015) since most studies use certification figures (e.g., reported in the annual ISO Survey) to measure the impact of standards in a company (de Vries & El Osrouti, 2019).

The aim of this study is, therefore, to gain insights into the ISO/IEC 27001 adoption. To address the limitations of earlier studies, we have firstly included aspects of conformity assessment by including firms that declare themselves compliant rather than having obtained a certificate. Secondly, we have included criteria for organizations to select certification bodies providing certification services, as most academic literature on MS standards (such as ISO 9001) focuses on the motives and benefits of adoption rather than on conformity assessment (Castka, Prajogo, Sohal, & Yeung, 2015).

To this end, we are conducting an online survey among German organizations to investigate the application of MS standards, with a focus on ISO/IEC 27001. For this purpose, we compare the motives as well as benefits of organizations that are either certified to this standard or apply it (without seeking certification), the difficulties encountered, the reasons for non-adoption,

and the usefulness of concrete measures to increase ISO/IEC 27001 adoption in Germany.

The remainder of this paper is structured as follows. First, we present an overview of ISO/IEC 27001 and, specifically, its adoption in Germany. Then we discuss relevant previous research on ISO/IEC 27001 on adoption and certification, followed by the diffusion of the innovation theory of Rogers (2003) as the theoretical foundations for our research. The next section outlines the research methodology we used to collect and analyze the empirical data collected through an online survey. In the fourth and fifth sections, we present and discuss the results of our analysis, followed by the conclusion, practical implications, limitations, and avenues for future research.

2. Literature review

2.1. Overview of ISO/IEC 27001

The international standard ISO/IEC 27001 is part of the ISO family of MS standards, which are defined, e.g., in the context of ISO 9001, as "a set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives". As the only certifiable standard, this standard is part of the ISO/IEC 27000 family of information security system standards, which comprises over 40 standards (ISO, 2019b). It is applicable to all types of companies, regardless of size, type, nature, or country of origin.

ISO/IEC 27001 has its roots in the British standard BS7799, published by the United Kingdom Government's Department of Trade and Industry (DTI) (Skopak & Sakanovic, 2016). The objective of ISO/IEC 27001 is to preserve the confidentiality, integrity, and availability of information, also known as the 'CIA triad'. ISO/IEC 27001 defines these terms 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".

Preserving information security is particularly important as organizations of all kinds, including governments, are exposed to severe risks if information is unintentionally disclosed, unreliable, or unavailable (van Wessel & de Vries, 2013).

In the context of *confidentiality*, security breaches can lead to reputational damages at substantial costs (Saint-Germain, 2005). A prominent example of a data breach is Yahoo's 2016 report that at least 500 million accounts were exposed in 2014 by what Yahoo called a "state-sponsored" actor (Cheng, Liu, & Yao, 2017).

In terms of *integrity*, information security can help ensure business continuity, especially when attacks can harm the core functions of organizations (Von Solms & Van Niekerk, 2013). As an example, malware called TRITON attacked the industrial control systems of a petrochemical plant in Saudi Arabia, causing a shutdown after altering its codebase (Mansfield-Devine, 2018), or Stuxnet where staff PCs of an Iran nuclear plant were targeted (Chen & Abu-Nimeh, 2011).

Availability is often mentioned in the context of massive distributed denial-of-service (DDoS) attacks where, as in the Mirai Botnet example, malware infected consumer Internet of Things (IoT) devices (e.g., home routers) and made access to a network, such as a hosting provider OVH, inaccessible (Antonakakis et al., 2017). Information security management includes the timely monitoring of an organization's risks and vulnerabilities, accessing their impact, and reducing or eliminating risks by implementing appropriate controls.

Therefore, ISO/IEC 27001 focuses not only on IT security but also on processes to preserve information security, including aspects of legal protection, human resource management, and protection of physical assets (Skopak & Sakanovic, 2016). Closely related to ISO/IEC 27001, ISO/IEC 27002 provides a list of commonly accepted control objectives and best practice controls that can be used to guide implementation.

An important aspect of ISO management systems is the continuous improvement of their processes, often referred to as the PDCA (Plan, Do, Check, Act) cycle, even though this is no longer explicitly mentioned in the latest version of ISO/IEC 27001 since 2013. As ISO/IEC 27001 is applicable to a wide range of organizations, it is generic in its content. Therefore, it needs to be implemented according to the needs of each organization, and attention has to be paid to the scope of application (SoA) of ISO/IEC 27001 for an organization.

Organizations meeting the requirements described in ISO/IEC 27001 can seek certification from a certification body. After an organization has implemented ISO/IEC 27001, certification can be obtained following a two-step process. After an organization has conducted an internal audit, an external auditor reviews all documentation (document review) and conducts an audit (main audit) to verify that the organization's activities comply with ISO/IEC 27001. After reviewing the result, the certification body issues a certificate with a validity of usually three years in case of a positive outcome. Within this period of validity, regular surveillance audits are conducted before a recertification audit takes place (Manders, 2015). While ISO 9001 certificates often apply to the entire organization, organizations often choose a specific part (such as the IT department or solely the data center) for which they seek certification, and hence ISO/IEC 27001 requires certified firms to issue an SoA in addition to their certificate.

Certification bodies can be accredited by accreditation bodies and have thus obtained formal attestation of their competence (ISO/IEC 17000) to certify firms against ISO/IEC 27001. Only certificates issued by a certification body accredited by accreditation bodies that are members of the International Accreditation Forum (IAF) are considered in the annual ISO Survey (2019a).

2.2. ISO/IEC 27001 adoption in Germany

According to the ISO Survey 2018 (issued in September 2019), there were 31,910 valid certificates worldwide as of 31st December 2018. Germany, with 1,057 valid ISO/IEC 27001 certificates and 2,003 sites, ranked fifth and sixth, respectively, in terms of the number of valid certificates and the number of sites worldwide (ISO, 2019a).

Since 2018, ISO has also asked participating certification bodies to distinguish between the number of certificates and sites (defined as "permanent location where an organization carries out work or a service" (ISO, 2019a)), which correspond to 59,934 sites globally at the end of 2018. This new methodology should be taken into account when comparing longitudinal data on ISO/IEC 27001 and other MS standards reported by ISO as part of the annual ISO Survey and might also explain why the number of valid ISO/IEC 27001 certificates in Germany initially declined in 2018. Figure 1, therefore, only depicts the number of valid certificates between 2006 and 2017, with an average increase of 32% p.a. over this period.

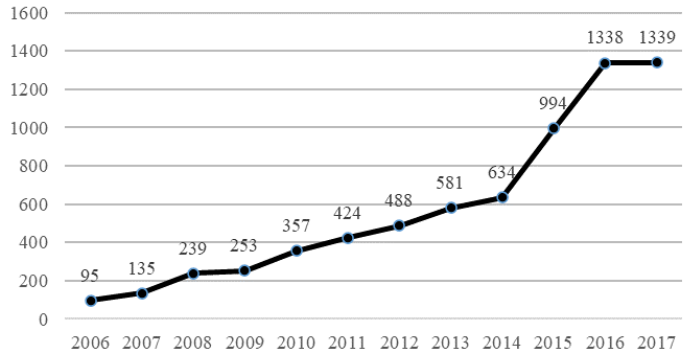

Figure 1. Number of valid ISO/IEC 27001 certificates in Germany, Source: ISO, 2019a

The ISO Survey (2019a) also contains the number of sectors covered by the certificates and recently also at the country level. However, this is only available for a limited set of valid certificates: in the case of Germany, for approximately 40%. According to this sector breakdown, 50% of all valid German ISO/IEC 27001 certificates were in the area of information technology, followed by other services with 23% and machinery and equipment with 5%.

2.3. Previous studies on ISO/IEC 27001

Despite the importance of information security, ISO/IEC 27001 has attracted comparable low interest from scholars (Fomin et al., 2008). A web mining-based analysis of 2,664 firms referencing ISO/IEC 27001 on their websites showed that firms that are larger and more innovative in terms of the number of employees are certified against ISO/IEC 27001 and most likely to provide ICT services (Mirtsch, Kinne, & Blind, 2020a), which is in line with the sector breakdown of the ISO (2019a) survey. By studying the diffusion of ISO/IEC 27001 on a global level using the number of valid certificates from the annual ISO survey from 2006 to 2017, (Mirtsch, Pohlisch, & Blind, 2020b) show that cross-cultural factors such as uncertainty avoidance and future orientation are driving factors alongside ICT development, drawing on macro-level data.

Van Wessel and de Vries (2013) used case studies in the United Kingdom and the Netherlands to investigate the reasons (motives) for implementing ISO/IEC 27001 and ISO/IEC 27002, the impact as well as the success factors. As a result, they found that firms adopt these standards for both internal reasons (increasing the quality of services offered (1), reducing the costs of security operations (2), and improving the company's risk profile (3)) and external reasons (meeting customer requirements (4), compliance with legal requirements (5), and marketing reputation/brand (6)). In terms of impact, the certification has led to new business opportunities but also to costs related to implementation (e.g., training), certification and consultancy, although the financial benefits apparently outweigh the costs incurred. Furthermore, adoption resulted in an improved quality of services offered, and even more so when companies obtained a certification rather than just implementing these standards (van Wessel & de Vries, 2013). Key success factors identified by van Wessel and de Vries (2013) include the involvement of business-driven departments (rather than only IT administration), senior management commitment, and adequate staff involvement in implementations. Furthermore, continuous improvement and clearly defined deviations, as well as previous experience with other MS standards, were factors that helped

companies to successfully implement and benefit from these two standards.

AbuSaad, Saeed, Alghathbar, and Khan (2011) investigated the implementation in Saudi Arabia, focusing on motives, obstacles, benefits, and lessons learned. The study showed that enhancing the organizations' security is the number one motivating factor for adopting ISO/IEC 27001, followed by competitive advantage. Surprisingly, customer requirements were not mentioned as a motivation. In terms of impact, participants cited changing organizational culture around information security, formalizing and giving visibility to information security, increasing trust in the organization, and validating and effectively managing business risks as the primary benefits. Identifying the organizations' assets was perceived as the primary obstacle for companies to implement ISO/IEC 27001, which is a prerequisite for determining the scope of certification (AbuSaad et al., 2011). Other obstacle factors included human resource (HR) or culture-related issues, as well as an unclear understanding of the content of the standard.

Another study conducted by Alshitri and Abanumy (2014) in Saudi Arabia explored the reasons for the low adoption of ISO/IEC 27001, focusing on public organizations. Building upon the findings of AbuSaad et al. (2011), they found that HR-related issues were the main barriers to ISO/IEC 27001 implementation, such as a lack of information security expertise and a lack of training as well as awareness programs. Of the 34 participating organizations, ten were certified to ISO/IEC 27001, and six organizations were implementing this standard but were not certified (Alshitri & Abanumy, 2014).

A third study conducted by Candiwan (2014) in Indonesia examined motivational factors (business continuity, tendering requirements, compliance with the role of industry and government regulation) as well as obstacles such as lack of top management support, lack of budget, and lack of qualified personnel.

A study conducted by Skopak and Sakanovic (2016) showed that out of 20 companies in Bosnia and Herzegovina, 85% of all firms contacted were familiar with ISO/IEC 27001 and 72% planned to adopt this standard in the future; however, only 5% (equivalent to 1 firm) were actually certified against ISO/IEC 27001 (Skopak & Sakanovic, 2016).

A more recent study conducted by Longras, Pereira, Cameiro, and Pinto (2018) surveyed 25 ISO/IEC 27001 certified Portuguese firms about the motives, difficulties, and limitations associated with this standard. The results showed that more than 90% of all ISO/IEC 27001 certified firms were also certified against ISO 9001, followed by nearly 40% against ISO 14001 and 20% against ISO/IEC 20000 (IT service management). Portuguese firms also cited HR issues (availability of qualified IT staff and allocation of roles), costs (most firms spent more than 50,000 Euros on the complete implementation and certification process), the interpretation of the standard's content, including the documentation effort, and the definition of the scope of certification as difficulties. Furthermore, adopting firms associate ISO/IEC 27001 certification to the General Data Protection Regulation (GDPR), where ISO/IEC 27001 certification apparently helps firms comply with the requirements set in the GDPR (Longras et al., 2018).

Another recent study from the Czech Republic draws a connection between a 2015 national law on cybersecurity and ISO/IEC 27001 certification revealing that regulatory compliance is the main reason for implementing this standard, in addition to protecting customers and their information (Svoboda & Horalek, 2018).

Table 1 provides an overview of previous surveys on the ISO/IEC 27001 adoption. In summary, all studies have shortcomings, firstly a very small number of participants.

This is mainly due to the relatively low number of valid ISO/IEC 27001 certificates in general – e.g., compared to other MS standards such as ISO 9001 or ISO 14001 – and specifically in these respective countries at the time the surveys were conducted.

Table 1. Previous surveys on ISO/IEC 27001 adoption

Year	Country	Sample size (certified)	# valid certificates *	Foci of the study	Reference
2011	Saudi-Arabia	8 (8)	13	Motives, barriers, impact lessons learned	AbuSaad et al. (2011)
2014	Saudi-Arabia	34 (10)	46	Barriers to implementation	Alshitri and Abanumy (2014)
2016	Bosnia and Herzegovina	20 (1)	10	Familiarity with standard, planned adoption	Skopak and Sakanovic (2016)
2018	Portugal	25 (25)	52	Barriers, costs, co-occurrences other standards	Longras et al. (2018)
2018	Czech Republic	33 (21)	463	Motives, relation to national cybersecurity law	Svoboda and Horalek (2018)

*In the respective year in terms of valid certificates according to the annual ISO Survey

Secondly, all these studies focusing on ISO/IEC 27001 lacked theoretical underpinning. This phenomenon was also observed in early diffusion studies on ISO 9001 for quality and ISO 14001 for environmental management, which were primarily descriptive, and only later published studies relied on theoretical concepts (Castka & Corbett, 2013).

However, to interpret empirical findings systematically, it is important to rely on theories from management or economics. This allows, firstly, to build on the findings in a structured way and, secondly, to transfer the findings to other areas and thus generalize one's own findings (Tuczek, Castka, & Wakolbinger, 2018).

2.4. Theoretical background on ISO/IEC 27001 adoption

For our study, we apply Rogers' (2003) diffusion of innovation theory. According to Rogers (2003), the decision on innovation diffusion is a five-stage process of a decision-making unit (e.g., an organization). In the case of ISO/IEC 27001 adoption starts with the organization gaining initial knowledge of this MS standard. This is followed by building an attitude, which also depends on how the organization perceives the characteristics of this innovation, including the expected benefits. After going through this persuasion stage, the organization decides either for or against this innovation, followed by an implementation of ISO/IEC 27001 in the case of the first decision. In the confirmation stage, the organizations evaluate the impact of the implementation of this standard and decide whether to continue or abandon this management system, possibly accompanied by certification.

As a specific type of innovation, Rogers (2003) introduced the concept of preventive innovations, which require action in the present to avoid unwanted consequences in the future. The adopting unit benefits from the preventive innovation only later, or perhaps not at all, if the unwanted event would not have occurred anyway (Rogers, 2002). This type of innovation oftentimes diffuses more slowly than non-preventive innovation, also due to the gap be-tween **k**nowledge, **a**ttitudes, and **p**ractice (KAP gap), where attitudes or values do not correlate with actual behavior. This situation may require intervention, e.g., by policymakers, to help close this gap (Rogers, 2003).

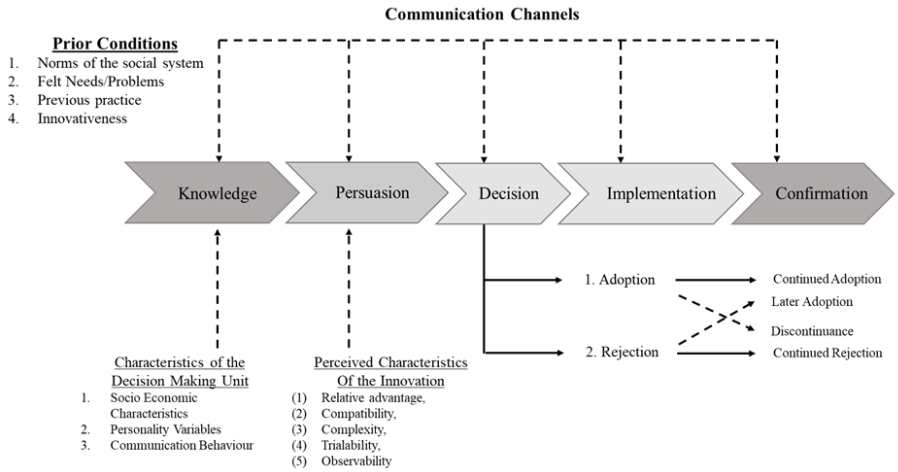

Figure 2. A Model of Five Stages in the Innovation Adoption Process, Source: Rogers (2003)

3. Methodology

3.1. Interviews and questionnaire design

To get an overview of relevant aspects, we conducted three in-depth interviews: with two firms certified to ISO/IEC 27001 and one certification body active in this field. In addition, this study builds upon seven transcribed interviews conducted as part of a thesis in the field of critical infrastructures: one representative of the German authority BSI (Federal Office for Information Security), five energy providers covered by the German IT Security Act, and one auditor of a certification body active in this field.

The outcome of these interviews, coupled with the results of previous studies from our literature research, enabled us to develop relevant research questions to analyze the ISO/IEC 27001 adoption in German organizations:

1. What is the awareness/ implementation and certification rate of this standard?
2. Why do organizations adopt this standard, and what are the reasons for non-adoption?
3. What is the perceived impact after ISO/IEC 27001 adoption?
4. Which barriers do adopters of ISO/IEC 27001 encounter during adoption?
5. Which measures are useful to increase ISO/IEC 27001 adoption?
6. Which criteria are relevant for organizations when selecting certification bodies?

The specific objective of the study is also to distinguish between organizations that implement ISO/IEC 27001 and those that seek additional certification.

The questionnaire was developed in an iterative process, integrating feedback from stakeholders involved in the design stage of the questionnaire, such as certification bodies and experts providing training on management systems. Finally, we conducted a pre-test with five firms of different sizes and industries. For this, we used the cognitive technique of the 'Think-Aloud Method" (Collins, 2003), and after the pre-test, we asked a series of questions on length and comprehensibility, which helped us to optimize the questionnaire accordingly.

3.2. Content of the questionnaire

The complete questionnaire contained 137 questions, of which only two were mandatory, and most were conditional.

Table 2 shows the different sections relevant to this study.

The questions were aimed at yes/no responses and multiple-choice on a 5-point Likert scale, where 1 stands for "not important" or "not agree at all" and 5 for "very important" or "fully agree," respectively.

Table 2. ISO/IEC 27001 Questionnaire Sections

Section	Content
1. Data about the organization	Industry affiliation (NACE) Size (employees, sales) International scope Innovativeness Standardization activity Participant's role in the organization
2. Use of management system standards	Certification/Implementation/Non-usage of MS standards Duration of certification
3. Non-adoption of ISO/IEC 27001	Awareness of ISO/IEC 27001 Reasons for non-adopting
4. Adoption of ISO/IEC 27001	Motivations Benefits Implementation difficulties Useful measures to increase the adoption rate
5. Conformity assessment of ISO/IEC 27001	Selection criteria for certification bodies

We first developed the items to measure the *motives* for implementing ISO/IEC 27001 and the *benefits* through literature research from previous studies on ISO/IEC 27001 (Candiwan, 2014), common MS standards such as ISO 9001 (Claver & Tari, 2008; Martinez-Costa, Choi, Martinez, & Martinez-Lorente, 2009; Nair & Prajogo, 2009) and ISO 14001 (Alberti, Caini, Calabrese, & Rossi, 2000; Alvarez-Garcia & del RioRama, 2016; Bellesi, Lehrer, & Tal, 2005; Murmura, Liberatore, Bravi, & Casolani, 2018) and ISO 50001 (Karcher, & Jochem, 2015), as well as on certification of German firms in general (Blind & Mangelsdorf, 2016).

We derived the items for the *barriers* from previous studies on ISO/IEC 27001 (AbuSaad et al., 2011; Alshitri & Abanumy, 2014; Candiwan, 2014) and based on our interviews (such as 'too few consulting services available'). Possible *measures to increase the adoption* of ISO/IEC 27001 were based on Rogers' (2002) recommendations to close the KAP gap, which refer to preventive innovations mentioned above and based on the recommendations resulting from our interviews.

To consider the *selection criteria of certification bodies*, we used items from previous studies (Castka et al., 2015; Poksinska, Dahlgaard, & Eklund, 2006). We added the aspect of the possibility of an integrated audit, which emerged during our interviews, as a possible important criterion.

3.3. Data collection

We collected the data as part of the newly set up QI-FoKuS initiative, where QI-FoKuS stands for "Quality Infrastructure – Research for Conformity Assessment and Safety". Therefore, a new recurring survey under this name was launched in autumn 2019. QI-FoKuS intends to create a long-term data basis to better understand the benefits of conformity assessment and accreditation and to identify future trends.

Potential participants were approached via multipliers. To recruit multipliers, our

project team made contact (by e-mail, telephone, and, upon request, in person) to:

- 30 industry associations of various branches and sizes from the network of our Federal Agency,
- 250 certification bodies listed in the dataset of the German accreditation body (https://www.dakks.de/content/akkreditierte-stellen-dakks),
- 100 representatives of Chambers of Commerce identified through a web search, and
- Other players in the field of quality infrastructure, such as the representative for ISO/IEC 27001 at the German standardization body DIN or the German Society for Quality (DGQ).

Through the multipliers, we sent out information on the survey, including the link to the online survey, and asked for publication in customers' or members' e-mail newsletters, on their websites, or in other customer communication media channels. To select participants, we used the key informant approach (Heckathorn, 1997; Lansing, Siegfried, Sunyaev, & Benlian, 2019) to ask quality managers or senior management to participate in our survey.

4. Survey findings

4.1. Sample description

Two hundred and forty-eight respondents started to fill out the questionnaire of our survey. Out of these, 134 completed the questionnaire in full, and 114 completed it in part, which corresponds to 46% of those who followed the hyperlinks to the survey. As a result of our break-off analysis, we decided to include only those participants who had completed Section 2 (Use of MS standards), which corresponds to 180 responses. Since we did not contact the organizations directly but through multipliers, we cannot estimate how many company representatives were exposed to our survey and, therefore, cannot calculate a response rate.

Table 3. Industry classes according to NACE for the full sample and the ISO/IEC 27001 sample

	All organizations		ISO/IEC 27001 adopters	
	n	%	n	%
Chemical and pharmaceutical Industry	37	20.6	8	15.
Other services	16	8.9	3	5.7
Electrical engineering	13	7.2	5	9.4
Mechanical engineering	13	7.2	3	5.7
Certification and testing	13	7.2	5	9.4
Metal production	11	6.1	2	3.8
Others	10	5.6	4	7.5
Human health /social work activities	8	4.4	2	3.8
ICT	8	4.4	8	15.1
All others	51	28.3	13	24.5
Total	n=180		n=53	

Overall, most of the respondents (n=99) were quality managers, followed by executives (n=30). Most of the respondents are active in the chemical & pharmaceutical industry (Table 3), which were contacted by the industry association via an e-mail newsletter explaining the disproportionally high number of responses. Regarding ISO/IEC 27001, most adopters belong to the ICT sector, which is in line with the sector breakdown of the ISO survey (2018) and a previous study based on web mining of firm websites (Mirtsch et al., 2020a).

Table 4. Company size by employees: full sample and the ISO/IEC 27001 sample

	1-9 (Micro)	**10-49 (Small)**	**50-249 (Medium)**	**250-499**	**500-999**	**>1000**
All (n=180)	20 (11%)	19 (10%)	41 (23%)	21 (12%)	11 (6%)	68 (38%)
ISO/IEC 27001	8 (15%)	6 (11%)	9 (17%)	3 (6%)	2 (4%)	24 (47%)

In terms of size, almost every second participant in the full sample and the sub-sample of ISO/IEC 27001 adopting organizations belonged to very large organizations (Table 4).

4.2. Use of management system standards

Comparing the ratio between the adoption and certification of organizations of the most popular management system standards (Table 5), ISO/IEC 27001 stands out for its low certification rate.

Table 5. Certification rates of selected MS standards

	Certified	Non-certified	Total adoption	% Certified of total adoption
ISO 9001 (n=150)	130	20	150	87
ISO 14001 (n=92)	75	17	92	82
ISO 450001 (n=69)	35	34	69	51
ISO 50001 (n=64)	48	16	64	75
ISO/IEC 27001 (n=53)	**20**	**33**	**53**	**38**
IATF 16949 (n=28)	21	7	28	75

While most organizations that have adopted the popular MS standards ISO 9001 and ISO 14001 have also been certified, less than every second organization obtained a certificate to ISO/IEC 27001. Out of these 20 ISO/IEC 27001 certified organizations, 43% were certified within the last three years, 38% between four and nine years ago, and only 10% more than ten years ago. Out of the non-certified ISO/IEC 27001 adopting organizations, 75% do not plan to become certified in the near future.

ISO/IEC 27001 adopting organizations have often also adopted another MS standard. Table 6 shows the co-occurrences differentiated by organizations that are certified to ISO/IEC 27001 and have implemented this MS standard without certification.

Table 6. Co-occurrences of ISO/IEC 27001 adopting organizations

	ISO/IEC 27001 adopting (n=20)		ISO/IEC 27001 non-adopting (n=33)	
	Certified	Non-certified	Certified	Non-certified
ISO 9001	12 (60%)	2 (10%)	24 (71%)	8 (24%)
ISO 14001	10 (50%)	1 (5%)	20 (59%)	6 (18%)
ISO 50001	7 (35%)	1 (5%)	10 (29%)	10 (29%)
ISO/IEC 20000	3 (15%)	1 (5%)	/	4 (12%)
ISO 45001	4 (20%)	4 (20%)	7 (21%)	14 (41%)
IATF 16949	4 (20%)	0	3 (9%)	6 (18%)
All other	6 (30%)	4 (20%)	10 (29%)	6 (18%)

For example, out of the 20 organizations certified against ISO/IEC 27001, 60% are also certified to ISO 9001 and 50% to ISO 14001, showing a high degree of co-occurrences between these MS standards. Organizations that have adopted ISO/IEC 27001 without certification showed even higher co-occurrence with ISO 9001

and ISO 14001, with 71% and 59%, respectively.

4.3. Non-adoption of ISO/IEC 27001

We asked those respondents of our survey who have not yet adopted ISO/IEC 27001 whether they are familiar with ISO/IEC 27001, which is the case for 71% (n=114) of all participants, while 29% of the participants have never heard of ISO/IEC 27001. For those respondents who are aware of ISO/IEC 27001, we asked whether they plan to adopt this standard in the near future or not. Table 7 shows that most organizations do not plan to adopt ISO/IEC 27001, and if they do, they tend to do so without certification.

In addition, we asked those organizations that do not plan to adopt ISO/IEC 27001 and for what reasons. It became clear that this is the case because neither customers, legislators, nor top management demand or consider it necessary to adopt ISO/IEC 27001 (Table 8).

Table 7. Planned adoption of ISO/IEC 27001, n=80

Yes, with certification	Yes, w/o certification	No	Don't know / NA
3 (4%)	13 (16%)	51 (64%)	13 (16%)

Table 8. Reasons for non-adoption of ISO/IEC 27001, n=64

Reason for non-adoption (multiple responses possible)	n=	%
My customers don't ask for it	27	42
The legislator does not require it	19	30
The top management sees no need or has rejected it	18	28
Not yet specifically thought about it	16	25
No personnel available for the introduction of this management system	15	23
IT is outsourced to a service provider	14	22
Costs outweigh the benefits	12	19
My company is not a potential attack victim	7	11
ISO 9001 covers information security sufficiently	7	11

4.4. Adoption of ISO/IEC 27001

In the following, we present the results for organizations that have adopted ISO/IEC 27001 in terms of motives, benefits, and barriers encountered. For this purpose, we asked the participants to rank the answers on a five-point Likert scale (1 does not apply, and 5 fully applies). We differentiated between organizations that are certified and those that have implemented ISO/IEC 27001 without being certified and show the mean score of each item in hierarchical order in Tables 9, 10, and 11. To test for significant differences between these two subgroups, we conducted Mann-Whitney-U Tests (MWU-Test, also referred to as Wilcoxon rank-sum test) as a nonparametric alternative to the t-test, which is suitable in the absence of normal distribution and which is based on ranks (Kruskal & Wallis, 1952).

Motives

The results presented in Table 9 show the motives for certified (ranked) and non-certified ISO/IEC 27001 adopting organizations, including the results of the subgroup comparison.

Ensuring legal compliance, followed by raising employees' awareness of information security of certified organizations among employees and reducing the risk of security breaches for the implementing organizations are the highest-ranked motives for adopting ISO/IEC 27001. In contrast, pressure arising from competitors that have already adopted this standard and have adopted ISO/IEC 27001 following a concrete occasion was at the bottom of the ranking.

Table 9. Motives for adopting ISO/IEC 27001

Motives	Certified	Non-certified	Subgroup comparison	
	mean (N)	mean (N)	MWU Test	p-value
Ensure legal compliance	**4.4 (14)**	**4.0 (25)**	1.11	0.29
Increase employees' IS awareness	4.1 (15)	3.5 (25)	2.45	0.12
Reduce risk of security breaches	3.9 (14)	3.9 (24)	0.12	0.73
Improve internal processes	3.6 (14)	2.8 (24)	0.86	0.35
Fulfill customer requirements	3.3 (13)	2.8 (24)	0.86	0.35
Fulfill top management requirement	3.2 (14)	2.9 (23)	0.35	0.55
Improve domestic market access	3.0 (12)	2.3 (23)	1.71	0.19
For marketing/reputational reasons	2.9 (14)	2.6 (23)	0.32	0.57
To be first to adopt ISO/IEC 27001	2.5 (13)	1.7 (24)	3.38	**0.07**
Improve international market access	2.4 (14)	2.0 (23)	0.34	0.56
Competitors adopted ISO/IEC 27001	2.3 (13)	1.7 (23)	2.92	**0.09**
In response to a concrete occasion	1.2 (13)	1.7 (22)	2.86	**0.09**

The results, furthermore, reveal that certified organizations are significantly more driven by competitive motives (either to be certified first or to catch up with competitors), and non-certified organizations adopting ISO/IEC 27001 are more motivated to implement this MS standard after a concrete occasion than certified organizations.

Benefits

The responses on the benefits of organizations that have adopted ISO/IEC 27001 are presented in Table 10.

Table 10. Benefits after adopting ISO/IEC 27001

Benefits	Certified	Non-certified	Subgroup comparison	
	mean (N)	mean (N)	MWU Test	p-value
Increased employees' information security awareness	**3.9 (15)**	3.8 (25)	0.28	0.60
Reduced risk of security breaches	3.8 (15)	4.1 (24)	0.81	0.37
Increases org. information security	3.7 (15)	**4.2 (25)**	1.08	0.30
Higher legal compliance	3.6 (15)	3.8 (24)	0.34	0.56
Better reputation	3.4 (14)	2.5 (24)	4.06	**0.04**
Reduction of security breach costs	2.9 (14)	2.7 (20)	0.32	0.57
Higher sales (related, e.g., to certificates)	2.8 (14)	1.8 (22)	5.01	**0.03**
Lower insurance premiums	1.9 (11)	2.3 (17)	0.49	0.48

Participants state that employees' information security awareness has increased while the risk of security breaches has decreased. Comparing the subgroups reveals that certified organizations benefit more from a better reputation and increased revenues related to the proof of adoption and the corresponding certification than non-certified organizations.

Obstacles

Adopting organizations perceived the time invested as the greatest difficulty. This difficulty is followed by the need for support from external consultants for certified organizations – supposedly also related to the high complexity of the standard's content and the lack of internal expertise of the IT personnel. In terms of the difficulties encountered in adopting ISO/IEC 27001, there are significant differences between

both subgroups, with low motivation of employees and lack of top management commitment being a greater difficulty for non-certified organizations than for certified organizations (Table 11).

Table 11. Encountered difficulties related to ISO/IEC 27001 adoption

Difficulties encountered	Certified	Non-certified	Subgroup comparison	
	mean (N)	mean (N)	MWU Test	p-value
High time investment	**3.4 (14)**	**3.6 (23)**	0.54	0.46
External consulting needed	3.2 (14)	2.7 (21)	0.93	0.33
High cost investment	2.9 (14)	3.0 (23)	0.18	0.67
Complexity of standard content	2.9 (14)	2.8 (23)	0.03	0.86
Lack of internal expertise (IT personnel)	2.4 (14)	2.9 (23)	0.85	0.36
Difficult definition of scope	2.3 (14)	2.3 (22)	0.11	0.74
Uncertainty about benefit	2.3 (14)	2.5 (23)	0.22	0.64
Few consulting services available	1.9 (12)	2.6 (19)	2.13	0.14
Little motivation of employees	1.9 (14)	2.6 (23)	2.91	**0.09**
Missing commitment of top management	1.5 (14)	2.3 (22)	2.94	**0.09**

Measures to increase the adoption of ISO/IEC 27001

We asked participants how they rated the concrete measures we proposed and asked about their usefulness on a 5-point Likert scale (1=not useful at all and 5=very useful). Most of the measures were rated as useful. However, as shown in table, the results reveal significant differences when comparing the two subgroups. While certified organizations rate that the legislator and customer require adoption as high(er), non-certified organizations rate these measures as useful to a lesser extent. Both subgroups suggest providing financial support alongside implementation guides and practical training for employees. Support for the exchange of best practices is also perceived as highly useful by both subgroups, especially by the certified organizations.

As a final item of this section, we asked the participants if there had been an incident in their organization that had affected the confidentiality, integrity, or availability of important information.

Table 12. Measures to increase the adoption of ISO/IEC 27001

Usefulness of measures to increase the adoption	Certified	Non-certified	Subgroup comparison	
	mean (N)	mean (N)	MWU Test	p-value
Customer requires adoption	**4.5 (12)**	3.5 (23)	4.34	**0.02**
Provide practical training for employees	4.4 (13)	3.6 (25)	4.14	**0.04**
Legislator requires adoption	4.2 (13)	3.3 (26)	4.83	**0.03**
Support best practice exchange	4.2 (13)	3.5 (26)	3.47	**0.06**
Increase awareness of ISO/IEC 270011	4.1 (14)	3.7 (26)	1.45	0.23
Financial support for consulting services	4.0 (13)	3.8 (25)	0.55	0.46
Financial support for certification expenses	3.9 (13)	3.8 (25)	0.29	0.59
Implementation guidance, esp. for SMEs	3.8 (13)	**4.2 (24)**	0.36	0.55

Table 13. Previous information security breaches

Incident happened	Yes	No	Don't know	No answer	Total
All participants	44 (24%)	90 (50%)	27 (15%)	19 (11%)	180
ISO/IEC 27001 adopters	16 (30%)	18 (34%)	8 (15%)	11 (21%)	53

The results in Table 13 reveal that organizations that have adopted ISO/IEC 27001 (with or without certification) have had fewer security breaches in the past. Also noteworthy – when considering this group – is the higher number of non-responses compared to the full sample.

4.5. Selection criteria for certification bodies of ISO/IEC 27001

Table 14 shows the mean scores of the certified organizations and the reasons for choosing their certification bodies, including the number of participants who chose the lowest and highest scores (1=not important and 5=very important).

Table 14. Selection criteria for certification bodies (Ranking)

Selection criteria (n=12-13)	mean	# Participants lowest rating	# Participants highest rating
Certification body is accredited	3.9	0	12
Possibility of an integrated audit for multiple management systems	3.7	3	7
Competence of auditors	3.7	1	8
Special industry knowledge	3.3	1	5
Reputation of certification body	3.2	0	5
Low fees of certification bodies	3.2	2	3
Fast and easy procedures	3.0	0	7
International orientation of certification body	3.0	0	7
Low travel and other expenses of the auditor	2.8	1	3
Top management guideline	1.5	8	0
Recommendation of other	1.4	9	0
Customer request	1.4	11	1

Accreditation of certification received the highest scores in terms of importance, followed by the possibility of an integrated audit for multiple management systems. In contrast, external reasons such as customer requests, recommendations from others, or top management were of less importance to the organizations when choosing their certification bodies.

5. Discussion of the findings

For our discussion, we apply Rogers' (2003) five-stage model as described in Section 2.4.

Prior conditions:

The *analysis of the motives* for adopting ISO/IEC helps to investigate the felt needs and problems as 'prior conditions', according to Rogers (2003). Organizations perceive the need to increase legal certainty and prevent security breaches, which motivates them to adopt ISO/IEC 27001 while raising awareness among their employees. Institutional pressure exerted by competitors appears to be less motivating and less responsive to customers' needs. These findings are in line with the previous studies discussed above. Furthermore, the adoption of ISO/IEC 27001 is spurred by the previous adoption of another MS standard, such as ISO 9001, as indicated by the high co-occurrence (Table 6), which has also been shown before for ISO 14001 and ISO 9001 (Delmas & Montiel, 2008).

Knowledge stage

To consider adopting ISO/IEC 27001, organizations first need to be aware of this MS standard. Almost one-third of the respondents to our survey were not aware of this MS standard. It is, therefore, recommended to launch initiatives (e.g., led by standardization bodies, certification bodies, consultants, or governmental authorities) to raise awareness of information security, the need for an information security MS and ISO/IEC 27001. This aspect was also scored highest when participants were asked about suitable measures to increase the adoption of ISO/IEC 27001 among German organizations.

Persuasion stage

Following Rogers' (2003) innovation adoption model, adopting units evaluate relative advantage, compatibility, complexity, trialability, and observability to develop a favorable or unfavorable attitude towards adopting ISO/IEC 27001. Unknown benefits may also influence the persuasion stage, as the benefits are not easily observable, which is in line with the findings of previous studies showing that the (immediate) financial impact on the performance of firms that have adopted ISO/IEC 27001 is not measurable (Hsu et al., 2016). This finding also supports our classification of the ISO/IEC 27001 adoption as a *preventive innovation*, which often shows no immediate effect because it prevents an adverse event (Roger, 2003).

An analysis of the perceived barriers shows that adopting organizations face downsides in terms of time and cost investment and the need for external consultancy. Furthermore, the complexity and trialability are perceived as problematic, which is reflected in the high scores for the complexity of the content of the norm and the need for external consultancy for implementation, which might discourage organizations from implementing this MS standard without (costly) external guidance.

Decision/implementation stage

Within the sample, we observed that almost 30% of all organizations have decided to adopt ISO/IEC 27001. Within this group, only 38% have obtained a certificate, which is relatively low compared to other MS standards (Table 5). This finding indicates that ISO/IEC 27001 differs significantly from other MS standards in the implementation stage when it comes to seeking independent attestation of conformity. Out of the more than 70% of non-adopters of ISO/IEC 27001 who are aware of this standard, most participants do not plan to adopt ISO/IEC 27001 in the future, and if they do, most of them plan to adopt ISO/IEC 27001 without certification, again indicating the lower prominent role of certification for this MS standard. The reasons for rejection (analyses of non-adopters) are mainly due to the lack of external (e.g., customers and legislators) and internal (top management) demand for the adoption of this standard.

Confirmation stage

Once ISO/IEC 27001 has been implemented, organizations evaluate the benefits to either substantiate or reverse their decision. Most organizations that adopt the standard benefit from increased employees' awareness and have been able to minimize the risk of security breaches and overall information security in their organizations. In most cases, apart from certain organizations falling under the IT Security Act, obtaining an ISO/IEC 27001 is voluntary for organizations. However, our findings show that organizations seeking certification benefit more from a better reputation and increased sales than organizations adopting this standard without seeking additional certification, which may be related to the signaling effect of certificates.

In the context of our study, only one organization decided to abandon certification. However, most organizations have only recently adopted this standard (43% of our sample had been certified for

less than three years), which does not allow for far-reaching conclusions in terms of the confirmation stage.

6. Conclusion, limitations, and future research

This paper examines the major roles of the factors (motives, benefits, barriers, and measures to be overcome) for ISO/IEC 27001 adoption in Germany. The findings of this study have provided further understanding of the motives and benefits of adopting ISO/IEC 27001, including the barriers and ways to overcome them. The results suggest that organizations are mainly driven by preventive motives and confirm previous theoretical considerations that ISO/IEC 27001 helps to prevent possible events rather than (directly) benefiting economically. Commercial aspects such as increased turnover or reputation gain are therefore less relevant, which also does not allow quantification of the impact of ISO/IEC 27001. This critical aspect has also been recognized by the standards developing organizations, which have published a guideline on the organizational economics of information security management (ISO/IEC TR 27016:2014). This guideline aims to enable economic decisions to be made by presenting theoretical examples of business case calculations based, for example, on minimizing the negative impacts of identified risks and meeting stakeholder commitments and expectations. However, the usefulness of this guideline has not yet been sufficiently discussed scientifically and could be the subject of future research.

The analysis of ISO/IEC 27001 non-adopting organizations and the promising measures to increase the adoption of ISO/IEC 27001 indicates that institutional pressure needs to be increased to significantly push the adoption rate of this MS standard. This can be done either by regulators mandating the standard (as is already the case for some organizations such as energy providers under the NIS directive) or by customers, e.g., along the supply chain, e.g., introducing ISO/IEC 27001 into quality assurance agreements alongside ISO 9001 and ISO 14001. However, organizations must be able to remain competitive, especially in a global context. Implementing an information security MS is already costly and time-intensive, especially if it covers large parts of the organization rather than solely, e.g., the data servers. Obtaining a certificate requires even more investment. Therefore, regulators, as well as customers, should carefully consider whether certification is required or whether a self-declaration of conformity in addition to a specific statement of applicability may be sufficient. In cases where adoption is not required (following a risk-based approach), stakeholders could also actively promote the further adoption of ISO/IEC 27001, whereby we hope to present possible measures that were rated as highly useful by the participants of our survey.

As far as limitations are concerned, conducting a survey is particularly helpful in identifying underlying motives, although it does raise four problematic issues. Firstly, surveys often suffer from positive response bias, as has already been shown exemplarily in the case of ISO 9001 (Manders, 2015). This is all the more the case when quality managers fill out questionnaires (de Vries & El Osrouti, 2019), which was frequently the case in our study. Secondly, we did not operationalize the impact variables in quantifiable terms (such as concrete figures on security breaches before and after the implementation of ISO/IEC 27001). We did this for reasons of simplicity and confidentiality and, therefore, measured perception of impact rather than the impact itself.

Thirdly, our survey suffers from a lack of representativeness. Due to our multiplier approach, we had to rely on others to forward the link to their customers and members, as we could not draw a

representative picture of ISO/IEC 27001 adoption in Germany. Finally, our study is characterized by a small sample size. Despite great efforts to mobilize multipliers, the number of participants was rather moderate, with 134 fully completed questionnaires and 46 incomplete (usable) questionnaires. The low response rate is in line with previous studies on information security research, which reveals that it is difficult for researchers to gain data on information security practices. Due to this sensitive issue, firms may be unwilling to respond to mass mailings as a survey instrument (Kotulic & Clark, 2004).

As a contribution to theory, we aim to contribute to the adoption of MS literature by shedding some light on an MS that was ranking third according to ISO (2019a) but has gained little attention from scholars in the past (Fomin et al., 2008). Furthermore, we hope to enrich the adoption of innovation literature by classifying the adoption of ISO/IEC 27001 as a preventive innovation, according to Rogers (2002), allowing future research to build on this proposed classification.

Acknowledgment: The author would like to thank her BAM colleagues Dr. Claudia Koch, Dr. Gabriele Dudek, Dr. Tilman Denkler, Michael Franke, and Jonas Haas for their work on the survey, as well as Petra Keitzl for project management and Susanne Stobbe for language editing and proofreading. The author would also like to thank Prof. Dr. Knut Blind from the Technische Universität Berlin for his collaboration on the QI-FoKuS initiative, and finally acknowledges the valuable suggestions of two anonymous reviewers.

References:

AbuSaad, B., Saeed, F. A., Alghathbar, K., & Khan, B. (2011, 5th December to 7th December). *Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned*, Perth Western Australia.

Accenture and Ponemon Institute. (2019, 6th March). The cost of cybercrime. *Ninth annual cost of cybercrime study. Unlocking the value of improved cybersecurity protection.* Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Alberti, M., Caini, L., Calabrese, A., & Rossi, D. (2000). Evaluation of the costs and benefits of an environmental management system. *International Journal of Production Research, 38*(17), 4455-4466. https://doi.org/10.1080/00207540050205226

Alshitri, K. I., & Abanumy, A. N. (2014, 6th May to 9th May). *Exploring the Reasons Behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia*, Seoul, South Korea.

Alvarez-Garcia, J., & del RioRama, M. D. (2016). Sustainability and EMAS: Impact of Motivations and Barriers on the Perceived Benefits from the Adoption of Standards. *Sustainability, 8*(10). https://doi.org/10.3390/su8101057

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610-613. DOI: 10.1126/science.1130992

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., et al. (2017). *Understanding the Mirai Botnet.* Paper presented at the USENIX Security Symposium, Vancouver, BC.

Bellesi, F., Lehrer, D., & Tal, A. (2005). Comparative advantage: The impact of ISO 14001 environmental certification on exports. *Environmental Science & Technology, 39*(7), 1943-1953. https://doi.org/10.1021/es0497983

Blind, K., & Mangelsdorf, A. (2016). Zertifizierung in deutschen Unternehmen–zwischen Wettbewerbsvorteil und Kostenfaktor. In *Zertifizierung als Erfolgsfaktor* (pp. 23-32): Springer. DOI: 10.1007/978-3-658-09701-1_3

Bundesnetzagentur. (2018). IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz. Retrieved from https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf;jsessionid=B7B3F268790093AC5A473CEAECBDA6FF?__blob=publicationFile&v=4

Candiwan, C. (2014). *Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia.* Paper presented at the Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security, Kuala Lumpur, Malaysia.

Castka, P., & Corbett, C. J. (2013). Management systems standards: diffusion, impact and governance of ISO 9000, ISO 14000, and other management standards. *Foundations and Trends® in Technology, Information and Operations Management, 7*(3–4), 161-379. http://dx.doi.org/10.1561/0200000042

Castka, P., Prajogo, D., Sohal, A., & Yeung, A. C. (2015). Understanding firms′ selection of their ISO 9000 third-party certifiers. *International Journal of Production Economics, 162*, 125-133. https://doi.org/10.1016/j.ijpe.2015.01.012

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer, 44*(4), 91-93. DOI: 10.1109/MC.2011.115

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), e1211. https://doi.org/10.1002/widm.1211

Claver, E., & Tari, J. J. (2008). The individual effects of total quality management on customers, people and society results and quality performance in SMEs. *Quality and Reliability Engineering International, 24*(2), 199-211. https://doi.org/10.1002/qre.885

Collins, D. (2003). Pretesting survey instruments: an overview of cognitive methods. *Quality of life research, 12*(3), 229-238. https://doi.org/10.1023/A:1023254226592

de Vries, H. J., & El Osrouti, F. (2019). *Impact studies on standards and standardisation - Looking back and moving forward.* Paper presented at the EURAS 2019, Rome, Italy.

Delmas, M., & Montiel, I. (2008). The diffusion of voluntary international management standards: Responsible Care, ISO 9000, and ISO 14001 in the chemical industry. *Policy Studies Journal, 36*(1), 65-93. https://doi.org/10.1111/j.1541-0072.2007.00254.x

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2019). General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations' Compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 94-109). Springer, Cham. DOI: 10.1007/978-3-030-27813-7_7

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92-100.

Fomin, V. V., de Vries, H. J., & Barlette, Y. (2008). *ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption*, Nice, France.

Heckathorn, D. D. (1997). Respondent-driven sampling: a new approach to the study of hidden populations. *Social problems, 44*(2), 174-199. https://doi.org/10.2307/3096941

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. In 2016 *49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE.

ISO. (2019a). *The ISO Survey of Management System Standard Certifications 2018*. Retrieved from https://www.iso.org/the-iso-survey.html

ISO. (2019b). ISOfocus January-February 2019. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/en/2019/ISOfocus_132/ISOfocus_132_en.pdf

Karcher, P., & Jochem, R. (2015). Success factors and organizational approaches for the implementation of energy management systems according to ISO 50001. *The TQM Journal, 27*(4), 361-381. https://doi.org/10.1108/TQM-01-2015-0016

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607. https://doi.org/10.1016/j.im.2003.08.001

Kruskal, W. H., & Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. *Journal of the American statistical Association, 47*(260), 583-621. DOI: 10.1080/01621459.1952.10483441

Lansing, J., Siegfried, N., Sunyaev, A., & Benlian, A. (2019). Strategic signaling through cloud service certifications: comparing the relative importance of certifications' assurances to companies and consumers. *The Journal of Strategic Information Systems, 28*(4), 101579. https://doi.org/10.1016/j.jsis.2019.101579

Longras, A., Pereira, T., Cameiro, P., & Pinto, P. (2018). On the track of ISO/IEC 27001: 2013 implementation difficulties in Portuguese organizations. In *2018 International Conference on Intelligent Systems (IS)* (pp. 886-890). IEEE.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019, June). How ISO 27001 can help achieve GDPR compliance. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Manders, B. (2015). *Implementation and Impact of ISO 9001* (Vol. Ph.D.). Rotterdam: (No. EPS-2014-337-LIS). Erasmus Research Institute of Management – ERIM Ph.D. Series.

Mansfield-Devine, S. (2018). Critical infrastructure: understanding the threat. *Computer Fraud & Security, 2018*(7), 16-20. https://doi.org/10.1016/S1361-3723(18)30065-4

Martinez-Costa, M., Choi, T. Y., Martinez, J. A., & Martinez-Lorente, A. R. (2009). ISO 9000/1994, ISO 9001/2000 and TQM: The performance debate revisited. *Journal of Operations Management, 27*(6), 495-511. https://doi.org/10.1016/j.jom.2009.04.002

Mirtsch, M., Kinne, J., & Blind, K. (2020a). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management, 68*(1), 87-100. DOI: 10.1109/TEM.2020.2977815

Mirtsch, M., Pohlisch, J., & Blind, K. (2020b, 15.06-17.06.2020). *Exploring the international diffusion of the information security management system standard ISO/IEC 27001: exploring the role of culture.* Paper presented at the Twenty-Eighth European Conference on Information Systems (ECIS2020) A Virtual AIS Conference.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3), 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Murmura, F., Liberatore, L., Bravi, L., & Casolani, N. (2018). Evaluation of Italian Companies' Perception About ISO 14001 and Eco Management and Audit Scheme III: Motivations, Benefits and Barriers. *Journal of Cleaner Production, 174*, 691-700. https://doi.org/10.1016/j.jclepro.2017.10.337

Nair, A., & Prajogo, D. (2009). Internalisation of ISO 9000 standards: the antecedent role of functionalist and institutionalist drivers and performance implications. *International Journal of Production Research, 47*(16), 4545-4568. https://doi.org/10.1080/00207540701871069

Poksinska, B., Dahlgaard, J. J., & Eklund, J. A. (2006). From compliance to value-added auditing–experiences from Swedish ISO 9001: 2000 certified organisations. *Total Quality Management & Business Excellence, 17*(7), 879-892. https://doi.org/10.1080/14783360600595294

Rogers, E. M. (2002). Diffusion of preventive innovations. *Addictive behaviors, 27*(6), 989-993. https://doi.org/10.1016/S0306-4603(02)00300-3

Rogers, E. M. (2003). *Diffusion of innovations*. New York, NY: Free Press.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *The Information Management Journal 39*(4), 60-66.

Skopak, A., & Sakanovic, S. (2016). *Adoption of Standard for Information Security ISO/IEC 27001 in Bosnia and Herzegovina.* Paper presented at the International Conference on Economic and Social Studies (ICESoS) Sarajevo, Bosnia and Herzegovina.

Svoboda, T., & Horalek, J. (2018). Analysis of the information security management in Czech Republic. *Advanced Science Letters, 24*(11), 8562-8566. https://doi.org/10.1166/asl.2018.12303

Tuczek, F., Castka, P., & Wakolbinger, T. (2018). A review of management theories in the context of quality, environmental and social responsibility voluntary standards. *Journal of Cleaner Production, 176*, 399-416. https://doi.org/10.1016/j.jclepro.2017.12.161

Tunçalp, D. (2014). Diffusion and Adoption of Information Security Management Standards Across Countries and Industries. *Journal of Global Information Technology Management, 17*(4), 221-227. https://doi.org/10.1080/1097198X.2014.982454

Uwizeyemungu, S., & Poba-Nzaou, P. (2015, 9-11 Feb. 2015). Understanding information technology security standards diffusion: An institutional perspective. In 2015 *International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 5-16). IEEE.

van Wessel, R., & de Vries, H. J. (2013). Business impact of international standards for information security management. Lessons from case companies. *Journal of ICT Standardization, 1*, 25-40. https://doi.org/10.13052/jicts2245-800X.122

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Mona Mirtsch
Bundesanstalt für Materialforschung
und -prüfung (BAM),
Berlin, Germany;
Technische Universität Berlin,
Chair of Innovation Economics
mona.mirtsch@bam.de
ORCID 0000-0002-2036-4579