Received 1 September 2020
Revised 16 December 2020
Accepted 29 January 2021

The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda

Giovanna Culot, Guido Nassimbeni, Matteo Podrecca and Marco Sartor

Polytechnic Department of Engineering and Architecture, University of Udine, Udine, Italy

Abstract

Purpose – After 15 years of research, this paper aims to present a review of the academic literature on the ISO/IEC 27001, the most renowned standard for information security and the third most widespread ISO certification. Emerging issues are reframed through the lenses of social systems thinking, deriving a theory-based research agenda to inspire interdisciplinary studies in the field.

Design/methodology/approach – The study is structured as a systematic literature review.

Findings – Research themes and sub-themes are identified on five broad research foci: relation with other standards, motivations, issues in the implementation, possible outcomes and contextual factors.

Originality/value – The study presents a structured overview of the academic body of knowledge on ISO/IEC 27001, providing solid foundations for future research on the topic. A set of research opportunities is outlined, with the aim to inspire future interdisciplinary studies at the crossroad between information security and quality management. Managers interested in the implementation of the standard and policymakers can find an overview of academic knowledge useful to inform their decisions related to implementation and regulatory activities.

Keywords ISO/IEC 27001, ISO 27001, IEC 27001, Information security, Systematic literature review, Management system standards

Paper type Literature review

1. Introduction

Economy and society are becoming increasingly data-driven, yet most of the debate across managerial disciplines has been focusing on how to extract value from data – e.g. through business model innovation (Spiekermann and Korunustovska, 2017; Hagiu and Wright, 2020; Iansiti and Lahkani, 2020) – rather than protecting what seems to be a crucial asset today: information. Emerging technologies, platform-based business models and the spread of smart working practices are multiplying the number of entry points in computer networks and thus their vulnerability (Hooper and McKissack, 2016; Lowry *et al.*, 2017; Corallo *et al.*, 2020). Holistic approaches are required to face the increasingly complex challenge of information system security (ISS): substantial managerial focus is needed to balance trade-off decisions between protection and legal compliance, on the one hand, and cost and operational agility, on the other

The authors acknowledge the financial support of the Regione Autonoma Friuli-Venezia Giulia (Specifc Program 89/2019 - Fondo Sociale Europeo 2014/2020) and the POR FESR project G4Mob Regione Veneto.

The TQM Journal
Vol. 33 No. 7, 2021
pp. 76-105
Emerald Publishing Limited
1754-2731
DOI 10.1108/TQM-09-2020-0202

(e.g. Vance *et al.*, 2020; D'Arcy and The, 2019; Burt, 2019; Antonucci, 2017). In spite of an increasing practitioners' interest in the topic (e.g. Gartner, 2018; McKinsey, 2019), ISS is still perceived in academia as an essentially technical topic (Aguliyev *et al.*, 2018; Lezzi *et al.*, 2018; Sallos *et al.*, 2019).

Over the years, ISS standards and frameworks have been playing a pivotal role in the dissemination of now much-needed holistic – technical, organizational and managerial – approaches (Von Solms, 1999; Ernst and Young, 2008). Among them, ISO/IEC 27001 is probably the most renowned one, being the third most widespread ISO certification worldwide, following ISO 9001 and ISO 14001 (ISO, 2019). The standard was designed and published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 as an evolution of BS 7799. It "[. . .] specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization"; the requirements "[. . .] are generic and are intended to be applicable to all organizations, regardless of type, size or nature" (ISO/IEC 27001:2013). Several leading organizations ask their business partners to be ISO/IEC 27001 certified – e.g. Netflix for post-production partners – and widespread publicity has been given over the years to the attainment of ISO/IEC 27001 certification by prominent technological providers, including Apple Internet Services, Amazon Web Services, GE Digital, several Microsoft business units and – more recently – Facebook's Workplace (e.g. Venters and Whitley, 2012).

Overall, the literature on ISS standards is marked by ongoing concerns about their efficacy and validation (e.g. Siponen and Willison, 2009; Silva *et al.*, 2016; Niemimaa and Niemimaa, 2017). After 15 years of scientific research on ISO/IEC 27001 and in light of its growing popularity, we believe that it is time for academia to assess how these fundamental concerns have been addressed so far with respect to this specific standard and to question related research prospects against a context characterized by an ever-increasing connectivity and digitalization. We believe that more interdisciplinarity in the study of ISS standards is necessary considering how – according to many observers (e.g. Blackburn *et al.*, 2020; The Economist, 2020) – the COVID-19 health crisis is expected to accelerate the role of digital technologies in the business environment as well as in daily life.

This study moves in this direction by developing a systematic literature review on ISO/IEC 27001. As Webster and Watson (2002) point out, a systematic approach is the starting point for advancing research in a given field, laying strong foundations for future studies. Differently than previous reviews, our work does not focus on a specific topic in the ISO/IEC 27001 research – i.e. diffusion in Barlette and Fomin (2010) and technical approaches in Ganji *et al.* (2019) – but aims at providing a comprehensive synthesis of the debate in the field. The results are read through the lenses of social systems thinking to formulate a theory-based research agenda to inspire future studies at the intersection between information systems (IS) and managerial disciplines, including quality management. In line with renewed calls for theory-grounded research (e.g. Breslin *et al.*, 2020; Post *et al.*, 2020) and following Seuring *et al.* (2020) considerations, we extend the reach of three specific system theoretical approaches to the study of ISO/IEC 27001. As we leverage theoretical perspectives never applied for ISO/IEC 27001 and not common in research on other voluntary standards (Sartor *et al.*, 2016, 2019; Orzes *et al.*, 2018), we trust that our effort can stimulate the academic debate by integrating new streams of theory and allowing scientific exchange beyond what is already present.

Under this premise, this study delivers two main contributions to the literature. First, we present and organize the body of knowledge on ISO/IEC 27001 across several research streams and topics, providing a comprehensive overview targeted at scholars from different backgrounds. Second, we add a novel analytical perspective to the research on ISO/IEC 27001 through the lenses of social systems thinking, which may apply to the study of other voluntary standards as well.

Our paper has also substantial practical implications. The results of the literature review provide managers with an overall picture of the knowledge created over the years by academic research on the ISO/IEC 27001 standard, including relevant elements to consider in pursuing, implementing and managing the certification. Moreover, policymakers may find pertinent perspectives that inform their decisions regarding public support to the diffusion process of the certification. The paper actually shifts the focus of the debate from firm-level implementation of ISO/IEC 27001 to a system-level perspective, urging decision-makers to consider ISS needs and practices in the broader business environment in which organizations exchange data and information.

The remainder of the paper is structured as follows. The next section illustrates the methodology adopted for the literature review. Thereafter, we present the descriptive characteristics of the contributions included in our analysis. The results of the thematic coding are presented in two main sections. Next, the discussion revolves around the main issues and current knowledge gaps, followed by the formulation of a theory-based research agenda. We conclude outlining the contributions of our research.

2. Review approach

Management system standards are inherently multi-dimensional phenomena that can be analyzed according to several research perspectives (Uzumeri, 1997; Heras-Saizarbitoria and Boiral, 2013); we opted, thus, for a systematic approach to the literature review to minimize the implicit biases of the researchers involved in the identification, selection and coding of papers. The approach – following the guidelines of Tranfield *et al.* (2003), Rousseau *et al.* (2008) and Seuring and Gold (2012) – is in line with previous studies on other voluntary standards (e.g. Sartor *et al.*, 2016; Boiral *et al.*, 2018).

The review protocol was structured to meet the following research objectives: (1) provide a comprehensive overview of the literature on ISO/IEC 27001; (2) classify themes, sub-themes and type of evidence; (3) underscore recurring patterns, conflicting results and unexplored research areas.

The first step was the identification of the literature. We performed a formal search on multiple online scientific databases: Elsevier's Scopus and Science Direct, Clarivate's Web of Science, EBSCO Business Source Complete and EconLit, ProQuest's Social Sciences, JSTOR, Wiley Online Library and Emerald Insight. The keywords were selected to include different spellings of the standard – i.e. "ISO270**," "ISO 270**," "IEC 270**," "IEC270**," "ISO/IEC 270**," "ISO / IEC 270**," "ISO / IEC270**" and "ISO/IEC270**" – using the operator OR between the terms. The research on title, abstract and keywords covered the period until November 2020. We included only peer-reviewed journal articles, books and book chapters written in English for a total of 537 unique records.

As a second step, abstracts and full texts were screened for their fit with the objectives of the study. Two researchers were involved independently. We excluded contributions that: (1) referred to other standards and (2) merely mentioned the ISO/IEC 27001 without a structured analysis or discussion. We included both theoretical and empirical contributions that: (1) focused specifically on ISO/IEC 27001, (2) analyzed ISO/IEC 27001 together with other standards, (3) discussed ISS/cybersecurity issues at large with explicit reference to ISO/IEC 27001. This way, 116 contributions were pre-selected, their content was further analyzed and their references enabled the identification of other works through a forward/backward citation analysis (Webster and Watson, 2002). This process led to a final list of 96 contributions.

The third step in the process was to analyze the material to capture thematic trends, meanings, arguments and interpretations (Mayring, 2000; Duriau *et al.*, 2007). Books and book chapters were classified based on year and authors' affiliation/geography. Journal

articles were classified based on year, publication outlet, disciplinary area, authors' affiliation/geography, methodology and underpinning theory (if any).

Thereafter, we performed a content analysis on journal articles following Seuring and Gold's (2012) methodological recommendations. The coding categories and main themes included in Figure 1 were defined deductively, drawing from previous literature reviews on other standards and frameworks (e.g. Stevenson and Barnes, 2002; Heras-Saizarbitoria and Boiral, 2013; Manders *et al.*, 2016; Boiral *et al.*, 2018) and refined inductively through iterative cycles during the coding process. The specific sub-themes were identified inductively, aggregating the arguments emerging from the content analysis by similarity.

The coding activity was conducted independently by two researchers (Duriau *et al.*, 2007). Each researcher mapped on an Excel spreadsheet the recurrence of the sub-themes in the papers, coding whether the evidence was of a conceptual (C) or rather empirical (E) nature. In addition, the researchers noted some relevant passages for each paper/sub-theme to facilitate the interpretation of the results. The few instances of disagreement were resolved through formal discussion.

Finally, the results of the coding activity were examined. We calculated the descriptive characteristics of the papers included in the review and the proportion of studies addressing each sub-theme. A synthesis of the relevant passages reported in the literature for each sub-theme was also prepared and discussed within the research team. The following sections illustrate the outcomes of our analysis.

As books and book chapters are practitioner-oriented and rarely peer-reviewed, we did not include them in the scientific coding and present them in a standalone subsection. The coding process followed the same methodological approach as journal articles.

3. Characteristics of the literature

The classification of the 96 contributions brings to light how the debate on ISO/IEC 27001 developed within the scientific and practitioners community. The main findings are summarized in Figure 2 and clarified in the following paragraphs.

The first contribution on the topic was published in 2005, the same year of the release of ISO/IEC 27001. Since then, the average number of contributions is six per year, with an

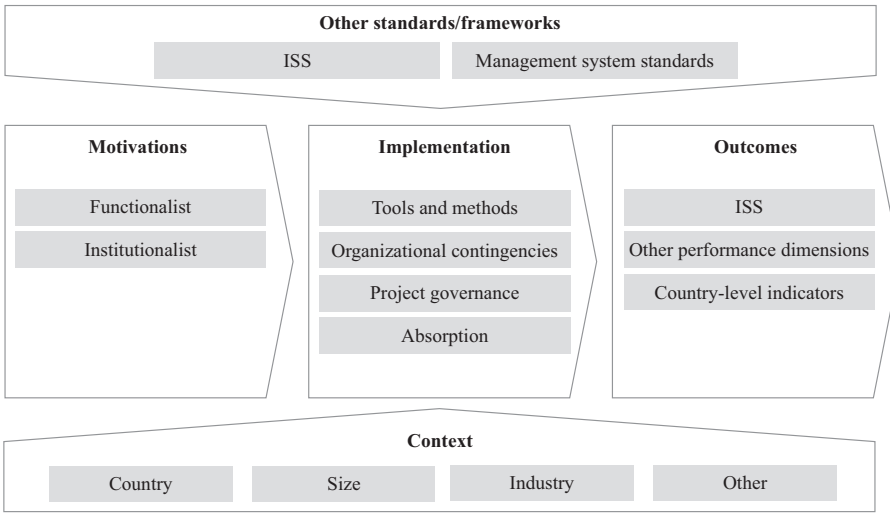

Figure 1.
Coding framework

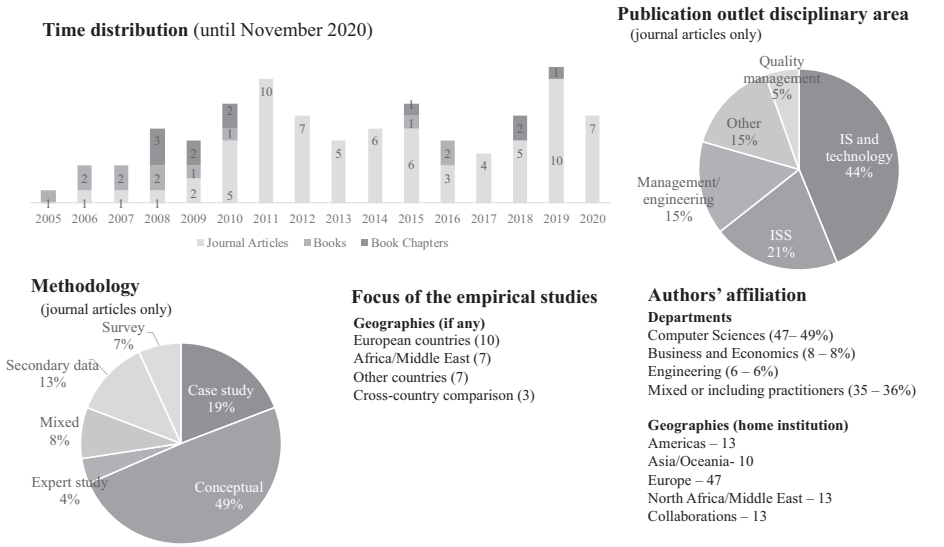

Figure 2.
Main characteristics of the contributions included in the review ($n = 96$)

uptake in the interest in recent years. This trend is correlated to the growing popularity of the standard (ISO, 2019) and probably to ISS becoming a hot topic in the aftermath of publicly reported scandals (e.g. Starwood Hotels, Cambridge Analytica/Facebook, Apple, Evernote, Heartland).

The analysis of the publication outlets shows that most of the papers belong to the IS literature, either in journals specifically related to ISS or on outlets more broadly related to IS and technology, including computer sciences. The strong technical connotation is confirmed by the analysis of the authors' affiliation.

In terms of geography, the authors belong mainly to institutions located in European countries. The distribution partially reflects the geographical focus of the empirical studies included in the review and is consistent with the international diffusion of ISO/IEC 27001 certifications (ISO, 2019).

From a methodological standpoint, the vast majority of the papers has a conceptual nature. It should be noted that research on ISO/IEC 27001 is characterized by a relatively low theoretical underpinning: six papers built on established theories, i.e. the circuit of power framework in Smith *et al.* (2010), the resource-based view (RBV) and the crisis management theory in Bakar *et al.* (2015), the technology acceptance model (TAM) in Ku *et al.* (2009), Van Wessel *et al.* (2011) and Dos Santos Ferreira *et al.* (2018), the theory of cultural differences in Asai and Hakizabera (2010) and the technology–organization–environment (TOE) framework in Mirtsch *et al.* (2021).

4. Thematic findings

4.1 ISO/IEC 27001 and other standards/frameworks

Only 33% of the journal articles included in the review focus exclusively on ISO/IEC 27001. The vast majority of contributions examines it together with other ISS standards and management certifications. Themes and issues are essentially related to standard comparison and integration, as illustrated in the following paragraphs and in Table 1.

Regarding the relation of ISO/IEC 27001 and *other standards with similar scope*, it should be noted that the list of options available to organizations approaching ISS and cybersecurity

Main themes/research results	Relevant papers *(evidence: C = conceptual; E = empirical)*
Comparison/integration with other standards with similar scope (ISS)	
ISO/IEC 27001 complemented by standards with stronger technological scope	Akowuah *et al.* (2013) (C), Almeida and Respício (2018) (C), Broderick (2006) (C), Fuentes *et al.* (2011) (C), Leszczyna (2019) (C), Rezakhani *et al.* (2011) (C), Stewart (2018) (C)
ISO/IEC 27001 complemented by standards for information/document management	Lomas (2010) (C), Stewart (2018) (C), Topa and Karyda (2019) (C)
Presence of issues related to the integration of ISO/IEC 27001 and other ISS standards	Beckers *et al.* (2016) (C), Bettaieb *et al.* (2019) (C), Bounagui *et al.* (2019) (C), Faruq *et al.* (2020) (C), Leszczyna (2019) (C), Mesquida *et al.* (2014) (C), Montesino *et al.* (2012) (C), Mukhtar and Ahmad (2014) (C), Pardo *et al.* (2012) (C), Pardo *et al.* (2013) (C), Pardo *et al.* (2016) (C), Tsohou *et al.* (2010) (C), Tarn *et al.* (2009) (C), Simić-Draws *et al.* (2013) (C), Sheikhpour and Modiri (2012a) (C), Sheikhpour and Modiri (2012b) (C)
Comparison/integration with other management system standards	
Better outcomes through the implementation of ISO/IEC 27001 in combination with other management standards	Bakar *et al.* (2015) (C), Barafort *et al.* (2017) (C), Barafort *et al.* (2018) (C), Barafort *et al.* (2019) (C), Hannigan *et al.* (2019) (E)
Time and cost synergies through the implementation of multiple management system standards (as opposed to a single one)	Crowder (2013) (E), Hoy and Foley (2015) (E), Majerník *et al.* (2017) (C)
Presence of issues related to the integration of ISO/IEC 27001 and other management systems standards	Barafort *et al.* (2017) (C), Barafort *et al.* (2018) (C), Barafort *et al.* (2019) (C), Heston and Phifer (2011) (C), Hoy and Foley (2015) (E), Majerník *et al.* (2017) (C)
Higher organizational complexity because of multiple standards	Heston and Phifer (2011) (C)
ISO/IEC 27001 often implemented after ISO 9001	Cots and Casadesús (2015) (E), Gillies (2011) (E), Mirtsch *et al.* (2021) (E)
International diffusion of ISO/IEC 27001 and ISO/IEC 20000 correlated	Cots and Casadesús (2015) (E)
ISO/IEC 27001 more/less strongly correlated to country-level indicators than other ISO management system standards	Armeanu *et al.* (2017) (E), Başaran (2016) (E)

Table 1.
ISO/IEC 27001 and other standards/ frameworks

is long and articulated. In general terms: standards may cover information security at large including non-information technology (non-IT) assets – as ISO/IEC 27001 – or rather have a technological connotation. This technological connotation might, in turn, be generalist – such as the Control Objectives for Information and Related Technologies (COBIT) and the Information Technology Infrastructure Library (ITIL) – or rather target specific IS layers and related safeguards. Moreover, ISS initiatives are characterized by different purposes, including the definition of requirements (e.g. the HI TRUST Common Security Framework – CSF and ISO 15408 – Common Criteria), the provision of risk assessment instruments (e.g. the National Institute of Standards and Technology – NIST Special Publication – SP 800–30, ISO 27005 and COBIT) and the dissemination of best practices (e.g. ISO 27002, Committee of Sponsoring Organizations of the Treadway Commission – COSO, Information Security Forum – ISF and NIST 800–53).

In light of these differences, several studies indicate complementarities and synergies between ISO/IEC 27001 and other standards/frameworks for a more comprehensive

approach to ISS and cybersecurity (e.g. Lomas, 2010; Rezakhani *et al.*, 2011; Fuentes *et al.*, 2011). Substantial issues, however, are reported in the literature with respect to their integration, including a different scope, the number of requirements and the only partial overlap among them and the different terminology used (Broderick, 2006; Pardo *et al.*, 2012; Beckers *et al.*, 2013; Bettaieb *et al.*, 2019). Against these challenges, several papers (17 contributions, 23%) suggest harmonization methods, also supported by empirical testing (e.g. Pardo *et al.*, 2012, 2013; Mesquida *et al.*, 2014; Bettaieb *et al.*, 2019). The issues addressed in these studies are diverse. Tarn *et al.* (2009), Rezakhani *et al.* (2011), Tsohou *et al.* (2010), Pardo *et al.* (2012), Leszczyna (2019) and Al-Karaki *et al.* (2020) present a framework for the categorization of various ISS standards; along the same lines, Mesquida *et al.* (2014) and Pardo *et al.* (2013, 2016) approach ISO standards related to software quality, IT service management and ISS. Seven papers (Susanto *et al.*, 2011; Montesino *et al.*, 2012; Sheikhpour and Modiri, 2012a, b; Mukhtar and Ahmad, 2014; Bettaieb *et al.*, 2019; Faruq *et al.*, 2020) focus specifically on the alignment between the security controls recommended by ISO/IEC 27001 with other standards. Beckers *et al.* (2016), Bounagui *et al.* (2019), Leszczyna (2019) and Ganji *et al.* (2019) explore integration issues. An interesting perspective is provided by Simić-Draws *et al.* (2013), which defines a method for law-compatible technology design.

Similar integration issues are analyzed in the literature with respect to other *Management system standards*, especially other ISO management systems. Overall, the potential benefits of management system integration have been described in terms of implementation synergies (e.g. Crowder, 2013) and better outcomes (e.g. Bakar *et al.*, 2015; Hannigan *et al.*, 2019), despite possibly an increasing level of complexity (Heston and Phifer, 2011). However, researchers also highlight partial misalignments in the terminology, structure and scope of management system standards (Barafort *et al.*, 2019). Methods and harmonization strategies are described in six papers in our review (8%). Heston and Phifer (2011) illustrate a framework for the selection of standards depending on organizational archetypes. Majerník *et al.* (2017) describe a conceptual model for the integration of ISO/IEC 27001, ISO 9001 for quality management, ISO 14001 for environmental management and OHSAS 18001 for occupational health and safety (now replaced by the ISO 45001). The work of Barafort *et al.* (2017, 2018, 2019) focuses on risk management activities foreseen by ISO/IEC 27001, ISO 9001, ISO 21500 (guidance on project management) and ISO/IEC 20000 (IT service management). Hoy and Foley (2015) delve into the integration of ISO 9001 and ISO/IEC 27001 audits.

Along the same lines, a further area of inquiry concerning ISO/IEC 27001 and other ISO management standards examines diffusion patterns, the order of implementation and possible effects on country-level economic indicators (Gillies, 2011; Cots and Casadesús, 2015; Başaran, 2016; Armeanu *et al.*, 2017). The results show that ISO/IEC 27001 is often implemented after ISO 9001 (Mirtsch *et al.*, 2021), and its diffusion is correlated with ISO/IEC 20000, following the logic that more specific standards are subsequently adopted after more general ones (Cots and Casadesús, 2015).

4.2 Motivations

In the literature on voluntary standards, significant attention has been paid to the motivations driving organizations in the pursuit of certifications (e.g. Heras-Saizarbitoria and Boiral, 2013; Sartor *et al.*, 2016). This is also a common topic in the ISO/IEC 27001 literature, observed in 48% of the studies, although mostly through conceptual arguments.

Following Nair and Prajogo (2009), we classified the motivations as *functionalist* – i.e. organizations expect the standard to improve processes and documentation – and *institutionalist* – i.e. organizations view the certification as a means to better qualify against external stakeholders, including competitors, customers and regulatory agencies. Results are shown in Table 2.

Main themes/research results	Relevant papers *(evidence: C = conceptual; E = empirical)*
Functionalist	
ISO/IEC 27001 is pursued for functionalist motivations, including	
Support in achieving higher levels of ISS	Broderick (2006) (C), Gillies (2011) (E), Hlača *et al.* (2008) (E), Itradat *et al.* (2014) (C), Kossyva *et al.* (2014) (C), Ku *et al.* (2009) (E), Liao and Chueh (2012b) (C), Mesquida *et al.* (2014) (C), Mukhtar and Ahmad (2014) (C), Pardo *et al.* (2012) (C), Pardo *et al.* (2016) (C), Rezaei *et al.* (2014) (E), Susanto *et al.* (2012) (C), Van Wessel *et al.* (2011) (E)
Increased efficiency in processes related to information management	Annarelli *et al.* (2020) (E), Bakar *et al.* (2015) (C), Crowder (2013) (E), Dionysiou (2011) (C), Hlača *et al.* (2008) (E), Kossyva *et al.* (2014) (C), Liao and Chueh (2012b) (C), Mukhtar and Ahmad (2014) (C), Susanto *et al.* (2012) (C), Van Wessel *et al.*, 2011 (E)
Institutionalist	
ISO/IEC 27001 is pursued for Institutionalist motivations, including	
Expected image improvements	Bakar *et al.* (2015) (C), Crowder (2013) (E), Culot *et al.* (2019) (E), Deane *et al.* (2019) (C), Dionysiou (2011) (C), Freeman (2007) (C), Gillies (2011) (E), Hlača *et al.* (2008) (E), Ku *et al.* (2009) (E), Liao and Chueh (2012a) (C), Liao and Chueh (2012b) (C), Lomas (2010) (C), Majerník *et al.* (2017) (C), Mesquida *et al.* (2014) (C), Pardo *et al.* (2016) (C), Rezaei *et al.* (2014) (E), Stewart (2018) (C), Ţigănoaia (2015) (C), Van Wessel *et al.*, 2011 (E)
Governmental regulatory and promotion activities	Annarelli *et al.* (2020) (E), Crowder (2013) (E), Dionysiou (2011) (C), Everett (2011) (C), Gillies (2011) (E), Hlača *et al.* (2008) (E), Ku *et al.* (2009) (E), Lomas (2010) (C), Smith *et al.* (2010) (E), Tsohou *et al.* (2010) (C), Van Wessel *et al.*, 2011 (E)
Market demands	Barafort *et al.* (2019) (C), Beckers *et al.* (2013) (C), Cowan (2011) (E), Dionysiou (2011) (C), Everett (2011) (C), Freeman (2007) (C), Gillies (2011) (E), Hoy and Foley (2015) (C), Mirtsch *et al.* (2021) (E), Ţigănoaia (2015) (C), Van Wessel *et al.*, 2011 (E)
Isomorphism	Deane *et al.* (2019) (C), Everett (2011) (C), Hlača *et al.* (2008) (E), Liao and Chueh (2012b) (C), Majerník *et al.* (2017) (C), Raabi *et al.* (2020) (C), Stewart (2018) (C), Susanto *et al.* (2012) (C), Tsohou *et al.* (2010) (C)
Strength of the "ISO brand"	Deane *et al.* (2019) (C), Majerník *et al.* (2017) (C)

Table 2. Motivations for adopting ISO/IEC 27001

Most of the studies reporting *functionalist* motivations refer to expectations around higher levels of ISS. This is obviously related to the scope of the standard as well as to the continuous improvement logic underpinning the ISMS (Lomas, 2010; Smith *et al.*, 2010; Pardo *et al.*, 2016) and the acquisition of new skills and competences (Ku *et al.*, 2009; Bakar *et al.*, 2015). Several papers also indicate expectations around more efficiency in the processes related to information management (e.g. Kossyva *et al.*, 2014; Hlača *et al.*, 2008; Annarelli *et al.*, 2020). This seems particularly relevant for organizations with previous experience in the implementation of other management systems, as they are aware of the benefits of a structured approach on processes and accountabilities (Crowder, 2013).

Several *institutionalist* motivations also emerge from our analysis. Many authors report expectations for a better corporate image: through the attainment of the certification, it is possible to demonstrate that the organization can be considered a trustworthy partner by its stakeholders, including employees, suppliers, financial institutions and customers (Freeman, 2007; Liao and Chueh, 2012a). This, in turn, appears to be an indirect goal to attract more customers and consolidate client relationships (Beckers *et al.*, 2013). In this respect,

Lomas (2010) underlines that in the UK, information security scandals have raised public awareness; Ku *et al.* (2009) stress that organizations embrace the ISO/IEC 27001 certification to show that they are willing to take a more proactive stance.

Along the same lines, it has been suggested that ISO/IEC 27001 may be adopted following market demands, i.e. large private-sector corporations demand their suppliers to be certified (Ţigănoaia 2015; Barafort *et al.*, 2019). The reason for this might be independent of large corporations being certified themselves, but rather – as reported by Everett (2011) – be related to a standardization in the bidding and procurement process. In this respect, however, it should be noted that several companies pursue an informal implementation – i.e. they shape ISMS in compliance with the standard but do not seek the certification – as ISMS requirements can be self-certified through suppliers' questionnaires (Cowan, 2011; Dionysiou, 2011).

A further motivation mentioned in the studies refers to the presence of governmental regulatory and promotion activities fostering ISO/IEC 27001 diffusion. The past decade has seen a progressive intensification of national (e.g. in the USA, the "National Strategy to Cyberspace Security") and international initiatives (e.g. the Organization for Economic Cooperation and Development – OECD guidelines, European-level initiatives such as the recent EU Cybersecurity act). Overall, these initiatives have been contributing to the dissemination of ISS awareness (Ku *et al.*, 2009); some of them have fostered explicitly the ISO/IEC 27001 certification, as in the case of Japan (Everett, 2011; Gillies, 2011). Smith *et al.* (2010) note that the Australian Government preferred ISO/IEC 27001 over other ISS standards because of its flexibility in accommodating local legal requirements. The reach of European-level policies is well described in Dionysiou (2011), together with the peculiar example of Cyprus adopting certification as a "ticket to the European market" (p. 198).

Finally, some studies point to the presence of isomorphic dynamics. In the case illustrated by Hlača *et al.* (2008), the ISO/IEC 27001 was adopted in light of the growing number of certified companies worldwide. The rationale behind this is illustrated in Stewart (2018) through the concept of network effects. This dynamic seems further reinforced by the global reputation of the ISO umbrella of standards (Deane *et al.*, 2019).

4.3 Implementation

A considerable number of studies (68%) report issues and opportunities related to the implementation of the standard. We classified them according to three main questions: *(1)* how effectively ISO/IEC 27001 *tools and methods* provide support to the implementing organization?; *(2)* how do organizations structure the *project governance*?; *(3)* what differences in the *actual adoption of practices* have been documented?

The themes and sub-themes identified in the studies are illustrated in Table 3.

As for the efficacy of the *(1) tools and methods* indicated by ISO/IEC 27001, the literature is ambivalent. Whereas several authors (e.g. Smith *et al.*, 2010) praise ISO/IEC 27001 flexibility, a number of studies see this as a potential drawback in the implementation process (e.g. Lomas, 2010; Rezaei *et al.*, 2014). The requirements are often perceived as too formal and wide-ranging; they provide guidance for what should be done, but organizations are responsible for choosing "how" to achieve those goals (Bounagui *et al.*, 2019). The lack of precise methodological indications may translate into low accuracy in the risk analysis and asset assessment. Much is left to the expertise of the individuals in charge (e.g. Ku *et al.*, 2009; Liao and Chueh, 2012a), with often too much emphasis placed on the technical side (Ozkan and Karabacak, 2010; Itradat *et al.*, 2014).

Some specific issues in this respect emerge from the literature. The most relevant one is related to the security controls, in particular considering the set of 133 controls described in the Annex A of the 2005 version of the standard. Although no longer mandatory in the

Main themes/research results	Relevant papers *(evidence: C = conceptual; E = empirical)*
Tools and methods	
High flexibility of the guidelines	Bamakan and Dehghanimohammadaba (2015) (C), Barafort *et al.* (2017) (C), Barafort *et al.* (2019) (C), Beckers *et al.*, (2013) (C), Beckers *et al.* (2016) (C), Bounagui *et al.* (2019) (C), Culot *et al.* (2019) (E), Dionysiou (2011) (C), Fuentes *et al.* (2011) (C), Ganji *et al.* (2019) (C), Gillies (2011) (E), Heston and Phifer (2011) (C), Itradat *et al.* (2014) (E), Ku *et al.* (2009) (E), Liao and Chueh (2012a) (E), Liao and Chueh (2012b) (C), Lomas (2010) (C), Mirtsch *et al.* (2021) (E), Ozkan and Karabacak (2010) (E), Raabi *et al.* (2020) (C), Rezaei *et al.* (2014) (C), Simić-Draws *et al.* (2013) (C), Stewart (2018) (C), Van Wessel *et al.* (2011) (E)
Security controls difficult to assess/ implement	Almeida and Respício (2018) (C), Bettaieb *et al.* (2019) (C), Crowder (2013) (E), Ho *et al.* (2015) (E), Liao and Chueh (2012a) (E), Liao and Chueh (2012b) (C); Montesino *et al.* (2012) (E) Simić-Draws *et al.* (2013) (C), Susanto *et al.* (2011) (C), Susanto *et al.* (2012) (C), Stewart (2018) (C), Topa and Karyda (2019) (C), Van Wessel *et al.*, 2011 (E)
Difficult assessment of external interdependencies	Beckers *et al.* (2013) (E), Culot *et al.* (2019) (E), Lomas (2010) (C), Smith *et al.* (2010) (E), Stewart (2018) (C)
Further effort needed to integrate legal requirements	Beckers *et al.* (2013) (C), Broderick (2006) (C), Diamantopoulou *et al.* (2020) (C), Lomas (2010) (C), Simić-Draws *et al.* (2013) (C)
Possible integration with GDPR requirements	Annarelli *et al.* (2020) (E), Diamantopoulou *et al.* (2020) (C), Gaşpar and Popescu (2018) (C), Lopes *et al.* (2019) (E), Serrado *et al.* (2020) (E)
Relevant cultural and psychological elements not adequately addressed	Asai and Hakizabera (2010) (E), Topa and Karyda (2019) (C), van Wessel *et al.* (2011) (E)
Project governance	
Senior management commitment	Beckers *et al.* (2013) (C), Beckers *et al.* (2016) (C), Crowder (2013) (E), Everett (2011) (C), Gillies (2011) (E), Kossyva *et al.* (2014) (C), Ku *et al.* (2009) (E), Liao and Chueh (2012a) (E), Ozkan and Karabacak (2010) (E), Smith *et al.* (2010) (E), Stewart (2018) (C), Van Wessel *et al.* (2011) (E)
Cross-functional coordination	Crowder (2013) (E), Itradat *et al.* (2014) (E), Kossyva *et al.* (2014) (C), Ku *et al.* (2009) (E), Simić-Draws *et al.* (2013) (C), Smith *et al.* (2010) (E), Van Wessel *et al.* (2011) (E)
Support of external consultants	Annarelli *et al.* (2020) (E), Dionysiou (2011) (E), Gillies (2011) (E), Hlača *et al.* (2008) (E), Mirtsch *et al.* (2021) (E), Rezaei *et al.* (2014) (C), Van Wessel *et al.* (2011) (E)
Organizational learning through self-implementation	Crowder (2013) (E), Gillies (2011) (E), Ku *et al.* (2009) (E), Van Wessel *et al.* (2011) (E)
Significant time/cost to implement	Annarelli *et al.* (2020) (E), Broderick (2006) (C), Culot *et al.* (2019) (E), Deane *et al.* (2019) (C), Dionysiou (2011) (C), Everett (2011) (C), Gillies (2011) (E); Hlača *et al.* (2008) (E), Kossyva *et al.* (2014) (C), Majerník *et al.* (2017) (C), Mirtsch *et al.* (2021) (E), Montesino *et al.* (2012) (C), Ozkan and Karabacak (2010) (E), Pardo *et al.* (2016) (C), Smith *et al.* (2010) (E), Stewart (2018) (C), Van Wessel *et al.* (2011) (E)
Actual adoption of practices (absorption)	
Symbolic/informal implementation of the standard	Culot *et al.* (2019) (E), Everett (2011) (E), Lomas (2010) (C), Mirtsch *et al.* (2021) (E)
Low employees' compliance	Asai and Hakizabera (2010) (E), Heston and Phifer (2011) (C), Smith *et al.* (2010) (E), Topa and Karyda (2019) (C), Van Wessel *et al.* (2011) (E)

Table 3.
Implementation of ISO/ IEC 27001

current version (ISO/IEC 27001:2013), it is still worth mentioning the main problems highlighted by previous research. Controls seemed not to be applicable in organizations with low-technological profiles (Liao and Chueh, 2012b), entailed too rigid procedures (Crowder, 2013) and were costly to implement due to the possibility of an only partial automation through hardware and software tools (Montesino *et al.*, 2012). As for the new version of the ISO/IEC 27001, Ho *et al.* (2015) note that the standard still does not provide guidance on the mutual interdependence among the different control items; similarly, Stewart (2018) and Topa and Karyda (2019) refer to the lack of indications regarding a cost/benefit assessment in the selection of controls. On this, Bettaieb *et al.* (2019) propose an approach based on machine learning for the identification of the most relevant controls, given the characteristics and the context of the implementing organization.

The literature has also highlighted a lack of guidance regarding possible interdependencies between the organization and the external environment. As reported by Smith *et al.* (2010) and Stewart (2018), many implementations fail because of an unstructured approach toward shared assets – e.g. services and IT infrastructure shared among local units of the same corporation – and poor identification of the organizations' dependencies from third parties and outsourced services.

The support provided by ISO/IEC 27001 in aligning the organization ISMS to local legislation has also been discussed. The standard states that the implementing organization should identify autonomously the applicable local regulation and contractual obligations (Diamantopoulou *et al.*, 2020; Simić-Draws *et al.*, 2013); however, in the absence of precise instructions, organizations face complex reconciliations and the challenge of complying with multiple local legislations in the case of multinational enterprises (Broderick, 2006). In connection to this, recent studies have investigated how the norm supports organizations in complying with the General Data Protection Regulation (GDPR), issued in 2016, to regulate data protection and privacy in the European Union and the European Economic Area. The ISO/IEC 27001 was last updated in 2013, i.e. before the GDPR publication, while the new regulatory requirements were included in the new ISO/IEC 27552 (Privacy Information Management). Nevertheless, previous research has highlighted similar requirements between the GDPR and ISO/IEC 27001 (Annarelli *et al.*, 2020) as well as the fact that a structured ISMS is a prerequisite to meet the European directives (Serrado *et al.*, 2020).

Another issue underscored in the studies concerns the fact that ISO/IEC 27001 does not provide adequate guidance on cultural and psychological dimensions relevant for ensuring employees' compliance (Van Wessel *et al.*, 2011). As highlighted by Topa and Karyda (2019), there are only limited indications regarding the appraisal of individual habits and values, e.g. privacy concerns and compliance attitude. Similarly, Asai and Hakizabera (2010) underline the presence of cultural differences in the attitude toward ISS.

With regard to the second overarching theme – *(2) project governance* – the studies show that IT, organizational and legal competencies are necessary, and therefore, companies need to formulate well-defined coordination mechanisms (e.g. Crowder, 2013). In terms of the structure of the project team and implementation phases, the literature reports various approaches, normally starting with local pilots and then moving on to large-scale rollouts (Ku *et al.*, 2009; Van Wessel *et al.*, 2011). Along the same lines – although it is a well-documented fact that a successful management system requires leadership endorsement (e.g. Crowder, 2013) – several articles indicate that ISO/IEC 27001 is mostly developed by IT departments alone (Van Wessel *et al.*, 2011; Akowuah *et al.*, 2013). Stewart (2018) notes that information security leaders are unlikely to be included in the management committee. Everett (2011) reports that limited directors' awareness often results in low budget allocation. An unsolved implementation issue seems to be the potential involvement of consultants. Whereas specialistic ISS competencies lead many organizations to seek external support (e.g. Dionysiou, 2011; Hoy and Foley, 2015; Annarelli *et al.*, 2020), several studies underline how

this may hamper organizational learning and lead to unsuccessful implementation (Ku *et al.*, 2009; Gillies, 2011). In any case, there is agreement on the fact that the process to obtain the ISO/IEC 27001 certification usually absorbs significant company resources in terms of working hours and financial resources (e.g. Gillies, 2011; Van Wessel *et al.*, 2011).

Finally, the last theme emerging from our review concerns the possibility of differences in the *(3) actual adoption of practices*, namely, to what extent the written documentation is internalized by the organization (Nair and Prajogo, 2009). This has emerged as a key research area in relation to other standards and voluntary initiatives (e.g. Heras-Saizarbitoria and Boiral, 2013; Orzes *et al.*, 2018), but few studies addressed specifically the question with regard to ISO/IEC 27001. Some papers stress that a "cosmetic and not substantial" application of the standard might take place (Culot *et al.*, 2019, p. 83) and that some companies "put in as little effort as possible" (Everett, 2011, p. 7). Moreover, the reasons why several companies conform to ISO/IEC 27001 requirements but not seek formal certification are overall under-investigated (Mirtsch *et al.*, 2021).

Comparatively more attention has been paid to employee compliance. The studies refer to organizational inertia – i.e. employees are skeptical about the required reconfiguration of processes and reluctant to change (e.g. Heston and Phifer, 2011; Topa and Karyda, 2019) – and opposition whenever the implementation of the standard is externally mandated (Smith *et al.*, 2010).

4.4 Outcomes

As illustrated in Table 4, few studies (26%) have cited the outcomes of the ISO/IEC 27001 certification, with just half of them providing empirical evidence in support. Only three studies focus explicitly on the impact of the standard. Tejay and Shoraka (2011) and Deane *et al.* (2019) analyze through an event study the impact of the certification on stock market

Main themes/research results	Relevant papers *(evidence: C = conceptual; E = empirical)*
Outcomes specific to the scope of the standard (ISS)	
More efficient risk prevention	Al-Karaki *et al.* (2020) (C), Annarelli *et al.* (2020) (E), Everett (2011) (E), Freeman (2007) (C), Fuentes *et al.* (2011) (C), Rezaei *et al.* (2014) (E), Van Wessel *et al.* (2011) (E)
Higher business continuity	Bakar *et al.* (2015) (C), Rezaei *et al.* (2014) (E), Susanto *et al.* (2012) (C), Van Wessel *et al.* (2011) (E)
Other performance dimensions	
Streamlined processes	Annarelli *et al.* (2020) (E), Crowder (2013) (E), Everett (2011) (E), Freeman (2007) (C), Fuentes *et al.* (2011) (C), Van Wessel *et al.*, 2011 (E)
Better stakeholder relationship	Hannigan *et al.* (2019) (E), Mirtsch *et al.* (2021) (C), Rezaei *et al.* (2014) (E), Van Wessel *et al.*, 2011 (E)
Reduced partner opportunism	Kossyva *et al.* (2014) (C)
Lower flexibility	Van Wessel *et al.* (2011) (E)
Adequate return on investment	Van Wessel *et al.* (2011) (E)
Lower risk of profit loss	Bakar *et al.* (2015) (C), Van Wessel *et al.* (2011) (E)
Higher market value	Deane *et al.* (2019) (E), Tejay and Shoraka (2011) (E)
Lower insurance costs	Gillies (2011) (C), Susanto *et al.* (2012) (C)
Country-level indicators	
Correlation with intellectual property indicators	Başaran (2016) (E)
Correlation with confidence sentiment indicators	Armeanu *et al.* (2017) (E)

Table 4.
Outcomes of ISO/IEC 27001

performance; Kossyva *et al.* (2014) discuss conceptually its benefits in a co-opetitive setting. The other papers either report impacts in the description of case studies and through expert opinions (Van Wessel *et al.*, 2011; Crowder, 2013; Rezaei *et al.*, 2014; Hannigan *et al.*, 2019; Annarelli *et al.*, 2020) or derive outcomes from conceptual reasoning (Freeman, 2007; Dionysiou, 2011; Fuentes *et al.*, 2011; Gillies, 2011; Bakar *et al.*, 2015).

The performance dimensions emerging from our analysis are diverse, some more in line with *the scope of the standard* – i.e. lower risk levels (Freeman, 2007; Rezaei *et al.*, 2014) and improved business continuity (Van Wessel *et al.*, 2011; Bakar *et al.*, 2015) – *others* related to organizational and financial improvements. The studies refer to streamlined and efficient processes because of ISMS redesign (Fuentes *et al.*, 2011; Crowder, 2013). Process improvements may translate into increasing employees' and customers' satisfaction, even though Van Wessel *et al.* (2011) report that, for one of the companies they analyzed, the certification also meant losing some operational flexibility. Kossyva *et al.* (2014) suggest a reduction in miscommunication and opportunism in information exchange.

Some authors looked at the impact of the certification from a financial perspective. The cases analyzed in Van Wessel *et al.* (2011) report a payback period in line with the expectations. Bakar *et al.* (2015) claim that ISO/IEC 27001 may prevent the leaking of private information to unauthorized parties, and subsequent legal actions, bad publicity and profit losses. Moreover, the insurance premium of certified companies is lower (Gillies, 2011; Susanto *et al.*, 2012).

Besides organizational-level benefits, it should be noted that two papers correlate ISO/IEC 27001 diffusion with *country-level indicators*. The study of Armeanu *et al.* (2017) shows that the presence of ISO standards has a positive influence on the economic sentiment indicator, a cross-industry composite confidence indicator published monthly by the European Commission. Başaran (2016) illustrates the strength of the association between the number of ISO certificates and industrial property rights granted in Turkey.

4.5 Context

Several studies (50%) indicate that the adoption of ISS standards as well as ISO/IEC 27001 motivations, implementation and outcomes should be read against the context in which the organization operates, as shown in Table 5.

Most of the papers stressing differences among *countries* refer to international (e.g. Europe, OECD) and governmental (e.g. Japan, Australia) initiatives fostering the diffusion of ISO/IEC 27001 (e.g. Lomas, 2010; Dionysiou, 2011; Serrado *et al.*, 2020). Other studies highlight higher adoption in offshored countries – e.g. Taiwan, Singapore and India – because of the need to ensure a secure environment for intellectual property to maintain attractiveness (Ku *et al.*, 2009). Less export-oriented countries might – on the contrary – be less likely to see high adoption rates (Dyonysiou, 2011). Interestingly, Heston and Phifer (2011) point out that multinational enterprises (MNEs) – although structuring their process homogeneously at global level – might formally pursue the certification only in some countries depending on local opportunities and constraints.

Country-specific elements are underscored also in relation to cultural differences in terms of employees' attitudes toward ISMS compliance (Asai and Hakizabera, 2010; Topa and Karyda, 2019). Moreover, the approach to ISO/IEC 27001 implementation seems different between European and Chinese companies (Van Wessel *et al.*, 2011).

Differences based on organizations' *size* are mentioned in the literature to a lesser extent. Even though smaller public companies might expect greater returns from certification than larger firms (Deane *et al.*, 2019), only large companies seem to assign sufficient priority to ISS due to resource availability (Dionysiou, 2011; Gillies, 2011). With regard to the implementation process – as stressed by Stewart (2018) – ISO/IEC 27001 is designed for

Main themes/research results	Relevant papers *(evidence: C = conceptual; E = empirical)*
Country	
Adoption driven by regulatory/promotion activities	Cots and Casadesús (2015) (E), Dionysiou (2011) (C), Everett (2011) (C), Gillies (2011) (E), Khajouei *et al.* (2017) (E), Ku *et al.* (2009) (E), Lomas (2010) (C), Ozkan and Karabacak (2010) (C), Serrado *et al.* (2020) (E), Smith *et al.* (2010) (E), Ţigănoaia (2015) (C), Van Wessel *et al.* (2011) (E)
Higher adoption in export-driven countries	Dionysiou (2011) (C), Gillies (2011) (E), Ku *et al.* (2009) (E), Van Wessel *et al.* (2011) (E)
Implementation/compliance affected by cultural factors	Asai and Hakizabera (2010) (E), Ku *et al.* (2009) (E), Topa and Karyda (2019) (C), Van Wessel *et al.* (2011) (E)
MNEs pursue formal implementation only in selected countries	Heston and Phifer (2011) (E)
Size	
SMEs have lower ISS awareness	Dionysiou (2011) (E), Gillies (2011) (E), Mirtsch *et al.* (2021) (E)
Different implementation issues related to organizations' size	Al-Karaki *et al.* (2020) (C), Deane *et al.* (2019) (E), Dionysiou (2011) (E), Gillies (2011) (E), Mirtsch *et al.* (2021) (E), Smith *et al.* (2010) (E), Stewart (2018) (C)
Greater increase in market value in small public companies upon certification announcement	Deane *et al.* (2019) (E)
Industry	
Higher adoption rates in regulated/information-intensive industries	Akowuah *et al.* (2013) (C), Deane *et al.* (2019) (E), Dionysiou (2011) (C), Everett (2011) (C), Heston and Phifer (2011) (C), Itradat *et al.* (2014) (C), Mirtsch *et al.* (2021) (E), Mukhtar and Ahmad (2014) (C), Serrado *et al.* (2020) (E)
Standard seen applicable only to highly digitalized organizations	Crowder (2013) (E), Liao and Chueh (2012a) (C), Liao and Chueh (2012b) (C), Lomas (2010) (E)
Certification perceived as a source of competitive differentiation in some industries	Crowder (2013) (E), Ku *et al.* (2009) (E)
Other	
Emerging technological trajectories need more specific approaches	Beckers *et al.* (2013) (C), Beckers *et al.* (2016) (C), Bounagui *et al.* (2019) (C), Culot *et al.* (2019) (E), Leszczyna (2019) (C), Lomas (2010) (C), Park and Lee (2014) (C), Raabi *et al.* (2020) (C)
Characteristics of the organizational culture	Al-Karaki *et al.* (2020) (C), Asai and Hakizabera (2010) (E), Broderick (2006) (C), Dionysiou (2011) (E), Dos Santos Ferreira *et al.* (2018) (E), Everett (2011) (C), Gillies (2011) (E), Itradat *et al.* (2014) (E), Kossyva *et al.* (2014) (C), Ku *et al.* (2009) (E), Liao and Chueh (2012a) (E), Mirtsch *et al.* (2021) (E), Simić-Draws *et al.* (2013) (C), Smith *et al.* (2010) (E), Stewart (2018) (C), Ţigănoaia (2015) (C), van Wessel *et al.* (2011) (E)

Table 5.
Context of ISO/IEC 27001

an "average organization," and it might not be suitable for companies deviating the most from this average profile, e.g. owing to their dimension or level of centralization (Smith *et al.*, 2010; Stewart, 2018).

In terms of *industry*-specific dynamics, the literature points to differences in the diffusion patterns. Although the standard is generic by design, it is adopted more in regulated industries – such as financial services and health care (Dionysiou, 2011; Heston and Phifer, 2011; Mukhtar and Ahmad, 2014) – and where information security attacks have been

historically more frequent (Deane *et al.*, 2019). In other industries, there seems to be less interest (Everett, 2011; Liao and Chueh, 2012a, b), although it might represent a differentiation factor (Ku *et al.*, 2009; Crowder, 2013). Finally, although the standard does not require the implementing organization to have any form of IT in place, it is often perceived as applicable only to highly digitalized contexts (Crowder, 2013).

On the contrary, the most recent literature shines the spotlight on the limited effectiveness of ISO/IEC 27001 against emerging technologies. Overall, the studies underline the fact that the emergence of cloud computing, the internet of things and platform-based business models makes it increasingly difficult to define the scope and boundaries of the ISMS (Culot *et al.*, 2019). Being ISO/IEC 27001 process-driven seems better suited to meet these challenges than more document-oriented standards (Beckers *et al.*, 2013). However, ISO/IEC 27001 alone seems not sufficient to guarantee both IS security and safety (Park and Lee, 2014), but it may represent the backbone on which more specific standards are integrated (Leszczyna, 2019).

Lastly, the literature highlights the presence of contingencies related to the organizational culture. Depending on this, ISS can be understood as a purely technical issue rather than a far-reaching business goal (e.g. Everett, 2011). In a survey, cultural change is identified as the main challenge to overcome (Gillies, 2011); organizations more prone to innovation and change are expected to be more successful in the standard implementation (e.g. Ku *et al.*, 2009; Liao and Chueh, 2012a).

4.6 Themes and topics related to books and book chapters

In addition to what has been illustrated in the previous sections, the results of the analysis of the books and chapters on ISO/IEC 27001 are consistent with the themes emerging from the coding of academic articles. As shown in Table 6, besides some contributions providing a general overview of the norm (e.g. Accerboni and Sartor, 2019; Arnason and Willet, 2007), most of the books focus either on the relationship of ISO/IEC 27001 with other standards for ISS (e.g. Calder 2008, 2018; Calder and Geraint, 2008) or on complementing the norm guidelines with implementation methods, technical tools (e.g. Calder, 2006a; Calder and Watkins, 2008; Beckers, 2015) and risk management approaches (e.g. Calder and Watkins, 2010). Legal issues and the auditing process have received comparatively little attention so far (Pompon, 2016). Managerial topics related to the standard implementation refer to limited leadership awareness (Calder, 2010) as well as to motivations and guidelines' effectiveness (Erkonen, 2008; Dionysiou *et al.*, 2015).

Table 6.
Books and book chapters on ISO/IEC 27001

Aim of the contribution	Relevant contributions *(B = book; BC = book chapter)*
General overview of the norm/requisites	Accerboni and Sartor (2019) (BC), Arnason and Willet (2007) (B), Calder (2006b) (B)
Comparison/integration issues of ISS standards	Barlette and Fomin (2010) (BC), Calder (2008) (BC), Calder and Moir (2009a) (BC), Calder (2018) (BC), Calder and Geraint (2008) (BC)
Illustrate implementation guidelines/methods	Calder (2005) (B), Calder (2006a) (B), Calder and Watkins (2008) (B), Humphreys (2007) (B), Stoll (2018) (BC)
Present technical tools useful for implementation	Beckers (2015) (B), Vasudevan *et al.* (2008) (B), Honan (2009) (B)
Define methods for risk assessment and management	Calder and Watkins (2010) (B)
Illustrate the legal implications (also connected to the GDPR)	Calder and Moir (2009b) (BC), IT Governance privacy team (2016) (B)
Describe the auditing process	Pompon (2016) (B)
Managerial issues related to ISO/IEC 27001	Calder (2010) (BC), Dionysiou *et al.* (2015) (BC), Erkonen (2008) (BC)

5. Summary and research challenges

The systematic review on ISO/IEC 27001 helps to clarify the main themes and results elaborated in almost 15 years of academic research on the standard. Emerging clearly from the literature is that: (1) a structured approach to information and cybersecurity requires the integration of multiple standards; (2) the motivations to pursue the ISO/IEC 27001 certification are also related to governmental incentives and market demands; (3) implementation entails several challenges due to guidelines that are generic by design, different approaches/internalization levels are possible; (4) there is limited evidence demonstrating the outcomes of the certification; (5) integration of ISS standards, motivations, implementation and outcomes are dependent on a series of contextual factors, including the technological environment in which the organization operates. Overall, the paucity of empirical studies on ISO/IEC 27001 is striking, especially in light of significant public efforts to sustain the diffusion of the certification. The fact that the academic debate has seen a limited cross-fertilization between subject areas further exacerbates the knowledge gaps on this subject.

Today, value creation is all about exchanging information within and beyond organizational boundaries (Culot *et al.*, 2020; Hagiu and Wright, 2020). New forms of inter-organizational collaborations allow intellectual property and data to flow between organizations (Bititci *et al.*, 2012; Pagani and Pardo, 2017). The scale and scope of such interactions are posing new challenges to ISS (Hinz *et al.*, 2015; Jeong *et al.*, 2019; Feng *et al.*, 2020). Supply chains are becoming increasingly digitalized, augmenting the risk of losing intellectual property (Kache and Seuring, 2017; Ardito *et al.*, 2019; Büyüközkan and Göçer, 2018). Online platforms and tech giants are connecting vast numbers of suppliers and customers (Jacobides *et al.*, 2018; Benitez *et al.*, 2020); the participants of these ecosystems place their trust in the platform orchestrators' ability to ensure ISS at large, including those of relevant third parties (Burns *et al.*, 2017). The spread of cloud-based solutions implies massive outsourcing of data storage and computing capabilities (Beckers *et al.*, 2013; Markus, 2015).

Overall, this scenario demands ISS to be seen no longer as an issue affecting single organizations in isolation but more as a question of flows and relations involving multiple partners; an inherently "wicked problem" calling for a broad rethinking of assumptions (Lowry *et al.*, 2017). This rings all the more relevant with regard to the challenges that the COVID-19 pandemic is generating. Social distancing resulted for many organizations in a surge of work-from-home arrangements, higher activity on customer-facing networks and greater use of online services and platforms, all of which are causing immense stress on ISS controls and operations (Boehm *et al.*, 2020; Deloitte, 2020). In parallel, several concerns have been raised about contact-tracing applications deployed in the attempt to contain the contagion; the potential damages from the misuse of personal and biometric data are unprecedented (Harari, 2020). As we write, the storm continues to rage in many areas of the world, yet many observers believe that a structural shift is taking place, making digitalization a key feature of the "new normal" (Smith, 2020; The Economist, 2020).

These considerations should also inform research on ISO/IEC 27001 going forward. Faced with a world where organizational boundaries are increasingly meaningless, the same concept of IS perimeter obsolete (Dhillon *et al.*, 2017; Cavusoglu *et al.*, 2015). Overall, there is an apparent contradiction between the low technological specificity and organizational-level focus of the standard, on the one hand, and ISS requirements that are increasingly advanced and systemic, on the other.

Two aspects emerging from the review seem particularly relevant in this respect. First, other standards, frameworks and not-standardized practices may be integrated on the structure of ISO/IEC 27001 for more comprehensive approaches. Second, the ISO/IEC 27001 certification is often pursued in accordance with inter-organizational requirements – e.g. large companies demanding their suppliers be certified, governmental actions sustaining the

certification, expectations of image improvements and better relations with key stakeholders. Both these aspects, however, have been only superficially addressed so far. The integration of multiple standards and practices has been mostly tackled by technical studies defining methods; whereas the inter-organizational implications of ISO/IEC 27001 have emerged in the literature only with regard to institutional motivations driving adoption.

Against this backdrop, we believe that a shift in the attention is needed from "the part" to "the whole" in the study of ISO/IEC 27001. In light of the growing number of certifications coupled with the endorsement of major digital players, it is important to intensify scientific efforts; the next section is thus devoted to the formulation of a set of research directions addressing these issues.

5.1 Theory-based research agenda

In line with renewed calls for more theory-grounded research (e.g. Breslin *et al.*, 2020; Post *et al.*, 2020), we conclude our study by outlining a series of research opportunities that read the emerging challenges and the current knowledge gaps through theoretical lenses. Several theories have been used over the years in the study of voluntary standards and can be successfully applied in future research on ISO/IEC 27001. The most prominent ones – following the review of Tuczek *et al.* (2018) – include:

(1) Transaction cost theory (Coase, 1937; Williamson, 1985): As the focus is placed on the costs arising from an economic exchange between a buyer and a seller, the theory has been used to analyze voluntary standards adoption patters and performance implications related to lower information asymmetries (e.g. Prajogo *et al.*, 2012).

(2) Resource-based view (Penrose, 1959; Barney, 1991): Under the assumption that firms should identify and make use of resources that are valuable, rare and difficult to imitate in order to gain competitive advantage, researchers have investigated the motivations to adopt voluntary standards, the implementation process and the impact on performance (e.g. Darnall, 2006; Schoenherr and Talluri, 2013; Jabbour, 2015);

(3) Institutional theory (Meyer and Rowan, 1977; DiMaggio and Powell, 1983): The perspective has been leveraged on mainly for investigating voluntary standards diffusion since societal influence might explain why organizations converge and become similar (e.g. Nair and Prajogo, 2009; Boiral and Henri, 2012).

(4) Signaling theory (Spence, 1973): Studies have addressed the role of voluntary standards in supplier selection under conditions of imperfect information, mostly focusing on performance implications, absorption levels and time-dependent dynamics (e.g. Terlaak and King, 2006; Narasimhan *et al.*, 2015).

(5) Stakeholder theory (Freeman, 1984): Due to the integration of business and social issues under this view, prior research has explored how the pressure from (non-business) stakeholders might influence the motivations driving standard implementation and absorption as well the impact on operational and reputational performance (e.g. Castka and Prajogo, 2013).

Although these theories can be applied effectively also for the study of ISO/IEC 27001, we believe that future research should not be limited to the standard implementation within single organizations, but (1) address its role within the suite of ISS practices and standards and (2) take into consideration that the scope of ISS reaches beyond organizational boundaries. Figure 3 clarifies how these two perspectives can be investigated, including a possible theoretical underpinning and a summary of the main research opportunities, which

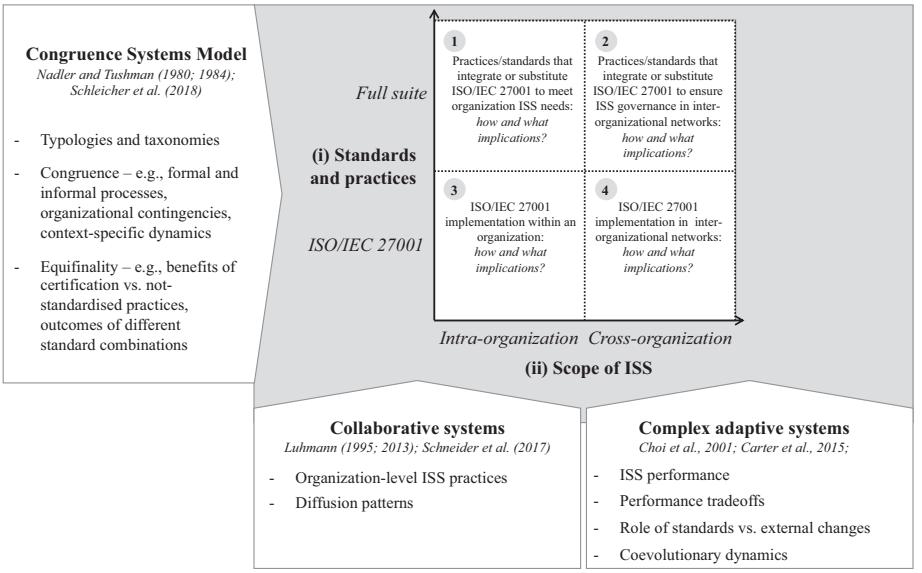

Figure 3.
Research agenda

are outlined in the following paragraphs. In the figure, the perspectives form a matrix that identifies four overarching research areas with different scopes.

With respect to these four quadrants, the rationale behind the research agenda is based on the tenets of social systems thinking (e.g. Checkland, 1997; Weinberg, 2001). We drew from various approaches within this school of thought to provide a comprehensive, yet parsimonious analytical framework targeted at academics from different backgrounds. Reframing and reorganizing research topics through a system-based approach has proved to offer a good basis to provide new stimulus to scientific research and novel outlooks to the business community (e.g. Bititci *et al.*, 2012; Schleicher *et al.*, 2018).

In simple terms, a system is a set of interrelated elements, such that a change in one element affects others in the system (Von Bertalanffy, 1956); the system is characterized by a common purpose, functions as a whole and adapts to changes in the environmental conditions (Boulding, 1956; Katz and Kahn, 1978). Different theories co-exist under this umbrella, this plurality yielding a rich research stream with a strong interdisciplinary connotation (Mele *et al.*, 2010; Post *et al.*, 2020).

Based on the findings of our review and the challenges outlined in the previous section, it is possible to consider as social systems both:

(1) the suite of standards, formal and informal practices – including ISO/IEC 27001 – that are implemented by organizations to manage ISS and cybersecurity; and

(2) the network of relations in which organizations are embedded, be it supply chains, platform-based ecosystems or industries.

Different frameworks can be applied to these two systems. The first finds analytical support, particularly in the congruence systems model as originally formulated by Nadler and Tushman (1980, 1984) and recently re-elaborated by Schleicher *et al.* (2018). The model sees organizational practices as systems, identifies their inputs and outputs as well as their underlying components, i.e. tasks, individuals, formal and informal processes. These components are assumed to exist in a state of relative balance, their congruence determining the overall

effectiveness of the system. Another important characteristic of such systems is the principle of equifinality (Katz and Kahn, 1978; Schleicher *et al.*, 2018), suggesting that different configurations of various system components can lead to the same output or outcome.

Several research opportunities stem from this view to investigate both the implementation of ISO/IEC 27001 – e.g. the congruence between requirements and actual practices, the opportunity to pursue a certification as opposed to informal implementation and not-standardized practices – and the managerial implications of multiple standard integration, including the analysis of congruence as a predictor of ISS performance. Overall, future research can develop typologies and taxonomies on the basis of the elements identified by the model to clarify the role of ISO/IEC 27001 within the suite of ISS standards and practices.

The second system-level view – i.e. network of relations in which organizations are embedded – is useful for analyzing how ISO/IEC 27001 supports ISS in a context characterized by inter-organizational information flows. The issue can be approached through the complexity-based perspectives germane to social systems thinking: these enable the analysis of emerging structures in the interaction among autonomous agents – e.g. firms – and consider the adaptation of the whole system to the external environment. Among these perspectives, two theoretical lenses seem particularly suited to the issue at hand:

(1) Collaborative systems – As outlined by Schneider *et al.* (2017) drawing from Luhmann (1995, 2013) – to elucidate how individual organizations shape their approach to ISS depending on the network of relations they are embedded in.

(2) Complex adaptive systems (CAS) – According to the conceptualization of Choi *et al.* (2001) and Carter *et al.* (2015) – which shift the unit of analysis from the single organization to the whole network of relations, thus enabling the analysis of ISS practices at the level of the supply chain and the business ecosystem.

On the one hand, collaborative systems are based on the general principle that organizational structures and processes need to adapt against changes in the economic, technological and regulatory environment (Luhmann, 1995). Individual organizations can opt for internal solutions, but can also pursue joint initiatives, such as embracing standards or orchestrating industry-wide responses. These joint initiatives are more likely to happen if there is a history of cross-organizational collaboration connecting the agents and when concerns about the relevance of the issue to be addressed are shared between them (Schneider *et al.*, 2017). These considerations are relevant to future research investigating organizations implementing internal ISS methodologies as opposed to standards, especially in light of new technologies and business models. Similarly, they can be tested with respect to standard diffusion patterns as well as taking the correlation between standards and implementation methodologies into account.

On the other hand, CAS is conceptualized as dynamic networks of autonomous agents (or firms) that interact with one another and in their environment to produce evolving systems (Choi *et al.*, 2001; Carter *et al.*, 2015). The study of CAS is characterized by three analytical dimensions: the internal mechanisms governing the relations among the agents, the adaptability of the network to changes in the external environment and the presence of co-evolutionary dynamics spreading through specific portions of the network. ISO/IEC 27001 – like other norms and standards – are internal mechanisms of control that limit the freedom of individual agents within the network with the goal of achieving higher system efficiency. The key questions for future research, which can be answered through a CAS perspective, are related to the role of ISO/IEC 27001 in guaranteeing ISS at the level of the supply chain/business ecosystem and the presence of possible performance trade-offs, for instance related to lower flexibility in suppliers' selection. Moreover, future studies can investigate the role of ISO/IEC 27001 and other ISS standards in supporting/impeding network reconfiguration against changes in the external environment, e.g. the rapid

changes triggered by the current pandemic outlined in the previous section. Moreover, it is possible to identify how ISS approaches spread through specific portions of the network, e.g. platform operators vs ecosystem participants, downstream vs upstream firms along manufacturing supply chains.

In sum, we believe that our reasoning may provide a fresh perspective on the knowledge gaps on ISO/IEC 27001. ISS requires broad interdisciplinary approaches because of the technical and societal nature of the issue coupled with the broad range of stakeholders' interests involved (Siedlok and Hibbert, 2014). For managerial and organizational disciplines, however, the study of ISS is still in many respects an uncharted territory. social systems thinking may provide a great entry point for researchers of different backgrounds to engage in issues that are increasingly relevant for managers in the emerging technological and business landscape.

6. Conclusions

The aim of this study was to map the state of the literature on ISO/IEC 27001 and formulate a theory-based research agenda at the intersection between IS and managerial disciplines, including quality management. The main insights and research challenges – also related to the increasing digitalization brought about by the current COVID-19 pandemic – were discussed, leading to the formulation of a theory-based research agenda grounded on social systems thinking.

This paper contributes to the academic literature in at least two ways. First, it provides an overview of the current knowledge of the standard, highlighting emerging themes and open issues, thereby providing solid foundations for future research on the topic. Second, it explicitly indicates a set of research opportunities, considering ISO/IEC 27001 as part of a system of standard and practices and in the context of networks of business relations. Drawing from Seuring *et al.* (2020) indications, we borrowed three theories related to social systems thinking to read the results of our analysis through new lenses. This enabled us to problematize the assumption behind ISO/IEC 27001 research as a firm-level phenomenon. We are confident that our study can be seen as a springboard for interdisciplinary research on the matter, including quality, supply chain and operations and human resource management.

The study delivers some implications for policymakers and corporate managers. Overall, we provide a comprehensive overview on the body of knowledge on the standard, allowing for a better understanding of motivations, implementation process and possible performance implications. Managers interested in implementing the standard can read these findings to better understand the implications of being certified as well as to focus potential issues related to the high flexibility of the guidelines, the lack of leadership support and the involvement of external consultants. Policymakers can leverage our results to inform promotion and regulatory activities aimed at sustaining the diffusion of the standard. In any case, the paper argues for a system-level view in ISS. We urge decision-makers to analyze the context in which information is exchanged and the governance of ISS within such context. The issue is topical considering the increasing relevance of digital ecosystems.

To conclude, ISS and the ISO/IEC 27001 standard are still treated by academia as a technical topic; comparatively few studies adopt a managerial perspective. Today, a change of course is required in front of an increasingly interconnected world, emerging technological opportunities and related challenges. If it holds true that data is the "new oil," then a substantial increase in the research effort is needed to understand how organizations may secure information assets and what role major international standards play in providing guidance against an ever-increasing complexity.

ORCID iDs
Matteo Podrecca http://orcid.org/0000-0003-1130-8759
Marco Sartor http://orcid.org/0000-0001-9286-1382

References

Accerboni, F. and Sartor, M. (2019), "ISO/IEC 27001", in Sartor, M. and Orzes, G. (Eds), *Quality Management: Tools, Methods, and Standards*, Emerald Publishing, Bingley, pp. 245-264.

Aguliyev, R., Imamverdiyev, Y. and Sukhostat, L. (2018), "Cyber-physical systems and their security issues", *Computers in Industry*, Vol. 100, pp. 212-223.

Akowuah, F., Yuan, X., Xu, J. and Wang, H. (2013), "A survey of security standards applicable to health information systems", *International Journal of Information Security and Privacy*, Vol. 7 No. 4, pp. 22-36.

Al-Karaki, J.N., Gawanmeh, A. and El-Yassami, S. (2020), "GoSafe: on the practical characterization of the overall security posture of an organization information system using smart auditing and ranking", *Journal of the King Saud University – Computer and Information Sciences*. doi: 10.1016/j.jksuci.2020.09.011.

Almeida, L. and Respício, A. (2018), "Decision support for selecting information security controls", *Journal of Decision Systems*, Vol. 27 suppl. 1, pp. 173-180.

Annarelli, A., Nonino, F. and Palombi, G. (2020), "Understanding the management of cyber resilient systems", *Computers and Industrial Engineering*, Vol. 149, 106829.

Antonucci, D. (2017), *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Wiley, Hoboken.

Ardito, L., Messeni Petruzzelli, A., Panniello, U. and Garavelli, A.C. (2019), "Towards Industry 4.0: mapping digital technologies for supply chain management-marketing integration", *Business Process Management Journal*, Vol. 29 No. 2, pp. 910-936.

Armeanu, S.D., Vintila, G. and Gherghina, S.C. (2017), "A cross-country empirical study towards the impact of following ISO management system standards on Euro-area economic confidence", *Amfiteatru Economic*, Vol. 19 No. 44, pp. 144-165.

Arnason, S.T. and Willett, K.D. (2007), *How to Achieve 27001 Certification: An Example of Applied Compliance Management*, CRC Press, Boca Raton.

Asai, T. and Hakizabera, A.U. (2010), "Human-related problems of information security in East African cross-cultural environments", *Information Management and Computer Security*, Vol. 18 No. 5, pp. 328-338.

Bakar, Z.A., Yaacob, N.A. and Udin, Z.M. (2015), "The effect of business continuity management factors on organizational performance: a conceptual framework", *International Journal of Economics and Financial Issues*, Vol. 5 No. 1S, pp. 128-134.

Bamakan, S.M.H. and Dehghanimohammadabadi, M. (2015), "A weighted Monte Carlo simulation approach to risk assessment of information security management system", *International Journal of Enterprise Information Systems*, Vol. 11 No. 4, pp. 63-78.

Barafort, B., Mesquida, A.L. and Mas, A. (2017), "Integrating risk management in IT settings from ISO standards and management systems perspectives", *Computer Standards and Interfaces*, Vol. 54 No. 3, pp. 176-185.

Barafort, B., Mesquida, A.L. and Mas, A. (2018), "Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context", *Computer Standards and Interfaces*, Vol. 60, pp. 57-66.

Barafort, B., Mesquida, A.L. and Mas, A. (2019), "ISO 31000-based integrated risk management process assessment model for IT organizations", *Journal of Software: Evolution and Process*, Vol. 31 No. 1, e1984.

Barlette, Y. and Fomin, V.V. (2010), "The adoption of information security management standards: a literature review", Information Resources Management Association (Ed.), *Information Resources Management: Concepts, Methodologies, Tools and Applications*, IGI Global, Hershey, pp. 69-90.

Barney, J. (1991), "Firm resources and sustained competitive advantage", *Journal of Management*, Vol. 17 No. 1, pp. 99-120.

Başaran, B. (2016), "The effect of ISO quality management system standards on industrial property rights in Turkey", *World Patent Information*, Vol. 45, pp. 33-46.

Beckers, K. (2015), *Pattern and Security Requirements: Engineering-Based Establishment of Security Standards*, Springer, Berlin.

Beckers, K., Côté, I., Faßbender, S., Heisel, M. and Hofbauer, S. (2013), "A pattern-based method for establishing a cloud-specific information security management system", *Requirements Engineering*, Vol. 18 No. 4, pp. 343-395.

Beckers, K., Dürrwang, J. and Holling, D. (2016), "Standard compliant hazard and threat analysis for the automotive domain", *Information*, Vol. 7 No. 3, pp. 1-35.

Benitez, G.B., Ayala, N.F. and Frank, A.G. (2020), "Industry 4.0 innovation ecosystems: an evolutionary perspective on value cocreation", *International Journal of Production Economics*, Vol. 228, 107735.

Bettaieb, S., Shin, S.Y., Sabetzadeh, M., Briand, L.C., Garceau, M. and Meyers, A. (2019), "Using machine learning to assist with the selection of security controls during security assessment", *Empirical Software Engineering*, Vol. 25, pp. 2550-2582.

Bititci, U., Garengo, P., Dörfler, V. and Nudurupati, S. (2012), "Performance measurement: challanges for tomorrow", *International Journal of Management Reviews*, Vol. 14 No. 3, pp. 305-327.

Blackburn, S., LaBerge, L., O'Toole, C. and Schneider, J. (2020), *Digital Strategy in a Time of Crisis*, McKinsey Digital, available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20strategy%20in%20a%20time%20of%20crisis/Digital-strategy-in-a-time-of-crisis-final.ashx (accessed 20 April 2020).

Boehm, J., Kaplan, J., Sorel, M., Sportsman, N. and Steen, T. (2020), *Cybersecurity Tactics for the Coronavirus Pandemic*, McKinsey Quarterly, available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20tactics%20for%20the%20coronavirus%20pandemic/Cybersecurity-tactics-for-the-coronavirus-pandemic-vF.ashx (accessed 14 May 2020).

Boiral, O. and Henri, J.F. (2012), "Modelling the impact of ISO 14001 on environmental performance: a comparative approach", *Journal of Environmental Management*, Vol. 99, pp. 84-97.

Boiral, O., Guillaumie, L., Heras-Saizarbitoria, I. and Tayo Tene, C.V. (2018), "Adoption and Outcomes of ISO 14001: a systematic review", *International Journal of Management Reviews*, Vol. 20 No. 2, pp. 411-432.

Boulding, K. (1956), "General systems theory - the skeleton of science", *Management Science*, Vol. 2 No. 3, pp. 197-208.

Bounagui, Y., Mezrioui, A. and Hafiddi, H. (2019), "Toward a unified framework for Cloud Computing governance: an approach for evaluating and integrating IT management and governance models", *Computer Standards and Interfaces*, Vol. 62, pp. 98-118.

Breslin, D., Gatrell, C. and Bailey, K. (2020), "Developing insights through reviews: reflecting on the 20th anniversary of the international journal of management reviews", *International Journal of Management Reviews*, Vol. 22 No. 1, pp. 3-9.

Broderick, J.S. (2006), "ISMS, security standards and security regulations", *Information Security Technical Report*, Vol. 11 No. 1, pp. 26-31.

Burns, A.J., Posey, C., Courtney, J.F., Roberts, T.L. and Nanayakkara, P. (2017), "Organizational information security as a complex adaptive system: insights from three agent-based models", *Information Systems Frontiers*, Vol. 19 No. 3, pp. 509-524.

Burt, A. (2019), "Cybersecurity is putting customer trust at the center of competition", *Harvard Business Review*, available at: https://hbr.org/2019/03/cybersecurity-is-putting-customer-trust-at-the-center-of-competition (accessed 03 May 2020).

Büyüközkan, G. and Göçer, F. (2018), "Digital Supply Chain: literature review and a proposed framework for future research", *Computers in Industry*, Vol. 97, pp. 157-177.

Calder, A. (2005), *Nine Steps to Success: An ISO27001 Implementation Overview*, IT Governance Publishing, Ely.

Calder, A. (2006a), *Implementing Information Security Based on ISO 27001/ISO 27002*, Van Haren, 's-Hertogenbosch.

Calder, A. (2006b), *Information Security Based on ISO 27001/ISO 27002*, Van Haren, 's-Hertogenbosch.

Calder, A. (2008), "ISO 27001 and ISO 17999", in Tarantino, A. (Ed.), *Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*, John Wiley & Sons, Hoboken, pp. 169-179.

Calder, A. (2010), "Leveraging ISO 27001", in Calder, A. (Ed.), *Selling Information Security to the Board: A Primer*, IT Governance Publishing, Ely, pp. 46-49.

Calder, A. (2018), "Alignment with other frameworks", in Calder, A. (Ed.), *NIST Cybersecurity Framework: A Pocket Guide*, IT Governance Publishing, Ely, pp. 63-68.

Calder, A. and Geraint, W. (2008), "The PCI DSS and ISO/IEC 27001", in Calder, A. and Carter, N. (Eds), *PCI DSS: A Pocket Guide*, IT Governance Publishing, Ely, pp. 38-39.

Calder, A. and Moir, M. (2009a), "The IT management system of tomorrow", in Calder, A. and Moir, S. (Eds), *IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT*, IT Governance Publishing, Ely, pp. 165-183.

Calder, A. and Moir, S. (2009b), "IT regulatory compliance", in Calder, A. and Moir, S. (Eds), *IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT*, IT Governance Publishing, Ely, pp. 40-45.

Calder, A. and Watkins, S. (2008), *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002*, Kogan Page, London.

Calder, A. and Watkins, S.G. (2010), *Information Security Risk Management for ISO27001/ISO27002*, IT Governance Publishing, Ely.

Carter, C.R., Rogers, D.S. and Choi, T.Y. (2015), "Towards the theory of the supply chain", *Journal of Supply Chain Management*, Vol. 51 No. 2, pp. 89-97.

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

Cavusoglu, H., Cavusoglu, H., Son, J.-Y. and Benbasat, I. (2015), "Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources", *Information Management*, Vol. 52 No. 4, pp. 385-400.

Checkland, P. (1997), *Systems Thinking, Systems Practice*, John Wiley & Sons, Chichester.

Choi, T.Y., Dooley, K.J. and Rungtusanatham, M. (2001), "Supply networks and complex adaptive systems: control versus emergence", *Journal of Operations Management*, Vol. 19 No. 3, pp. 351-366.

Coase, R.H. (1937), "The nature of the firm", *Economica*, Vol. 4 No. 16, pp. 386-405.

Corallo, A., Lazoi, M. and Lezzi, M. (2020), "Cybersecurity in the context of Industry 4.0: a structured classification of critical assets and business impacts", *Computers in Industry*, Vol. 114, 103165.

Cots, S. and Casadesús, M. (2015), "Exploring the service management standard ISO 20000", *Total Quality Management and Business Excellence*, Vol. 26 Nos 5-6, pp. 515-533.

Cowan, D. (2011), "External pressure for internal information security controls", *Computer Fraud and Security*, Vol. 2011 No. 11, pp. 8-11.

Crowder, M. (2013), "Quality standards: integration within a bereavement environment", *The TQM Journal*, Vol. 25 No. 1, pp. 18-28.

Culot, G., Fattori, F., Podrecca, M. and Sartor, M. (2019), "Addressing industry 4.0 cybersecurity challenges", *IEEE Engineering Management Review*, Vol. 47 No. 3, pp. 79-86.

Culot, G., Orzes, G., Sartor, M. and Nassimbeni, G. (2020), "The future of manufacturing: a Delphi-based scenario analysis on Industry 4.0", *Technological Forecasting and Social Change*, Vol. 157, 120092.

Darnall, N. (2006), "Why firms mandate ISO 14001 certification", *Business and Society*, Vol. 45 No. 3, pp. 354-381.

Deane, J.K., Goldberg, D.M., Rakes, T.R. and Rees, L.P. (2019), "The effect of information security certification announcements on the market value of the firm", *Information Technology and Management*, Vol. 20 No. 3, pp. 107-121.

Deloitte (2020), "COVID-19's impact on cybersecurity", available at: https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html (accessed 21 May 2020).

Dhillon, G., Syed, R. and Sà-Soares, F.D. (2017), "Information security concerns in IT outsourcing: identifying (in)congruence between clients and vendors", *Information Management*, Vol. 54 No. 4, pp. 452-464.

Diamantopoulou, V., Tsohou, A. and Karyda, M. (2020), "From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls", *Information and Computer Security*, Vol. 28 No. 4, pp. 645-662.

DiMaggio, P.J. and Powell, W.W. (1983), "The iron cage revisited: institutional isomorphism and collective rationality in organizational fields", *American Sociological Review*, Vol. 48 No. 2, pp. 147-160.

Dionysiou, I. (2011), "An investigation on compliance with ISO 27001 in Cypriot private and public organisations", *International Journal of Services and Standards*, Vol. 7 Nos 3-4, pp. 197-234.

Dionysiou, I., Kokkinaki, A., Magirou, S. and Iacovou, T. (2015), "Adoption of ISO 27001 in Cyprus enterprises: current state and challenges", in Khosrow-Pour, M. (Ed.), *Standards and Standardization: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, pp. 994-1017.

Dos Santos Ferreira, R., Frogeri, R.F., Coelho, A.B. and Piurcosky, F.P. (2018), "Information security management practices: study of the influencing factors in a Brazilian Air Force institution", *Journal of Information Systems and Technology Management*, Vol. 15, pp. 1-22.

Duriau, V.J., Reger, R.K. and Pfarrer, M.D. (2007), "A content analysis of the content analysis literature in organization studies: research themes, data sources, and methodological refinements", *Organizational Research Methods*, Vol. 10 No. 1, pp. 5-34.

D'Arcy, J. and Teh, P.-L. (2019), "Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization", *Information Management*, Vol. 56 No. 7, 103151.

Erkonen, S. (2008), "ISO standards draft content", in Tipton, H.F. and Krause, M. (Eds), *Information Security Management Handbook*, Auerbach Publications, Boca Raton, pp. 265-272.

Ernst and Young (2008), "Global information security survey: moving beyond compliance", available at: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/2008_E&YWhitePaper_GlobalInfoSecuritySurvey.pdf (accessed 19 December 2019).

Everett, C. (2011), "Is ISO 27001 worth it?", *Computer Fraud and Security*, Vol. 2011 No. 1, pp. 5-7.

Faruq, B.A., Herlianto, H.R., Simbolon, S.P.H., Utama, D.N. and Wibowo, A. (2020), "Integration of ITIL V3, ISO 20000 and ISO 27001:2013 for IT services and security management system", *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9 No. 3, pp. 3514-3531.

Feng, N., Cheng, Y., Feng, H., Li, D. and Li, M. (2020), "To outsource or not: the impact of information leakage risk on information security strategy", *Information Management*, Vol. 57 No. 5, 103215.

Freeman, R. (1984), *Strategic Management: A Strategic Approach*, Pitman, Boston.

Freeman, E.H. (2007), "Holistic information security: ISO 27001 and due care", *Information Systems Security*, Vol. 16 No. 5, pp. 291-294.

Fuentes, C., Lizarzaburu, E.R. and Vivanco, E. (2011), "Norms and International Standards related to reduce risk management: a literature review", *Risk Governance and Control: Financial Markets and Institutions*, Vol. 1 No. 3, pp. 58-73.

Ganji, D., Kalloniatis, C., Mouratidis, H. and Gheytassi, S.M. (2019), "Approaches to develop and implement ISO/IEC 27001 standard – information security management systems: a systematic literature review", *International Journal on Advances in Software*, Vol. 12 Nos 3-4, pp. 228-238.

Gartner (2018), "Cybersecurity and digital risk management: CIOs Must engage and prepare", *Gartner Research*, available at: https://www.gartner.com/en/doc/3846477-cybersecurity-and-digital-risk-management-cios-must-engage-and-prepare (accessed 02 May 2020).

Gaşpar, M.L. and Popescu, S.G. (2018), "Integration of the gdpr requirements into the requirements of the sr en iso/iec 27001: 2018 standard, integration security management system in a software development company", *Acta technica napocensis-series: Applied Mathematics, Mechanics, and Engineering*, Vol. 61 No. 3, pp. 85-96.

Gillies, A. (2011), "Improving the quality of information security management systems with ISO27000", *The TQM Journal*, Vol. 23 No. 4, pp. 367-376.

Hagiu, A. and Wright, J. (2020), "When data creates competitive advantage", *Harvard Business Review*, Vol. 98 No. 1, pp. 94-101.

Hannigan, L., Deyab, G., Al Thani, A., Al Marri, A. and Afifi, N. (2019), "The implementation of an integrated management system at Qatar biobank", *Biopreservation and Biobanking*, Vol. 17 No. 6, pp. 506-511.

Harari, Y.N. (2020), "The world after coronavirus", *Financial Times*, available at: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (accessed 21 May 2020).

Heras-Saizarbitoria, I. and Boiral, O. (2013), "ISO 9001 and ISO 14001: towards a research agenda on management system standards", *International Journal of Management Reviews*, Vol. 15 No. 1, pp. 47-65.

Heston, K.M. and Phifer, W. (2011), "The multiple quality models paradox: how much 'best practice'is just enough?", *Journal of Software Maintenance and Evolution: Research and Practice*, Vol. 23 No. 8, pp. 517-531.

Hinz, O., Nofer, M., Schiereck, D. and Trilling, J. (2015), "The influence of data theft on the share prices and systematic risk of consumer electronics companies", *Information Management*, Vol. 52 No. 3, pp. 337-347.

Hlača, B., Aksentijević, S. and Tijan, E. (2008), "Influence of ISO 27001: 2005 on the port of rijeka security", *Pomorstvo: Scientific Journal of Maritime Research*, Vol. 22 No. 2, pp. 245-258.

Ho, L.H., Hsu, M.T. and Yen, T.M. (2015), "Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL", *Information and Computer Security*, Vol. 23 No. 2, pp. 161-177.

Honan, B. (2009), *ISO27001 in a Windows Environment: The Best Practice Handbook for a Microsoft Windows Environment*, IT Governance Publishing, Ely.

Hooper, V. and McKissack, J. (2016), "The emerging role of the CISO", *Business Horizons*, Vol. 59 No. 6, pp. 585-591.

Hoy, Z. and Foley, A. (2015), "A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits", *Total Quality Management and Business Excellence*, Vol. 26 Nos 5-6, pp. 690-702.

Humphreys, E. (2007), *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Norwood.

Iansiti, M. and Lakhani, R.K. (2020), "Competing in the age of AI", *Harvard Business Review*, Vol. 98, pp. 60-67.

ISO (2019), "The ISO survey of management system standard certifications 2018", available at: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 (accessed 12 January 2020).

IT Governance Privacy Team Team (2016), *Eu General Data Protection Regulation (GDPR)–An Implementation and Compliance Guide*, IT Governance Publishing, Ely.

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F. and Daas, F. (2014), "Developing an ISO27001 information security management system for an Educational Institute: hashemite university as a case study", *Jordan Journal of Mechanical and Industrial Engineering*, Vol. 8 No. 2, pp. 102-118.

Jabbour, C.J.C. (2015), "Environmental training and environmental management maturity of Brazilian companies with ISO14001: empirical evidence", *Journal of Cleaner Production*, Vol. 96, pp. 331-338.

Jacobides, M.G., Cennamo, C. and Gawer, A. (2018), "Towards a theory of ecosystems", *Strategic Management Journal*, Vol. 39 No. 8, pp. 2255-2276.

Jeong, C.Y., Lee, S.-Y.-T. and Lim, J.-H. (2019), "Information security breaches and IT security investments impacts on competitors", *Information Management*, Vol. 56 No. 5, pp. 681-695.

Kache, F. and Seuring, S. (2017), "Challanges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management", *International Journal of Operations and Production Management*, Vol. 37 No. 1, pp. 10-36.

Katz, D. and Kahn, R.L. (1978), *The Social Psychology of Organizations*, Wiley, New York.

Khajouei, H., Kazemi, M. and Moosavirad, S.H. (2017), "Ranking information security controls by using fuzzy analytic hierarchy process", *Information Systems and e-Business Management*, Vol. 15 No. 1, pp. 1-19.

Kossyva, D.I., Galanis, K.V., Sarri, K.K. and Georgopoulos, N.B. (2014), "Adopting an information security management system in a co-opetition strategy context", *International Journal of Applied Systemic Studies*, Vol. 5 No. 3, pp. 215-228.

Ku, C., Chang, Y. and Yen, D.C. (2009), "National information security policy and its implementation: a case study in Taiwan", *Telecommunications Policy*, Vol. 33 No. 7, pp. 371-384.

Leszczyna, R. (2019), "Standards with cybersecurity controls for smart grid—a systematic analysis", *International Journal of Communication Systems*, Vol. 32 No. 6, e3910.

Lezzi, M., Lazoi, M. and Corallo, A. (2018), "Cybersecurity for Industry 4.0 in the current literature: a reference framework", *Computers in Industry*, Vol. 103, pp. 97-110.

Liao, K.H. and Chueh, H.E. (2012a), "An evaluation model of information security management of medical staff", *International Journal of Innovative Computing, Information and Control*, Vol. 8 No. 11, pp. 7865-7873.

Liao, K.H. and Chueh, H.E. (2012b), "Medical organization information security management based on ISO27001 information security standard", *Journal of Software*, Vol. 7 No. 4, pp. 792-797.

Lomas, E. (2010), "Information governance: information security and access within a UK context", *Records Management Journal*, Vol. 20 No. 2, pp. 182-198.

Lopes, I.M., Guarda, T. and Oliveira, P. (2019), "Implementation of ISO 27001 standards as GDPR compliance facilitator", *Journal of Information Systems Engineering and Management*, Vol. 4 No. 2, em0089.

Lowry, P.B., Dinev, T. and Willson, R. (2017), "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 546-563.

Luhmann, N. (1995), *Social Systems*, Stanford University Press, Stanford.

Luhmann, N. (2013), *Introduction to Systems Theory*, Polity Press, Cambridge.

Majerník, M., Daneshjo, N., Chovancová, J. and Sanciova, G. (2017), "Design of integrated management systems according to the revised ISO standards", *Polish Journal of Management Studies*, Vol. 15 No. 1, pp. 135-143.

Manders, B., de Vries, H.J. and Blind, K. (2016), "ISO 9001 and product innovation: a literature review and research framework", *Technovation*, Vols 48-49, pp. 41-55.

Markus, M.L. (2015), "New games, new rules, new scoreboards: the potential consequences of big data", *Journal of Information Technology*, Vol. 30 No. 1, pp. 58-59.

Mayring, P. (2000), "Quantitative content analysis", *Forum for Qualitative Social Research*, Vol. 1 No. 2, pp. 1-10.

McKinsey and Company (2019), "Perspectives on transforming cybersecurity", available at: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx (accessed 10 June 2019).

Mele, C., Pels, J. and Polese, F. (2010), "A brief review of systems theories and their managerial applications", *Service Science*, Vol. 2 Nos 1-2, pp. 126-135.

Mesquida, A.L., Mas, A., Feliu, T.S. and Arcilla, M. (2014), "MIN-ITs: a framework for integration of it management standards in mature environments", *International Journal of Software Engineering and Knowledge Engineering*, Vol. 24 No. 6, pp. 887-908.

Meyer, J.W. and Rowan, B. (1977), "Institutionalized organizations: formal structure as myth and ceremony", *American Journal of Sociology*, Vol. 83 No. 2, pp. 340-363.

Mirtsch, M., Kinne, J. and Blind, K. (2021), "Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web-mining based analysis", *IEEE Transactions on Engineering Management*, Vol. 68 No. 1, pp. 87-100.

Montesino, R., Fenz, S. and Baluja, W. (2012), "SIEM-based framework for security controls automation", *Information Management and Computer Security*, Vol. 20 No. 4, pp. 248-263.

Mukhtar, Z. and Ahmad, K. (2014), "Internal threat control framework based on information security management system", *Journal of Theoretical and Applied Information Technology*, Vol. 70 No. 2, pp. 316-323.

Nadler, D.A. and Tushman, M.L. (1980), "A model for diagnosing organizational behavior", *Organizational Dynamics*, Vol. 9 No. 2, pp. 35-51.

Nadler, D.A. and Tushman, M.L. (1984), "A congruence model for diagnosing organizational behavior", in Kolb, D.A., Rubin, J.M. and McIntyre, J.M. (Eds), *Organizational Psychology: Reading on Human Behavior in Organizations*, Prentice Hall, Englewood Cliffs, pp. 587-603.

Nair, A. and Prajogo, D. (2009), "Internalization of ISO 9000 standards: the antecedent role of functionalist and institutionalist drivers and performance implications", *International Journal of Production Research*, Vol. 47 No. 16, pp. 4545-4568.

Narasimhan, R., Schoenherr, T., Jacobs, B.W. and Kim, M.K. (2015), "The financial impact of FSC certification in the United States: a contingency perspective", *Decision Sciences*, Vol. 46 No. 3, pp. 527-563.

Niemimaa, E. and Niemimaa, M. (2017), "Information systems security policy implementation in practice: from best practices to situated practices", *European Journal of Information Systems*, Vol. 26 No. 1, pp. 1-20.

Orzes, G., Moretto, A.M., Ebrahimpour, M., Sartor, M., Moro, M. and Rossi, M. (2018), "United nations global compact: literature review and theory-based research agenda", *Journal of Cleaner Production*, Vol. 177, pp. 633-654.

Ozkan, S. and Karabacak, B. (2010), "Collaborative risk method for information security management practices: a case context within Turkey", *International Journal of Information Management*, Vol. 30 No. 6, pp. 567-572.

Pagani, M. and Pardo, C. (2017), "The impact of digital technology on relationships in a business network", *Industrial Marketing Management*, Vol. 67, pp. 185-192.

Pardo, C., Pino, F.J., Garcia, F., Piattini, M. and Baldassarre, M.T. (2012), "An ontology for the harmonization of multiple standards and models", *Computer Standards and Interfaces*, Vol. 34 No. 1, pp. 48-59.

Pardo, C., Pino, F.J., Garcia, F., Baldassarre, M.T. and Piattini, M. (2013), "From chaos to the systematic harmonization of multiple reference models: a harmonization framework applied in two case studies", *Journal of Systems and Software*, Vol. 86 No. 1, pp. 125-143.

Pardo, C., Pino, F.J. and Garcia, F. (2016), "Towards an integrated management system (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards", *International Journal of Software Engineering and Its Applications*, Vol. 10 No. 9, pp. 217-230.

Park, S. and Lee, K. (2014), "Advanced approach to information security management system model for industrial control", *The Scientific World Journal*, Vol. 2014, 348305.

Penrose, E. (1959), *The Theory of the Growth of the Firm*, Oxford University Press, Oxford.

Pompon, R. (2016), *IT Security Risk Control Management: An Audit Preparation Plan*, Apress, New York.

Post, C., Sarala, R., Gatrell, C. and Prescott, J.E. (2020), "Advancing theory with review articles", *Journal of Management Studies*, Vol. 57 No. 2, pp. 351-372.

Prajogo, D., Huo, B. and Han, Z. (2012), "The effects of different aspects of ISO 9000 implementation on key supply chain management practices and operational performance", *Supply Chain Management: International Journal*, Vol. 17 No. 3, pp. 306-322.

Raabi, A., Assoul, S., Touhami, K.O. and Roudies, O. (2020), "Information and cyber security maturity models: a systematic literature review", *Information and Computer Security*, Vol. 28 No. 4, pp. 627-644.

Rezaei, G., Ansari, M., Memari, A., Zahraee, S.M. and Shaharoun, A.M. (2014), "A huiristic method for information scaling in manufacturing organizations", *Jurnal Teknologi*, Vol. 69 No. 3, pp. 87-91.

Rezakhani, A., Hajebi, A. and Mohammadi, N. (2011), "Standardization of all information security management systems", *International Journal of Computers and Applications*, Vol. 18 No. 8, pp. 4-8.

Rousseau, D.M., Manning, J. and Denyer, D. (2008), "11 evidence in management and organizational science: assembling the field's full weight of scientific knowledge through syntheses", *The Academy of Management Annals*, Vol. 2 No. 1, pp. 475-515.

Sallos, M.P., Garcia-Perez, A., Bedford, D. and Orlando, B. (2019), "Strategy and organizational cybersecurity: a knowledge-problem perspective", *Journal of Intellectual Capital*, Vol. 20 No. 4, pp. 581-597.

Sartor, M., Orzes, G., Di Mauro, C., Ebrahimpour, M. and Nassimbeni, G. (2016), "The SA8000 social certification standard: literature review and theory-based research agenda", *International Journal of Production Economics*, Vol. 175, pp. 164-181.

Sartor, M., Orzes, G., Touboulic, A., Culot, G. and Nassimbeni, G. (2019), "ISO 14001 standard: literature review and theory-based research agenda", *Quality Management Journal*, Vol. 26 No. 1, pp. 32-64.

Schleicher, D.J., Bauman, H.M., Sullivan, D.W., Levy, P.E., Hargrove, D.C. and Barros-Riveira, B.A. (2018), "Putting the system into performance management systems: a review and agenda for performance management research", *Journal of Management*, Vol. 44 No. 6, pp. 2209-2245.

Schneider, A., Wickert, C. and Marti, E. (2017), "Reducing complexity by creating complexity: a systems theory perspective on how organizations respond to their environments", *Journal of Management Studies*, Vol. 54 No. 2, pp. 182-207.

Schoenherr, T. and Talluri, S. (2013), "Environmental sustainability initiatives: a comparative analysis of plant efficiencies in Europe and the US", *IEEE Transactions on Engineering Management*, Vol. 60 No. 2, pp. 353-365.

Serrado, J., Pereira, R.F., Mira da Silva, M. and Scalabrin Bianchi, I. (2020), "Information security frameworks for assisting GDPR compliance in banking industry", *Digital Policy, Regulation and Governance*, Vol. 22 No. 3, pp. 227-244.

Seuring, S. and Gold, S. (2012), "Conducting content-analysis based literature reviews in supply chain management", *Supply Chain Management: International Journal*, Vol. 17 No. 5, pp. 544-555.

Seuring, S., Yawar, S.A., Land, A., Khalid, R.U. and Sauer, P.C. (2020), "The applications of theory in literature reviews – illustrated with examples from supply chain management", *International Journal of Operations and Production Management*, Vol. 41 No. 1, pp. 1-20.

Sheikhpour, R. and Modiri, N. (2012a), "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management", *Indian Journal of Science and Technology*, Vol. 5 No. 2, pp. 2170-2176.

Sheikhpour, R. and Modiri, N. (2012b), "An approach to map COBIT processes to ISO/IEC 27001 information security management controls", *International Journal of Security and Its Applications*, Vol. 6 No. 2, pp. 13-28.

Siedlok, F. and Hibbert, P. (2014), "The organization of interdisciplinary research: modes, drivers and barriers", *International Journal of Management Reviews*, Vol. 16 No. 2, pp. 194-210.

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

Simić-Draws, D., Neumann, S., Kahlert, A., Richter, P., Grimm, R., Volkamer, M. and Roßnagel, A. (2013), "Holistic and law compatible IT security evaluation: integration of common criteria, ISO 27001/IT-Grundschutz and KORA", *International Journal of Information Security and Privacy*, Vol. 7, pp. 16-35.

Siponen, M. and Willison, R. (2009), "Information security management standards: problems and solutions", *Information Management*, Vol. 46 No. 5, pp. 267-270.

Smith, J. (2020), "Coronavirus upheaval triggers corporate search for supply chain technology", *The Wall Street Journal*, available at: www.wsj.com/amp/articles/coronavirus-upheaval-triggers-corporate-search-for-supply-chain-technology-11588189553 (accessed 20 April 2020).

Smith, S., Winchester, D., Bunker, D. and Jamieson, R. (2010), "Circuits of power: a study of mandated compliance to an information systems security 'de jure' standard in a government organization", *MIS Quarterly*, Vol. 34 No. 3, pp. 463-486.

Spence, M. (1973), "Job market signaling", *Quarterly Journal of Economics*, Vol. 87 No. 3, pp. 355-374.

Spiekermann, S. and Korunovska, J. (2017), "Towards a value theory of personal data", *Journal of Information Technology*, Vol. 32 No. 1, pp. 62-84.

Stevenson, T.H. and Barnes, F.C. (2002), "What industrial marketers need to know now about ISO 9000 certification: a review, update, and integration with marketing", *Industrial Marketing Management*, Vol. 31 No. 8, pp. 695-703.

Stewart, A. (2018), "A utilitarian re-examination of enterprise-scale information security management", *Information and Computer Security*, Vol. 26 No. 1, pp. 39-57.

Stoll, M. (2018), "An information security model for implementing the new ISO 27001", information resources management association", *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, pp. 216-238.

Susanto, H., Almunawar, M.N., Syam, W.P., Tuan, Y.C. and Bakry, S.H. (2011), "I-SolFramework views on ISO 27001", *Asian Transactions on Computers*, Vol. 1 No. 3, pp. 1-10.

Susanto, H., Almunawar, M.N., Syam, W.P. and Tuan, Y.C. (2012), "Information Security Challenge and Breaches: novelty approach on measuring ISO 27001 readiness level", *International Journal of Engineering and Technology*, Vol. 2 No. 1, pp. 67-75.

Tarn, J.M., Raymond, H., Razi, M. and Han, B.T. (2009), "Exploring information security compliance in corporate IT governance", *Human Systems Management*, Vol. 28 No. 3, pp. 131-140.

Tejay, G.P.S. and Shokara, B. (2011), "Reducing cyber harassment through *de jure* standards: a study on the lack of the information security management standard adoption in the USA", *International Journal of Management and Decision Making*, Vol. 11 Nos 5/6, pp. 324-342.

Terlaak, A. and King, A.A. (2006), "The effect of certification with the ISO 9000 Quality Management Standard: a signaling approach", *Journal of Economic Behavior and Organization*, Vol. 60 No. 4, pp. 579-602.

The Economist (2020), "The changes covid-19 is forcing on to business", *Economist*, available at: https://www.economist.com/briefing/2020/04/11/the-changes-covid-19-is-forcing-on-to-business (accessed 20 May 2020).

Ţigănoaia, B. (2015), "Some aspects regarding the information security management system within organizations–adopting the ISO/IEC 27001: 2013 standard", *Studies in Informatics and Control*, Vol. 24 No. 2, pp. 201-210.

Topa, I. and Karyda, M. (2019), "From theory to practice: guidelines for enhancing information security management", *Information and Computer Security*, Vol. 27 No. 3, pp. 326-342.

Tranfield, D., Denyer, D. and Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", *British Journal of Management*, Vol. 14 No. 3, pp. 207-222.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S. (2010), "A security standards' framework to facilitate best practices' awareness and conformity", *Information Management and Computer Security*, Vol. 18 No. 5, pp. 350-365.

Tuczek, F., Castka, P. and Wakolbinger, T. (2018), "A review of management theories in the context of quality, environmental and social responsibility voluntary standards", *Journal of Cleaner Production*, Vol. 176, pp. 399-416.

Uzumeri, M. (1997), "ISO 9000 and other meta-standards: principles for management practice?", *The Academy of Management Executive*, Vol. 11 No. 1, pp. 21-36.

Van Wessel, R., Yang, X. and De Vries, H.J. (2011), "Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study", *Technology Analysis and Strategic Management*, Vol. 23 No. 8, pp. 865-879.

Vance, A., Siponen, M.T. and Straub, D.W. (2020), "Effects of sanctions, moral beliefs, and neutralization on information security policy violations", *Information Management*, Vol. 57 No. 4, 103212.

Vasudevan, V., Mangla, A., Ummer, F., Shetty, S., Pakala, S. and Anbalahan, S. (2008), *Application Security in the ISO27001 Environment*, IT Governance Publishing, Ely.

Venters, W. and Whitley, E.A. (2012), "A critical review of cloud computing: researching desires and reality", *Journal of Information Technology*, Vol. 27 No. 3, pp. 179-197.

Von Bertalanffy, L. (1956), "General system theory", in Emery, F.E. (Ed.), *General System, Yearbook of the Society for the Advancement of General System Theory*, George Braziller, New York.

Von Solms, R. (1999), "Information security management: why standards are important", *Information Management and Computer Security*, Vol. 7 No. 1, pp. 50-58.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *Management Information System Quarterly*, Vol. 26 No. 2, pp. 13-23.

Weinberg, G.M. (2001), *An Introduction to General Systems Thinking*, Dorset House Publishing, New York.

Williamson, O.E. (1985), *The Economic Intstitutions of Capitalism*, Simon and Schuster, New York.

Corresponding author
Marco Sartor can be contacted at: marco.sartor@uniud.it