UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

www.uniud.it

Corso di dottorato di ricerca in:

Ingegneria Industriale e dell'Informazione

XXXV Ciclo

ISO/IEC 27001: An empirical multi-method research

Dottorando
Matteo Podrecca

Supervisore
Prof. Marco Sartor

Anno 2023

To my parents

"A life without a cause is a life without effect"

Paulo Coelho

ABSTRACT

The adoption of digital technologies, the emergence of platform-based business models, and the switch to smart working practices are increasing the number of potential entry points in firms' networks and therefore their potential vulnerabilities. However, despite the relevance of the issue, the managerial debate on the topic is still scant and several research gaps exist. Under this premise, this doctoral thesis touches on the following aspects.

First, by discussing the issue with senior executives and information security experts, it highlights the most relevant information security challenges in the context of Industry 4.0. In doing this, it also shows where current approaches fail short, and what emerging practices are gaining relevance.

Second, by conducting a systematic literature review, the thesis provides a comprehensive synthesis of the academic body of knowledge on ISO/IEC 27001 (i.e., the most renowned international management standard for information security and the fourth most widespread ISO certification) as well as it formulates a theory-based research agenda to inspire future studies at the intersection between information systems and managerial disciplines.

Third, by resorting to Grey models, it investigates the current and future diffusion patterns of ISO/IEC 27001 in the six most important countries in terms of issued certificates.

Fourth, by performing an event study complemented by an ordinary least squares regression on a dataset of 143 US-listed companies, the dissertation sheds light on the performance implications of ISO/IEC 27001 adoption as well as the role of some contextual factors in affecting the outcomes of the adoption.

Overall, this doctoral thesis provides several contributions to both theory and practice. From a theoretical point of view, it highlights the need for managerial disciplines to start addressing information security-related aspects. Moreover, it demonstrates that investments in information security pay off also from a financial perspective. From a practical point of view, it shows the increasingly central role that ISO/IEC 27001 is likely to have in the years to come and it provides managers with evidence on the possible performance effects associated to its adoption.

Keywords: Information security, Cybersecurity, ISO/IEC 27001, ISO 27001, Information systems, Systematic literature review, Secondary data, Grey models, Diffusion, Event study, Performance

TABLE OF CONTENTS

LIST OF TABLES **7**

LIST OF FIGURES **8**

CHAPTER 1. INTRODUCTION **9**

1.1. INFORMATION SECURITY: A NEW MANAGERIAL CHALLENGE 9
1.2. RESEARCH OBJECTIVES 10
1.3. STRUCTURE OF THE THESIS 12
1.4. MAIN CONTRIBUTION 13

CHAPTER 2. INFORMATION SECURITY CHALLENGES IN THE CONTEXT OF INDUSTRY 4.0 ..... **15**

2.1. PURPOSE 15
2.2. TOWARDS A NEW INFORMATION SECURITY PERSPECTIVE IN THE AGE OF INDUSTRY 4.0 15
2.3. METHODOLOGY 17
2.4. FINDINGS: CHALLENGES AND CONCERNS IN INDUSTRY 4.0 CYBERSECURITY MANAGEMENT 18
2.4.1. Managerial challenges *18*
2.4.2. Current frameworks and standards *20*
2.4.3. Emerging practices *21*

CHAPTER 3. ISO/IEC 27001 LITERATURE REVIEW AND RESEARCH DIRECTIONS **24**

3.1. PURPOSE 24
3.2. REVIEW APPROACH 24
3.3. CHARACTERISTICS OF THE LITERATURE 26
3.4. THEMATIC FINDINGS 28
3.4.1. ISO/IEC 27001 and other standards/frameworks *28*
3.4.2. Motivations *31*
3.4.3. Implementation *34*
3.4.4. Outcomes *38*
3.4.5. Context *40*
3.4.6. Themes and topics related to books and book chapters *43*
3.5. SUMMARY AND RESEARCH CHALLENGES 44
3.5.1. Theory-based research agenda *45*

CHAPTER 4. ISO/IEC 27001 DIFFUSION **50**

4.1. PURPOSE 50
4.2. LITERATURE BACKGROUND 50
4.2.1. ISO/IEC 27001 ..... *50*
4.2.2. Diffusion studies *52*
4.2.3. Grey models *54*
4.3. METHODOLOGY 55
4.3.1. Dataset and modelling approach *55*
4.3.2. Grey models *56*
4.3.3. Forecasting performance evaluation *59*
4.3.4. Growth analysis and doubling time *60*
4.4. RESULTS AND DISCUSSION 61
4.4.1. Performance evaluation of the models *61*
4.4.2. Presentation of the findings *65*

CHAPTER 5. PERFORMANCE IMPLICATIONS OF ISO/IEC 27001 CERTIFICATION 72
5.1. PURPOSE 72
5.2. LITERATURE BACKGROUND 72
5.3. RESEARCH FRAMEWORK 75
5.4. METHODOLOGY 79
5.5. RESULTS 86
5.5.1. Event study 86
5.5.2. Ordinary least squares regression 88
5.6. DISCUSSION 89
CHAPTER 6. CONCLUDING REMARKS 92
6.1. SYNOPSIS 92
6.2. CONTRIBUTION 93
6.2.1. Contribution to theory 93
6.2.2. Contribution to practice 94
6.3. LIMITATIONS AND FUTURE RESEARCH 95
REFERENCES 97
APPENDIX 1 126
APPENDIX 2 128

LIST OF TABLES

Table 1: Initial observed managerial challenges 18

Table 2: ISO/IEC 27001 and other standards/frameworks 28

Table 3: Motivations for adopting ISO/IEC 27001 31

Table 4: Implementation of ISO/IEC 27001 34

Table 5: Outcomes of ISO/IEC 27001 38

Table 6: Context of ISO/IEC 27001 40

Table 7: Books and Book chapters on ISO/IEC 27001 43

Table 8: Diffusion studies 53

Table 9: Lewis scale for MAPE evaluation 60

Table 10: ISO/IEC 27001 growth for Japan 61

Table 11: ISO/IEC 27001 growth for China 62

Table 12: ISO/IEC 27001 growth for UK 62

Table 13: ISO/IEC 27001 growth for India 63

Table 14: ISO/IEC 27001 growth for Germany 64

Table 15: ISO/IEC 27001 growth for Italy 64

Table 16: Dataset breakdown by industry and by ISO/IEC 27001 certification year 81

Table 17: Correlation matrix 85

Table 18: Results of the event-study analysis 87

Table 19: Results of the OLS analysis 89

LIST OF FIGURES

Figure 1: Summary of the studies included in the thesis 13

Figure 2: Information security elements for Industry 4.0 17

Figure 3: Coding framework 26

Figure 4: Main characteristics of the contributions included in the review 27

Figure 5: Research agenda 47

Figure 6: Graphical representation of Japan data 68

Figure 7: Graphical representation of China data 69

Figure 8: Graphical representation of UK data 69

Figure 9: Graphical representation of India data 70

Figure 10: Graphical representation of Germany data 70

Figure 11: Graphical representation of Italy data 71

CHAPTER 1. INTRODUCTION

1.1. Information security: a new managerial challenge

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). Moreover, several major attacks and alarming statistics reported in the media have contributed to create a sense of urgency among corporate directors and C-suite executives.

Holistic approaches are required in order 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 (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 & Young, 2008). Among them, ISO/IEC 27001 is probably the most renowned one, being the fourth most widespread ISO certification worldwide following ISO 9001, ISO 14001, and ISO 45001 (ISO, 2022). 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).

Despite the relevance of the topic, 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, 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 ever-increasing connectivity and digitalization. Furthermore, 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 has increased the role of digital technologies in the business environment as well as in daily life.

Against this background, this doctoral thesis aims at shedding light on the aforementioned issues by combining four different papers. It will start with an overview of the phenomenon analysing the main information security challenges in the landscape of Industry 4.0, and then focus on ISO/IEC 27001 by highlighting the state of the art of the academic knowledge on the topic and investigating its diffusion and impact on a firm's performance.

1.2. Research objectives

The four objectives of this thesis are:

Objective 1

Industry 4.0 is exponentially increasing the number of entry points for organizations to defend from nefarious actors. Complex digital value chains expose firms to risks beyond their direct control. The potential damage of cyberattacks is substantial in terms of continuity of business operations, theft of confidential information, and reputational harm. Despite this mounting sense of urgency, there is increasing confusion on what needs to be done and how. C-suite executives and entrepreneurs are puzzled due to the complexity of issues and concerns. Information security professionals, for their part, often fail to make the issue relevant and accessible to non-technical stakeholders. By discussing the issue with senior executives, I tried

to clarify why Industry 4.0 requires an evolving information security perspective, where current approaches fall short and what emerging practices are gaining relevance.

Objective 2

After 15 years of scientific research and in light of its growing popularity, I performed a systematic literature review on ISO/IEC 27001; the most renowned international management standard for information security and the fourth most widespread ISO certification. The review was aimed 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.

Objective 3

Extant research has highlighted several aspects that may hinder the diffusion of ISO/IEC 27001 (e.g., lack of clarity on the outcomes of ISO/IEC 27001 adoption, potential competition with other standards, implementation failure). As a result, after 15 years from ISO/IEC 27001 enactment, the number of issued certificates (85,000 as of 2020) is still lagging when compared with other management system standards (e.g., over the same period ISO 9001 and ISO 14001 were recording, respectively, 560,000 and 245,000 valid certificates - ISO, 2021). Against this background, I developed a study aimed at opening the debate on the future dissemination patterns of ISO/IEC 27001. To achieve these purposes I applied Grey Models (GM) – Even GM (1,1), Even GM (1,1,α,θ), Discrete GM (1,1), Discrete GM (1,1, α) – to the data related to the six most important countries in terms of issued certificates.

Objective 4

Despite its growing popularity, little is known about the financial performance implications of ISO/IEC 27001 for certified companies. Contrasting effects have been highlighted: against IS improvements and higher process efficiency, firms have also experienced lower operational flexibility and possible trade-offs with other business objectives with negative implications on profitability. Moreover, whereas many times the certification decision follows market requests, ISO/IEC 27001 impact on revenues is still a debated issue. Under this premise, I investigated the performance implications of ISO/IEC 27001 adoption by developing a set of theory-

grounded hypotheses that have been tested through a long-term event study complemented by an ordinary least squares regression on a dataset of 143 US-listed companies.

1.3. Structure of the thesis

Following this introduction, the doctoral thesis consists of four papers based on studies already published in international journals (Chapters 2, 3, 5) or currently under review (Chapter 4).

Chapter 2 is adapted from the article "*Addressing industry 4.0 cybersecurity challenges*"[1] authored by Giovanna Culot, Fabio Fattori, Matteo Podrecca, and Marco Sartor. The contribution – published in "*IEEE Engineering Management Review*" – provides an overview of the main information security issues in the context of Industry 4.0. Chapter 3 is adapted from the article "*The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*"[2] authored by Giovanna Culot, Guido Nassimbeni, Matteo Podrecca, and Marco Sartor. It is published in "*The TQM Journal*" and presents the first systematic literature review and research agenda on the ISO/IEC 27001. Chapter 4 is based on the article "*Forecasting the diffusion of ISO/IEC 27001: a Grey model approach*" authored by Matteo Podrecca and Marco Sartor (accepted for publication in "*The TQM Journal*"). It presents the first diffusion analysis on ISO/IEC 27001. Chapter 5 is based on the article "*Information security and value creation: The performance implications of ISO/IEC 27001*", authored by Matteo Podrecca, Giovanna Culot, Guido Nassimbeni, and Marco Sartor. Published in "*Computers in Industry*"[3], it analyses the relationship between the attainment of the ISO/IEC 27001 certification and firms' financial performance as well as it investigates the role of some contextual factors in affecting such relationship. Figure 1 provides an overview of these chapters.

[1]© 2019 IEEE. Reprinted, with permission, from 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. In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of University of Udine's products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink. If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[2]The publisher (Emerald) grants permission for the reuse of published content in dissertations.

[3]The publisher (Elsevier) grants permission for the reuse of published content in dissertations.

To conclude, Chapter 6 summarizes the results of the thesis, highlighting its contribution to theory and practice, as well as acknowledging its main limitations and providing some directions for future research avenues.

Figure 1: Summary of the studies included in the thesis

	Chapter 2	Chapter 3	Chapter 4	Chapter 5
Aim	Provide an overview of the main information security issues in the context of Industry 4.0	Present the academic body of knowledge on ISO/IEC 27001, and highlight potential avenues for future research on the topic	Investigate the future diffusion patterns of ISO/IEC 27001	Investigate the financial performance implications of ISO/IEC 27001 adoption and shed light on the role of some contextual factors that may affect this relationship
Methodology	Empirical – Workshop	Conceptual – Systematic literature review	Empirical – Secondary data analysis	Empirical – Secondary data analysis
Status	PUBLISHED	PUBLISHED	ACCEPTED	PUBLISHED
Reference	Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, Vol. 47 No. 3, pp. 79-86.	Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, Vol. 33 No. 7, pp. 76-105.	Podrecca, M., & Sartor, M. Forecasting the diffusion of ISO/IEC 27001: a Grey model approach *The TQM Journal*.	Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, Vol. 142, 103744.

1.4. Main contribution

This thesis contributes to both theory and practice.

As far as the theoretical contributions are concerned, the four articles contribute to the Operations Management and Quality Management literature in several significant ways. First, Chapter 2 shows that information security is not only a technical issue but requires, above all, managerial approaches. This way it highlights the need for managerial disciplines to start addressing information security-related aspects. Second, Chapter 3 presents and organizes the body of knowledge on ISO/IEC 27001 across several research streams and topics, providing a comprehensive overview targeted at scholars from different fields. Moreover, it adds 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. Third, Chapter 4 proposes the first diffusive analysis on ISO/IEC 27001 drawing a synthesis of previous, ongoing, and future patterns; it provides several hints for scholars to further shed light on the

drivers of its dissemination. Furthermore, it highlights the usefulness of Grey models to investigate and forecast the diffusion trends of international management standards. Fourth, Chapter 5 points out that IS investments pay off also from a financial perspective. It fits in the ongoing debate on the performance implications of IS initiatives, which are generally perceived as "defensive" tools and thus not aimed at any specific value creation opportunity. It also contributes to the literature on management systems conducting the first large-scale academic analysis on ISO/IEC 27001 impact on firms' financial performance.

From a practical point of view, the main implications are as follows. Chapter 2 lays out some emerging approaches to provide a guideline to specialists and managers with a non-information technology (IT) background. Second, the results of Chapter 3 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 chapter 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. Third, Chapter 4 helps companies to align their businesses with global requirements and strengthen their practices related to information security. The certification body (ISO) can find useful insights too: forecasts can be used to understand areas of improvement where to prioritize efforts. Fourth, Chapter 5 provides managers with evidence on the possible performance effects of ISO/IEC 27001 for certified firms. This is relevant for corporate decision-makers beyond technical departments as IS appears characterized by increasing cross-functional and leadership engagement.

CHAPTER 2. INFORMATION SECURITY CHALLENGES IN THE CONTEXT OF INDUSTRY 4.0

2.1. Purpose

The aim of this chapter is to provide an overview of the main information security challenges in the context of Industry 4.0. Specifically, in-depth interviews and a workshop were performed involving ten information security experts.

2.2. Towards a new information security perspective in the age of Industry 4.0

Until recently the focus of information security was to defend organizational perimeters; namely to protect unauthorized access to a privately-owned computer network. The dominant approach was to place safeguards – firewalls, intrusion-detection systems, malware protections – at the entrance of the perimeter to secure it from hackers. This approach is rapidly becoming obsolete as Industry 4.0 is blurring the boundaries between the physical and digital worlds (Tuptuk and Hailes, 2018). By the same token, communication technologies coupled with social and cultural factors are reshaping working habits towards "anywhere, anytime". In particular, the following observations can be made:

- the number of entry points for user access is multiplying through sensors, Wi-Fi connections, the Internet-of-Things (IoT), point-of-sale (POS) terminals and many other sources;
- companies are moving workloads to public clouds and many company-specific controls and practices become ineffective;
- company-owned laptops and mobile phones are also used for private purposes, privately-owned devices are used to access privileged company information and applications;
- networks are increasingly interconnected within the IT environment and with infrastructure and operational technologies environments; and
- data and intellectual property are shared across partners and supply chains, information systems are being integrated between suppliers and customers.

Securing a company one hundred percent is virtually impossible in this distributed and integrated Industry 4.0 context. Information security technologies are evolving fast, including encryption and machine-learning techniques (for a review see Lezzi *et al.*, 2019); although the

issue is broader than that. In front of such permeable, entwined and dynamic networks, controlling everything is not an option. Financial constraints and the adverse impact of information security applications and procedures on organizational speed and agility prevent this goal.

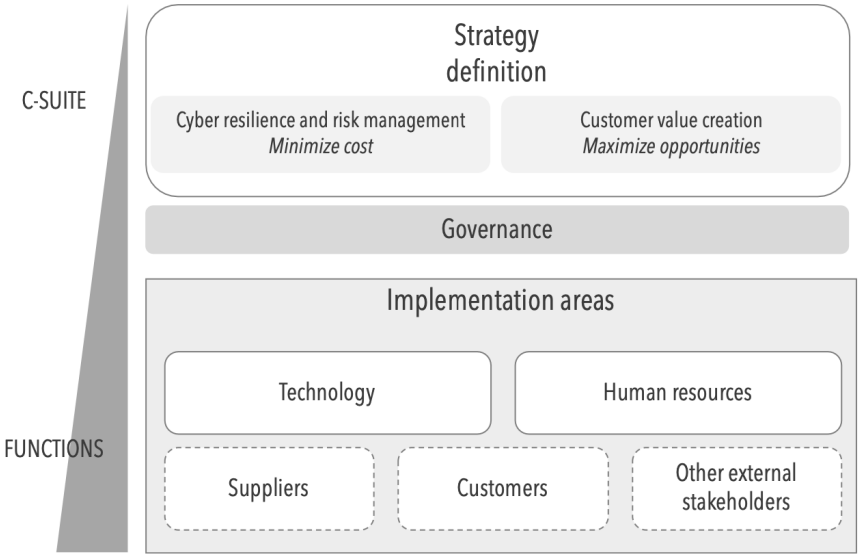
Against this backdrop, information security is first and foremost about ***strategy definition***. Managers are starting to approach the issue through the lenses of *cyber resilience* and *risk management* with the aim of minimizing the costs related to uncertainty and ensuring business operations continuity (BCG, 2019; McKinsey, 2019). By definition, this effort requires several decisions to be taken by cross-functional teams, many at the C-suite level. Another important aspect is how to position information security vis-à-vis the customer. Due to smart products, connected machinery and handling of customer data, many traditional manufacturing and service companies are now seeing information security as an opportunity for *customer value creation*. Secure access, reliable technology, and data protection become a core part of what companies sell; trust is becoming a critical component of commercial interaction (Burt, 2019). Through enhanced security features companies can upgrade their competitive positioning. Additional revenue streams might be generated through information security-related services.

The implementation of this strategic approach to information security involves several functions, not limited to IT. *Technology* is just one of the possible ***areas*** of information security implementation. Equally important, even though oft-forgotten, is to intervene on *human resources* (e.g. Schackelford, 2016). Since the dawn of information systems, users have always been their greatest liability. Employee negligence, malicious behavior, and process failure are still at the roots of the vast majority of successful cyberattacks (BCG, 2017; Greitzer, *et al*., 2019; Sanders, *et al*., 2019). Information security extends also outside the firm boundaries in the Industry 4.0 context. Direct *suppliers* and multi-tier supply chain partners may, therefore, contribute to possible threats (McKinsey, 2019). Similarly, *customers* are involved for connected products and advanced digital services. *Other external stakeholders* appear in relation to information security externalities and cross effects.

These ramifications of information security within and outside companies' fading perimeters require the involvement of multiple functions and strong ***governance***. Leading international practices show the involvement of executive management in orchestrating, monitoring and reporting progress and importance to the board of directors (Antonucci, 2017).

Figure 2 provides a graphical synthesis of the new approach to information security ushered in by Industry 4.0.

Figure 2: Information security elements for Industry 4.0



2.3. Methodology

To pursue the objectives of this chapter, we completed in-depth interviews and a workshop involving ten information security experts. In order to explore possible industry- and size-specific differences, the workshop participants were varied. Each had significant IT experience and especially in information security. Three members were from manufacturing companies (industrial goods and rail transport), two from the retail industry (wholesale and e-commerce), two from applied research institutions, one from the oil & gas sector, one from a certification body and one from an ICT system integrator.

Different firm-sizes were also represented, with one micro-company, two small and medium- sized enterprises and seven large companies ranging from 1,000 to more than 100,000 employees.

Our questions aimed at: *i)* identifying the most relevant challenges of managing information security in the context of Industry 4.0; *ii)* understanding the role of frameworks and standards; and *iii*) exploring emerging practices. Experts comments on this last point have been complemented with findings from the literature.

2.4. Findings: challenges and concerns in Industry 4.0 cybersecurity management

2.4.1. Managerial challenges

Our discussions confirmed the need for a new definition of information security. Expert comments corroborated the view outlined in the previous sections of this chapter. Comments included:

- *Information security needs to now be seen as a strategic, technological and organizational discipline* - Senior ICT Manager, Industrial Goods;

- *No one can define cybersecurity today: many believe it is still about information security but is actually much broader than that* - Cybersecurity Director, Industrial Goods;

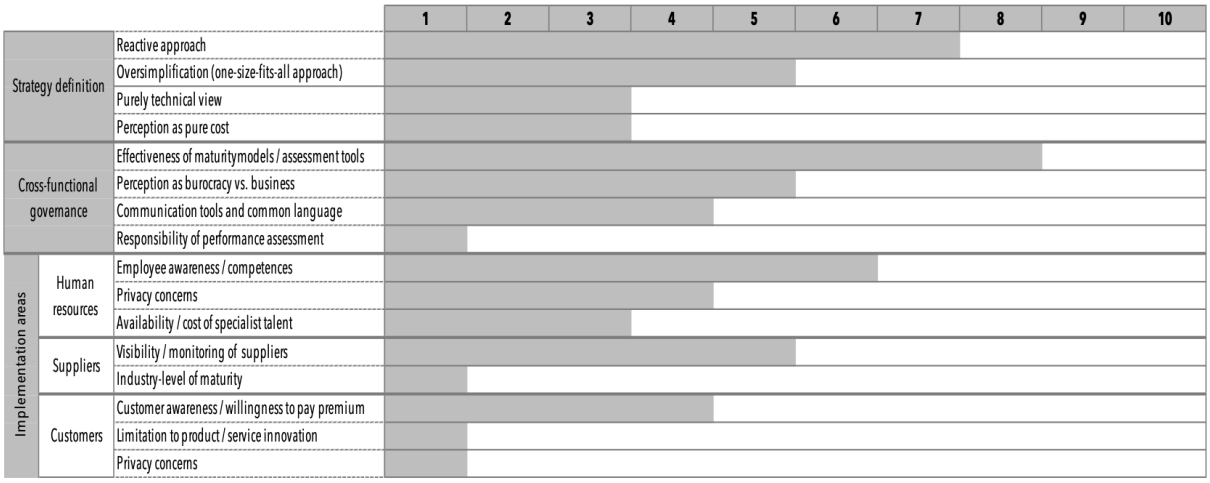
- *It is no longer about managing cyber risks, but about managing the trust. Cybersecurity should enlarge its focus to what is relevant to the customers* - Cybersecurity Director, Retail;

- *Cybersecurity needs to be based on a strategic vision. Change management is the way to translate this vision into reality* - Head of Digital Transformation, Energy;

- *As urban mobility ecosystems are emerging there is an increasing system-level attention to cybersecurity issues* - Chief Digital Officer, Rail transport.

However, several managerial challenges emerge. We asked the panel about past and current issues. A summary of results appears in Table 1 along three major categories of strategy definition, cross-functional governance, and functional applications.

Table 1: Initial observed managerial challenges



Note: *number of occurrences in panel interviews*

Several concerns are related to the involvement of C-suite executives in **strategy definition**. Respondents reported that:

- the attitude of corporate leaders is still flawed by the perception of information security as a *purely technical* issue;
- IT vendors have contributed to an *oversimplification* of the issue by equating the level of spending to the degree of protection. This one-size-fits-all approach has resulted in companies throwing resources at securing not relevant assets while losing agility;
- in traditional manufacturing companies, lack of interest is also related to the perception of information security as *pure cost*, not as a potential lever of value creation; and
- the approach is typically *reactive* rather than planned: information security comes up executive radar just after a major crisis.

These challenges are especially relevant for smaller companies with low level of product or service complexity. Big industrial players with high-tech products are already characterized by a stronger information security culture. However, even when the C-suite is actively involved, substantial hindrances to productive **cross-functional governance** might emerge. In particular, our interviews highlighted:

- the lack of *effective maturity models and assessment tools* to support decision-making in complex of Industry 4.0 environments and to ensure dialogue with managers with a non-technical background;
- unclear *responsibility of information security performance assessment*: more structured companies have their information systems tested for penetration and practices audited by third parties, yet cost-effectiveness and flexibility are seldom questioned;
- the paucity of *communication tools and common language* facilitating value judgments among different functions. Even though information security professionals have long learned to translate cyber risks into metrics relevant for their various counterparts – for example, money for finance, reputation for marketing, machine downtime for operations – there is no agreed-upon vocabulary or indicators; and
- perception of information security outside IT as unnecessary *bureaucracy in clash with business objectives*, with the results of procedure being ignored or requests of exceptions to the rule.

With respect to the **implementation areas** of information security, several challenges have emerged besides technology**,** each focusing on sine important organizational functions. ***Human***

resources need to build competencies and capabilities. *Specialist talent* is lacking, especially in terms of analysts and programmers. Overall organizations are characterized by low *employee awareness and basic information security competences*, e.g., password storage and phishing emails. More advanced companies have also lamented raising *privacy concerns* in terms of employee controls.

Externally to the company, smaller and less structured firms lament the *lack of visibility and monitoring* of their ***suppliers***. Larger companies often implement controls and tests on suppliers' information systems, including these controls into supply contracts. Other companies need to comply with technical specifications on product components, including blacklisting of certain component producers – for example, Chinese producers for a U.S. final client. Overall, however, there is limited control over multi-tier suppliers. In industries with a *low level of cybersecurity maturity,* this might represent a potential threat to data and other IP-protected information.

To conclude, a key concern in relation to ***customers*** and other external stakeholders is their awareness of the importance of information security. Companies experience a *low willingness to pay* for additional product features or services. Along the same lines, customers' information security lack of expertise may limit *product and service innovation*.

In business-to-business settings, customers might be reluctant to take responsibility for information security; often viewed as a complex matter outside their core competencies. In relation to complex smart equipment, excessive client constraints represent limitations to the type of service being offered. Finally, it has been reported that *privacy concerns* are also an important issue in relation to smart products operating in connection with the consumer or in public places.

2.4.2. Current frameworks and standards

Several standards have been issued over the years suggesting an array of information security methodologies, techniques, checklists and assessment tools. The most popular among these standards for IT are the ISO/IEC 27001 on information security management systems issued by the International Organization for Standardization (ISO) and the NIST cybersecurity framework promoted by the US National Institute of Standards and Technology (NIST).

For operational technologies, the most relevant standards are the ANSI-ISA-62433 series, created by the International Society for Automation (ISA) and further developed by the

International Electrotechnical Commission (IEC), and the series of documents, including the C37.240, issued by the Institute of Electrical and Electronic Engineers (IEEE).

Recently the European Telecommunication Standards Institutes (ETSI) has also released the first globally applicable standard for consumer IoT (ETSI TS 103 645) and the European Union Agency for Network and Information Security (ENISA) has published a set of good practices for Industry 4.0 (ENISA, 2018).

In a rapidly evolving scenario like Industry 4.0, these standards have the clear merit of suggesting a structured approach to information security. In particular, the ISO/IEC 27001 and the NIST framework promote a clear definition of roles and responsibilities, encourage a substantial involvement of business leadership and promote risk management practices. They also include a reference control objective list (ISO/IEC 27001) and a self-assessment tool (NIST). Certifications are also a signal to the market about the attention cybersecurity requires.

However, our interviews suggest that managers receive just limited support from these standards. In particular:

- standards are perceived as too complex and bureaucratic, not oriented towards business goals and practical solutions;
- technologies are evolving at an unprecedented pace: the more specific recommendations and checklists risk rapid obsolecence;
- implementation is resource-intensive and time-consuming; and
- often their adoption is cosmetic and not substantial, making it difficult to assess the level of information security of business partners based on the certification.

These findings are confirmed by the analysis of the literature related to the ISO/IEC 27001. Several authors (e.g., Mesquida *et al*., 2014) argue that its generality, which supports broader cross-industry application, make its implementation cumbersome. The intrinsic complexity and uncertainty of cybersecurity would call for more specific practical-oriented setups.

2.4.3. Emerging practices

This section contains elements about the "how-to" of companies to change their information security posture. As this change is happening very rapidly, the goal of this initial mapping is not to be exhaustive, but to provide to managers and researchers an initial list of possible avenues to explore.

The first set of practices relate to information security professionals and their relationship to other functions. In particular, enhanced risk management analyses are increasingly adopted extending classic approaches to cyber risk prioritization. These analyses include the Failure Mode and Effects Analysis (FMEA) and the application of risk priority numbers (RPN) to digital assets. Risks may be also prioritized using more quantitative analytical techniques including Monte Carlo analysis, statistical sums and expected monetary value.

Given the propensity for complex analyses, communication to non-IT functions can be simplified with visualization techniques and digital dashboards. This approach allows managers to read information security-related information at the desired level of detail. Outcome-oriented scorecards are also being adopted to foster cross-functional alignment and clear responsibilities. Overall, technical jargon needs to be mostly avoided.

Companies are also looking for benchmarks, adopting indexes such as multiyear expenditures on information security on overall IT expenditures, cost per risk-adjusted losses or cost per share of infrastructure protected. For building such benchmarks the involvement of the finance department is often needed.

The second set of practices concerns information security governance, namely the definition of roles, responsibilities, reporting lines and mechanisms. There is no agreed-upon best-way to design information security reporting lines. Companies base their organizational design: on the principles of collaboration among risk- and crisis-related functions – Chief Information Officer, Chief Risk Officer, Chief Information Security Officer; centralized responsibilities – core decisions taken by central team, periodic monitoring on affiliates; and proximity to the business – local teams reporting to a central authority.

In order to promote cross-functional dialogue, committee structures are being implemented from the top (the board) - down. A budget is allocated proactively with medium-term visibility. Core company processes are analysed for cyber risk and redesigned to accommodate effective involvement of the information security function – without slowing down normal business operations.

An interesting example of process redesign is how product development addressed information security requirements at one of the companies in our panel. In the development of IoT applications, the upfront application of information security architectures might be excessively time and cost consuming. Therefore, new IoT applications are launched as pilot programs with open, but strictly monitored network connections. Only once the pilot is

validated will the roll-out be structured respecting the information security standard. This approach allows for learning where sensitive issues exist.

Third, forward thinking companies have worked extensively on leadership involvement. In particular, in these companies, top management is actively engaged in internal communication initiatives, such as information security updates or roadshows, and in external communication initiatives serving as information security advocate. Corporate leadership is also often involved in institutional relations with industry associations, universities and regulators with the goal to create a common vision and a collaborative environment.

The fourth set of practices refers to function-specific solutions; in particular emerging in human resource management (HRM) and procurement function. In HRM, more advanced companies are piloting the usage of technology in information security training – such as gamification – and advanced forms of personnel monitoring. These advanced forms may include segmentation of personas rather than individual controls.

In procurement, suppliers are increasingly monitored on a regular basis – for example, using vendor risk rating, second- or third-party penetration tests, service-level agreements. Critical relationships are covered by insurance, even though cyber incidents may have very narrow coverage in actuarial tables. People registries are kept of who has access to company networks including employees, suppliers, and customers.

Finally, companies embracing a new approach to information security are aware of the profound and often difficult adjustments that are required at all levels of the organization. In moving from the as-is to the desired state, change management practices are in place with a multi-year transformation plan (e.g., 3-year plan for one of the companies in the panel), a dedicated budget and stakeholder engagement initiatives.

CHAPTER 3. ISO/IEC 27001 LITERATURE REVIEW AND RESEARCH DIRECTIONS

3.1. Purpose

The aim of this chapter is to develop the first systematic literature review on ISO/IEC 27001. In particular, (1) we collect extant research on ISO/IEC 27001; (2) we systematize and summarize research themes and sub-themes; (3) we identify the gaps of the research; and (4) we provide a research agenda to orient future studies on the topic.

3.2. Review approach

Management system standards are inherently multi-dimensional phenomena that can be analysed according to several research perspectives (Uzumeri, 1997; Heras-Saizarbitoria and Boiral, 2013); we opted thus for a systematic approach to the literature review in order 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: (i) provide a comprehensive overview of the literature on ISO/IEC 27001; (ii) classify themes, sub-themes and type of evidence; (iii) 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: (i) referred to other standards and (ii) merely mentioned the ISO/IEC 27001 without a structured analysis or discussion. We included both theoretical and empirical contributions that: (i) focused specifically on ISO/IEC 27001; (ii) analysed ISO/IEC 27001 together with other standards; (iii) discussed ISS/cybersecurity issues at large with explicit reference to ISO/IEC 27001. This way, 116 contributions were pre-selected, their content was further analysed and their references enabled the identification of other works through a forward/backward citation analysis (Webster and Watson, 2012). This process led to a final list of 96 contributions.

The third step in the process was to analyse 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).

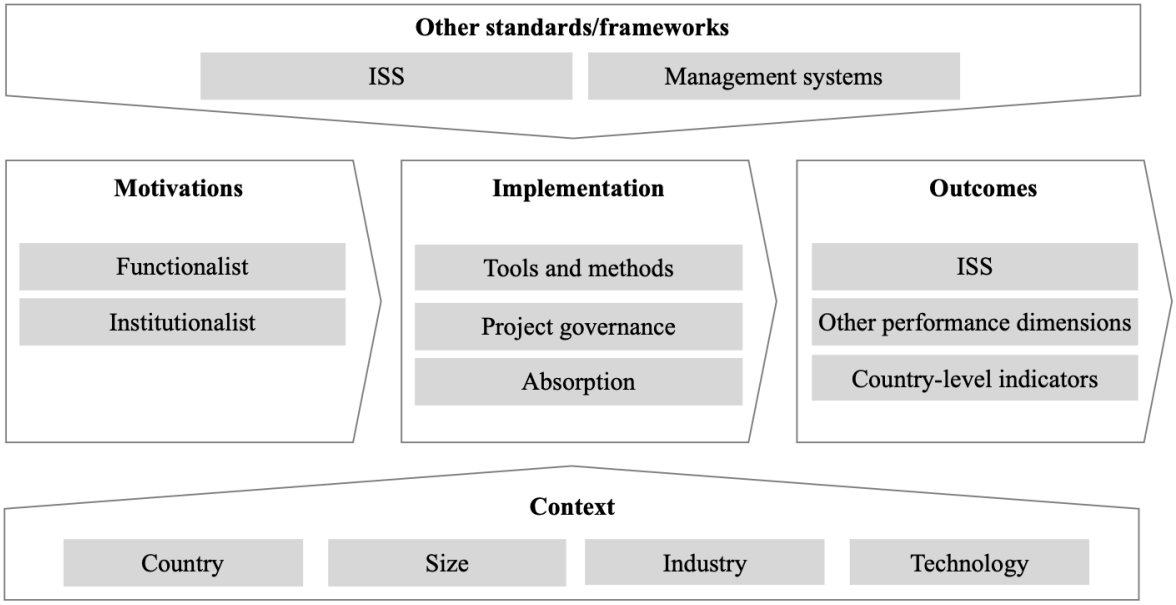
Thereafter, we performed a content analysis on journal articles following Seuring and Gold's (2012) methodological recommendations. The coding categories and main themes included in Figure 3 were defined deductively, drawing from previous literature reviews on other standards and frameworks (e.g., Stevenson 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 in order 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 stand-alone subsection. The coding process followed the same methodological approach as journal articles.

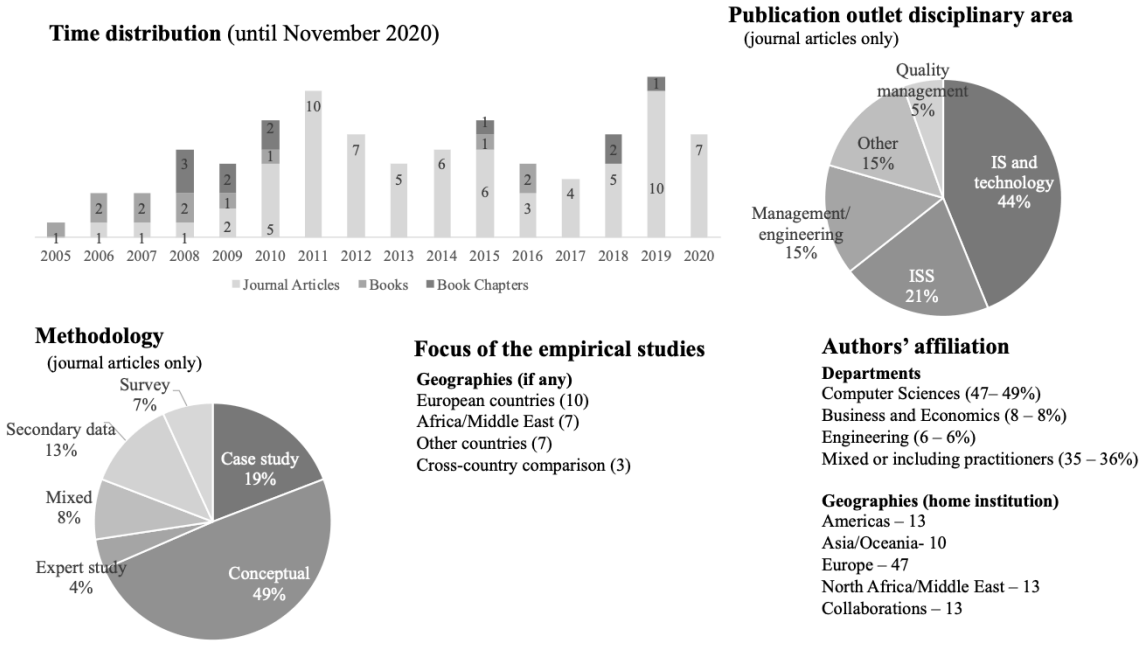
Figure 3: Coding framework



3.3. 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 4; and clarified in the following paragraphs.

Figure 4: Main characteristics of the contributions included in the review



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 6 per year, with an 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 Information Systems literature, either in journals specifically related to information system security 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.* (2020).

3.4. Thematic findings

3.4.1. 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 2.

Table 2: ISO/IEC 27001 and other standards/frameworks

Main themes / Research results	**Relevant papers** *(Evidence: C=conceptual; E=empirical)*
Comparison/integration with other standards with similar scope	
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 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.,* 2020 (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)

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 is long and articulated. In general terms: standards may cover information security at large including 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.* (2022) 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; 2012b; 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 analysed in the literature with respect to other *management 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, the structure, and the 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). Results show that ISO/IEC 27001 is often implemented after ISO 9001 (Mirtsch *et al*., 2020), 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).

3.4.2. 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 *institutional* – 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 3.

Table 3: Motivations for adopting ISO/IEC 27001

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)
Institutional	
ISO/IEC 27001 is pursued for institutional 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.,* 2020 (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)

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 *institutional* 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 last decade has seen a progressive intensification of national (e.g., in the US 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).

3.4.3. 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: *(i)* how effectively ISO/IEC 27001 *tools and methods* provide support to the implementing organization?; *(ii)* how do organizations structure the *project governance*?; *(iii)* what differences in the *actual adoption of practices* have been documented?

The themes and sub-themes identified in the studies are illustrated in Table 4.

Table 4: Implementation of ISO/IEC 27001

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 a*l., 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 a*l., 2014 (E); Ku *et al*., 2009 (E); Liao and Chueh, 2012a (E); Liao and Chueh, 2012b (C); Lomas, 2010 (C); Mirtsch *et al.,* 2020 (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.,* 2020 (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.,* 2020 (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	
Symbolic/informal implementation of the standard	Culot *et al.,* 2019 (E); Everett, 2011 (E); Lomas, 2010 (C); Mirtsch *et al.,* 2020 (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)

As for the efficacy of the *(i) 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 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 towards shared assets – e.g., services and information technology 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 towards ISS.

With regards to the second overarching theme – *(ii) 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 *(iii) 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 regards 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 underinvestigated (Mirtsch *et al.*, 2020).

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).

3.4.4. Outcomes

As illustrated in Table 5, 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) analyse through an event study the impact of the certification on stock market 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).

Table 5: Outcomes of ISO/IEC 27001

Main themes / Research results	**Relevant papers** *(Evidence: C=conceptual; E=empirical)*
Outcomes specific to the scope of the standard	
More efficient risk prevention	Al-Karaki *et al.*, 2022 (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	Cowan, 2011; Hannigan *et al*., 2019 (E); Mirtsch *et al.,* 2020 (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)

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 analysed, 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 analysed 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.

3.4.5. 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 6.

Table 6: Context of ISO/IEC 27001

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.,* 2020 (E)
Different implementation issues related to organizations' size	Al-Karaki *et al.*, 2022 (C); Deane *et al*., 2019 (E); Dionysiou, 2011 (E); Gillies, 2011 (E); Mirtsch *et al.,* 2020 (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.,* 2020 (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.*, 2022 (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.,* 2020 (E); Simić-Draws *et al*., 2013 (C); Smith *et al.,* 2010 (E); Stewart, 2018 (C); Ţigănoaia, 2015 (C); van Wessel *et al*., 2011(E)

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 in order 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 towards 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 regards to the implementation process – as stressed by Stewart (2018) – ISO/IEC 27001 is designed for 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 healthcare (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; 2012b), 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 information technology 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).

3.4.6. 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 7, 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 7: 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)

3.5. 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: (i) a structured approach to information and cybersecurity requires the integration of multiple standards; (ii) the motivations to pursue the ISO/IEC 27001 certification are also related to governmental incentives and market demands; (iii) implementation entails several challenges due to guidelines that are generic by design, different approaches/internalization levels are possible; (iv) there is limited evidence demonstrating the outcomes of the certification; (v) 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.*, 2019). Supply chains are becoming increasingly digitalized augmenting the risk of losing intellectual property (Kache and Seuring, 2015; Ardito *et al.*, 2019; Büyüközkan and Göçer, 2019). 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 regards 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.

3.5.1. 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

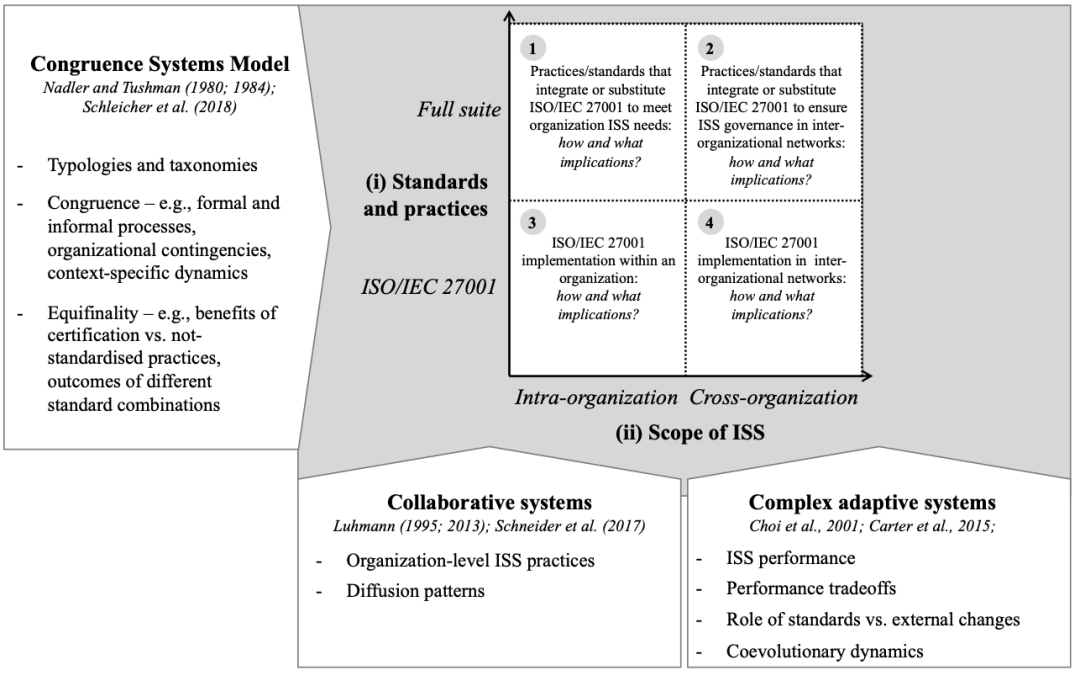
emerging challenges and the current knowledge gaps through theoretical lenses. Several theories have been used over the years in the study of voluntary standards and can be successfully applied in future research on ISO/IEC 27001. The most prominent ones – following the review of Tuczek *et al*. (2018) – include:

- 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 analyse voluntary standards adoption patters and performance implications related to lower information asymmetries (e.g., Prajogo *et al.,* 2012);
- 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);
- 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);
- 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);
- 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 (i) address its role within the suite of ISS practices and standards and (ii) take into consideration that the scope of ISS reaches beyond organizational boundaries. Figure 5 clarifies how these two perspectives can be investigated, including a possible theoretical underpinning and a summary of the main research opportunities which are outlined in the

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

Figure 5: Research agenda



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:

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

(ii) 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 analysing 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 System 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:

- Collaborative Systems – as outlined by Schneider *et al*. (2017) drawing from Luhmann (1995; 2013) – in order to elucidate how individual organizations shape their approach to ISS depending on the network of relations they are embedded in; and
- 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 are conceptualized as dynamic networks of autonomous agents (or firms) which 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 due to 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 uncharted territory. Social System 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.

CHAPTER 4. ISO/IEC 27001 DIFFUSION

4.1. Purpose

This chapter analyses the diffusion of ISO/IEC 27001. More in detail, we applied Grey Models (GM) – Even GM (1,1), Even GM (1,1,α,θ), Discrete GM (1,1), Discrete GM (1,1, α) – complemented by the relative growth rate and the doubling time indexes on the six most important countries in terms of issued certificates.

4.2. Literature background

Our study builds on three main research streams: literature on ISO/IEC 27001, studies investigating the diffusion of international management standards, and methodological papers on Grey models.

4.2.1. ISO/IEC 27001

Given the pivotal role played by data in both today's economy and society, ISO/IEC 27001 has attracted the interest of several scholars. Chapter 3 provides a systematic literature review on ISO/IEC 27001 highlighting that research on the topic has moved around three main areas: *motivations*, *implementation process*, and *outcomes*.

As for the *motivations*, scholars have highlighted both institutionalist (i.e., firms embrace ISO/IEC 27001 to achieve a formal certification to qualify in the eyes of external stakeholders) and functionalist (i.e., firms resort to the standard to improve their activities/processes) drivers. In terms of institutionalist motivations, extant research (e.g., Stewart, 2018) reports that ISO/IEC 27001 is adopted to improve the corporate image and attract more customers. Other studies argue that ISO/IEC 27001 is also implemented due to isomorphic phenomena or as a

response to specific client requests (e.g., Raabi *et al*., 2020). In this latter case, however, scholars (e.g., Cowan, 2011) have also warned that firms may decide to adhere only to some requirements of the standard (i.e., those explicitly requested by their customers) without achieving formal certification. Moving to the functionalist aspects, the main drivers are related to expectations around improved information security capabilities and skills, and increased efficiency of information security-related processes (e.g., Annarelli *et al*., 2020).

For what concerns the *implementation process*, several studies stress that ISO/IEC 27001 adoption requires a significant amount of resources. In particular, companies need to invest considerable time of their staff in activities and meetings related to the set-up/configuration of the information management system (e.g., Pardo *et al*., 2016), as well as relevant costs are reported in case organizations decide to resort to the help of external consultants (e.g., Rezaei *et al*., 2014). When it comes to the specific controls that firms should implement, extant research has also highlighted that the norm provides only limited advice on their mutual interdependence and a lack of guidance on cost/benefit assessments in their selection (e.g., Ho *et al*., 2015). Similarly, relevant difficulties have been highlighted as regards potential relationships between the organization and the external environment; many implementations fail because of an unstructured approach to shared assets and difficult identification of the organizations' dependencies on outsourced services (e.g., Stewart, 2018).

Moving to the *outcomes* of ISO/IEC 27001 adoption, the literature highlights lower IS risk levels (e.g., Al-Karaki *et al*., 2022) and improved business continuity (e.g., Rezaei *et al*., 2014) with consequent reduction of expenditures stemming from legal costs and bad news (e.g., due data leaks - Bakar *et al*., 2015). Scholars have also argued that the structured approach to information-related activities/processes demanded by ISO/IEC 27001 could result in clearer roles and accountabilities and fewer redundancies (e.g., Annarelli *et al*., 2020). Moreover, ISO/IEC 27001 can be considered a 'ticket to the market' for exporting firms – in particular, when they conduct their activities in contexts characterized by high diffusion degrees (e.g., Dionysiou, 2011) – and vendors located in offshored countries – e.g., India, Taiwan, Singapore – as it allows companies to show their international customers the care paid in ensuring data protection (e.g., Hlača *et al*., 2008). Despite these positive implications, the formalization required by some of the ISO/IEC 27001 dictates has also been connected to flexibility losses with negative implications for both labour productivity and the ability to fulfil customers' requests (Crowder, 2013; van Wessel *et al*., 2011). As a result, concerns related to potential

side effects on firms' profitability have been raised too (Tejay and Shoraka, 2011). Furthermore, some studies (e.g., Culot *et al*., 2019) have questioned the potential differentiating role of the standard, arguing that it only provides limited reputational benefits.

To conclude, it is worth acknowledging the specific context in which the empirical studies on ISO/IEC 27001 have been conducted[4]. Most of the authors (4 contributions) investigate issues related to US companies (Tarn *et al*., 2009; Tejay and Shoraka, 2011; Deane *et al*., 2019; Podrecca *et al*., 2022b). German organizations have been considered in three papers (Beckers *et al*., 2013; Mirtsch *et al*., 2020, 2021). Spain (Pardo *et al*., 2013; Mesquida *et al*., 2014), Iran (Rezaei *et al.*, 2014; Khajouei *et al.,* 2017), Taiwan (Ku *et al.*, 2009; Liao and Chueh, 2012a), and Turkey (Başaran, 2016; Ozkan and Karabacak, 2010) follow with two contributions each. Surprisingly, except for the German case, the focus of the studies is not consistent with the diffusion of the standard; many of the countries with the highest number of issued ISO/IEC 27001 certificates (ISO, 2021) have never been considered (e.g., Japan, India) or have been included only in studies resorting to a multi-country perspective (e.g., UK, China, Netherlands – van Wessel *et al*., 2011; UK, Italy – Annarelli *et al*., 2020).

Against this background characterized by the emergence of some controversial aspects that may hinder ISO/IEC 27001 adoption (e.g., avoidance of formal certification by firms, implementation failures due to lack of guidance on control selection and shared assets, lack of clarity around the outcomes of the adoption) and of discrepancies between the countries investigated in empirical studies and those recording the highest number of issued ISO/IEC 27001 certificates, a prominent need exists to investigate ISO/IEC 27001 future trajectories and to compare them with those of more mature and widespread management standards (i.e., ISO 9001, ISO 14001). As we will see in the next section, the diffusion patterns of these standards have been widely investigated, while a specific study on ISO/IEC 27001 is still missing.

4.2.2. Diffusion studies

First studies analysing the (long-term) dissemination patterns of international standards appeared in the early 2000s when Franceschini *et al*. (2004) noticed that their adoption follows an S-shaped (or sigmoid curve) divided into three different phases: an initial exponential growth (expansion) due to the firms' desire to give formal evidence of their commitment towards a

[4] Data are based on the literature review of Culot *et al*. (2021) complemented with the most recent papers on the topic (see Table A1 in the Appendix 1 for the full list of contributions).

specific topic (e.g. quality assurance, sustainability, social responsibility), a subsequent phase (maturation) characterised by a linear growth, and a last phase (retrocession) in which the interest reaches the peak and becomes stable gradually moving towards saturation.

The abovementioned patterns are close to those of population growth in environments with scarce resources (Pearl, 1978) and innovation adoption (Gurbaxani, 1990), i.e., two topics extensively studied by applying diffusion models like Verhulst (logistic) and Gompertz curves.

Franceschini *et al*. (2004) used these models to study diffusive patterns of some international management standards. Firstly, they resorted to Verhulst's equation to shed light on ISO 9001 dissemination across Europe. Subsequently, other scholars showed that the estimates of diffusive models can describe adoption trends of other standards (e.g., ISO 14001, SA8000, Global Reporting Initiative - GRI, United Nations Global Compact) both considering them at country and industry level (i.e., shedding light on the dissemination of international standards in specific countries and industries) (see Table 8).

A slightly different technique has, instead, been adopted by most recent contributions (Ikram *et al*., 2019; 2021). In particular, scholars have started to investigate the future dissemination of international standards using more sophisticated approaches, namely Grey models. When compared with Verhulst and Gompertz curves, the Grey method can provide several benefits such as high accuracy of the forecasts (e.g., several contributions based on logistic approaches underestimated the number of issued certificates) against a reduced computational effort (Liu *et al*., 2017; Javed and Liu, 2018). The next section provides a review of extant research on Grey models highlighting both their origin as well as further developments of this forecasting approach.

Table 8: Diffusion studies

Standard	Authors	Adopted approach	Level of analysis
ISO 9001	Franceschini *et al*., 2004	Logistic	Country
ISO 9001	Franceschini *et al*., 2006	Logistic	Country and economic sector
ISO 9001	Llach *et al*., 2011	Logistic	Economic sector
ISO 9001	Ikram *et al*., 2020	Grey	Country
ISO 9001 and ISO 14001	Marimon *et al*., 2006	Logistic	Country and economic sector
ISO 9001 and ISO 14001	Casadesús *et al*., 2008	Logistic	Country
ISO 9001 and ISO 14001	Marimon *et al*., 2009	Logistic	Country
ISO 9001 and ISO 14001	Marimon *et al*., 2010	Logistic	Country
ISO 9001 and industry-specific 'Q' standard	del Mar Alonso-Almeida *et al*., 2013	Logistic	Economic sector
ISO 14001	Marimon *et al*., 2011	Logistic	Economic sector
ISO 14001	Ikram *et al*., 2019	Grey	Country
ISO 20000	Cots and Casadesús, 2015	Logistic	Country
ISO 22000	Granja *et al*., 2021	Gompertz	Country
ISO/TS 16949	Franceschini *et al*., 2011	Logistic	Country
GRI	Marimon *et al*., 2012	Logistic	Country and economic sector

GRI	del Mar Alonso-Almeida *et al*., 2014	Logistic	Country and economic sector
GRI	del Mar Alonso-Almeida *et al*., 2015	Logistic	Universities
SA8000	Llach *et al*., 2015	Logistic	Country and economic sector
United Nations Global Compact	Podrecca *et al*., 2022a	Logistic	Country and economic sector
Integrated management systems (ISO 9001, ISO 14001, and OHSAS 18001)	Cabecinhas *et al*., 2018	Logistic + Gompertz	Country
Integrated management systems (ISO 9001, ISO 14001, and OHSAS 18001)	Cabecinhas *et al*., 2020	Logistic + Gompertz	Country

4.2.3. Grey models

First introduced in the ’80s by the Chinese scholar Julong Deng, Grey models are a data-driven intelligent time-series forecasting technique that is particularly useful in the study of samples characterized by reduced size, poor information, and uncertainty (Liu *et al*., 2016) (i.e., three limitations that usually affect studies dealing with the dissemination of management system standards - Ikram *et al*., 2019, 2021). The main characteristic of this forecasting approach is the capability of «extracting useful information from what is available» (Liu *et al*., 2015, p. 141); this way the law describing the system can be effectively explained and quantitative predictions can be done.

Starting from the original first order and one variable Grey Model (1,1) – GM (1,1), over the last 40 years the research on the grey forecasting technique has been particularly active due to both practical needs and its applicability to a wide range of situations. This has led to the development of four basic forms of GM (1,1), namely Even Grey Model (1,1) – EGM (1,1), Original Difference Grey Model (1,1) – ODGM (1,1), Even Difference Grey Model (1,1) – EDGM (1,1) and Discrete Grey Model (1,1) – DGM (1,1). Without entering into the specific peculiarities of each of them, we can refer to the classification of Liu *et al*. (2015) which argues that ODGM, EDGM, and DGM are more useful in the case of homogeneous exponential sequences of data, while EGM describes well non-exponential increasing and vibration (i.e., data moving around a reference value) sequences of data. Building on these basic forms, many contributions have focused on the characteristics of the models (e.g., Ji *et al*., 2001); on optimizing the parameters of the models (e.g., Jie and Bo, 2012); on strategies aimed at improving the initial values included in the models (e.g., Dang *et al*., 2005); and on identifying the application boundaries of the different models (e.g., Xie and Liu, 2006). As a result, the different (1,1) models have been used in a wide range of fields including agriculture (e.g., Li *et*

al., 2022), tourism (Dang *et al*., 2022), energy (Javed and Cudjoe, 2022), and management (Ikram *et al*., 2021).

Additional improvements in the discipline have led to the development of Grey (1,N) models. In (1,N) models the forecasted values depend not only on the sequence of original data of the dimension being estimated (e.g., the number of issued certificates), but scholars can also include some (independent) variables to investigate the sensitivity of the results to some contextual factors of interest (e.g., they can introduce the GDP growth to take into account the effect of the general economic situation) (Liu *et al*., 2017). Despite the accuracy improvements achievable thanks to (1,N) models, two main drawbacks hinder their large-scale applicability for prediction purposes (Ofosu-Adarkwa *et al*., 2020). First, these models can be used for predicting future values only when the original data vary slightly. Second, their estimates are based on the original data sequence of relevant factors (i.e., suppose we want to estimate ISO/IEC 27001 diffusion up to 2030, we would need the values of independent variables up to 2030, which is not feasible). For such reasons, scholars resorting to Grey models to estimate the future trends of international management standards have always adopted (1,1) models (Ikram *et al*., 2019, 2021).

4.3. Methodology

4.3.1. Dataset and modelling approach

The dataset used to investigate ISO/IEC 27001 diffusion comes from the list of ISO/IEC 27001 issued certifications available on the ISO website (ISO, 2021). Analysed data refer to the period from 2010 to 2020 and, consistently with extant research (e.g., Ikram *et al*., 2019, 2021), consider the six countries with the highest number of certified organizations (i.e., Japan, China, UK, India, Germany, Italy).

As previously argued, when compared with traditional Verhulst and Gompertz equations, Grey models provide several benefits including the higher reliability of the forecasts and the possibility to present the results in a simple mathematical form (Liu *et al*., 2017). Hence, we resorted to (1,1) Grey models to investigate the diffusion patterns of ISO/IEC 27001. Based on the classification of Liu *et al*. (2015) described in the previous section and considering the characteristics of the data, we decided to use both a model suitable for exponential sequences and a model useful for non-exponential increasing sequences. While EGM (1,1) was the only available model for non-exponential increasing sequences (Liu *et al*., 2015), in terms of

exponential sequences we preferred DGM (1,1) rather than OGM (1,1) or EDGM (1,1). This is because over the last years many scholars have proposed variations to the DGM (1,1) estimation algorithm aimed at improving its forecasting performance. As such, in line with the most recent contributions (e.g., Javed *et al*., 2020; Javed and Cudjoe, 2022), the Even Grey model - EGM (1,1), the discrete Grey model - DGM (1,1), and their generalized versions – EGM (1,1,α,θ), DGM (1,1,α) – were selected.

4.3.2. Grey models

4.3.2.1. DGM (1,1) and EGM (1,1)

Let's consider a sequence of raw data

$$X^{(0)} = \left(x^{(0)}(1), x^{(0)}(2), \dots, x^{(0)}(n)\right), x^{(0)}(k) \geq 0 \qquad (1)$$

its direct use is not appropriate in grey models as raw data are usually characterized by significant noise, and this decreases the forecast accuracy (Liu *et al*., 2017). To solve such issue, Deng (2004) introduced the concept of "accumulation of raw data". In the classical DGM (1,1) and EGM (1,1) the data accumulation is usually performed with the "once accumulating generation operator" usually called 1-AGO (i.e., a cumulative sum operator) (Liu *et al*., 2017). Therefore, the 1-AGO of the sequence of raw data (1) would result in

$$X^{(1)} = \left(x^{(1)}(1), x^{(1)}(2), \dots, x^{(1)}(n)\right) \qquad (2)$$

in which $x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i), k = 1,2, \dots, n.$

The 1-AGO sequence of data is then introduced in the DGM (1,1) and EGM (1,1) to forecast the desired values.

4.3.2.2. DGM (1,1)

The DGM (1,1) – the discrete form of a first-order single variable Grey model – time-response function of $X^{(0)}$ (i.e., the formula that provides the forecasts) is (Zhao *et al*., 2018)

$$\hat{x}^{(0)}(k) = (\beta_1 - 1)\left(x^{(0)}(1) - \frac{\beta_2}{1-\beta_1}\right)\beta_1^{k-2}, k = 2,3, \dots, n \qquad (3)$$

in which $\hat{x}^{(0)}(1) = x^{(1)}(1) = x^{(0)}(1)$

To estimate the parameters β1 and β2, an OLS approach can be adopted (Zhao *et al*., 2018), namely

$$[\beta_1, \beta_2]^T = [\mathrm{B}^T\mathrm{B}]^{-1}\mathrm{B}^T Y \qquad (4)$$

with

$$\mathrm{B} = \begin{bmatrix} x^{(1)}(1) & 1 \\ x^{(1)}(2) & 1 \\ \vdots & \vdots \\ x^{(1)}(n-1) & 1 \end{bmatrix} \text{ and } \mathrm{Y} = \begin{bmatrix} x^{(1)}(2) \\ x^{(1)}(3) \\ \vdots \\ x^{(1)}(n) \end{bmatrix}$$

The Appendix 2 provides a step-by step application of DGM (1,1) to a real case (i.e., the number of ISO/IEC 27001 issued certificates in Japan). For a more detailed discussion on DGM (1,1) the interested reader might refer, among others, to Zhao *et al*. (2018).

4.3.2.3. EGM (1,1)

The EGM (1,1) – the even form of a first-order single variable Grey model – time-response function of $X^{(0)}$ (i.e., the formula that provides the forecasts) is (Liu *et al*., 2017)

$$\hat{x}^{(0)}(k) = (1 - e^{a}) \left(x^{(0)}(1) - \frac{b}{a} \right) e^{-a(k-1)}, k = 1,2, \dots, n \qquad (5)$$

in which $\hat{x}^{(0)}(1) = x^{(1)}(1) = x^{(0)}(1)$

To estimate the parameters a and b, an Ordinary Least Square (OLS) approach can be adopted (Liu *et al*., 2017), namely

$$[\mathrm{a}, \mathrm{b}]^T = [\mathrm{B}^T \mathrm{B}]^{-1} \mathrm{B}^T Y \qquad (6)$$

with

$$\mathrm{B} = \begin{bmatrix} -z^{(1)}(2) & 1 \\ -z^{(1)}(3) & 1 \\ \vdots & \vdots \\ -z^{(1)}(n) & 1 \end{bmatrix} \text{and } \mathrm{Y} = \begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix}, \text{ where } z^{(1)}(k) = \frac{1}{2}(x^{(1)}(k) + x^{(1)}(k-1)).$$

The Appendix 2 provides a step-by step application of EGM (1,1) to a real case (i.e., the number of ISO/IEC 27001 issued certificates in Japan). For a more detailed discussion on EGM (1,1) the interested reader might refer, among others, to Liu *et al*. (2017).

4.3.2.4. EGM (1,1,α,θ) and DGM (1,1,α)

Despite the concept of 1-AGO is widely adopted, it presents some limitations that might worsen the prediction performance of GM (1,1) models. In particular, the models resulting from Deng (2004) definition of 1-AGO are linear models and thus they are oversimplified for many real applications in which diffusion patterns may accelerate or reduce over time. This issue prompted researchers to propose alternative operators for data accumulation. One of the most successful attempts was made by Ma *et al*. (2020) that proposed the conformable fractional

accumulation of raw data and the inverse conformable accumulation of simulated data. The fractional-order accumulation allows considering nonlinearity in data (i.e., it accounts for any potential increase or decrease in the diffusion rate of the phenomenon being investigated) and thus improves the reliability of the model and its adherence to reality (Javed and Cudjoe, 2022).

Let's consider the same sequence of raw data as in (1)

$$X^{(0)} = \left(x^{(0)}(1), x^{(0)}(2), \dots, x^{(0)}(n)\right), x^{(0)}(k) \geq 0 \qquad (7)$$

its conformable fractional accumulated series of data (Javed *et al*., 2020; Javed and Cudjoe, 2022) is defined as

$$X^{(\alpha)} = \left(x^{(\alpha)}(1), x^{(\alpha)}(2), \dots, x^{(\alpha)}(n)\right) \qquad (8)$$

in which $x^{(\alpha)}(k) = \sum_{i=1}^{k} \left(\frac{x^{(0)}(i)}{i^{1-\alpha}}\right), k = 1,2, \dots, n.$ $\alpha \in (0,1]$.

The conformable fraction accumulated sequence of data is then introduced in the DGM (1,1,α) and EGM (1,1,α,θ) to forecast the desired values.

4.3.2.5. DGM (1,1,α)

The DGM (1,1,α) – the discrete form of a grey forecasting model with a first-order differential equation containing one variable and conformable fractional accumulation – time-response function of $X^{(0)}$ (i.e., the formula that provides the forecasts) is (Javed and Cudjoe, 2022)

$$\hat{x}^{(0)}(k) = (k-1)^{1-\alpha}(\beta_1 - 1)\left(x^{(0)}(1) - \frac{\beta_2}{1-\beta_1}\right)\beta_1^{k-2}, k = 2,3, \dots, n \qquad (9)$$

in which $\hat{x}^{(0)}(1) = x^{(\alpha)}(1) = x^{(0)}(1)$

To estimate the parameters β1 and β2, an OLS approach can be adopted (Javed and Cudjoe, 2022), namely

$$[\beta_1, \beta_2]^T = [\mathrm{B}^T\mathrm{B}]^{-1}\mathrm{B}^T Y \qquad (10)$$

with

$$\mathrm{B} = \begin{bmatrix} x^{(\alpha)}(1) & 1 \\ x^{(\alpha)}(2) & 1 \\ \vdots & \vdots \\ x^{(\alpha)}(n-1) & 1 \end{bmatrix} \text{ and } \mathrm{Y} = \begin{bmatrix} x^{(\alpha)}(2) \\ x^{(\alpha)}(3) \\ \vdots \\ x^{(\alpha)}(n) \end{bmatrix}$$

while α can be identified by minimizing the forecasting error. In particular, according to Javed and Cudjoe (2022), this can be done by solving the following optimization problem

$$\min \left(\frac{1}{n}\sum_{k=1}^{n}\left|\frac{x^{(0)}(k) - \hat{x}^{(0)}(k)}{x^{(0)}(k)}\right| \times 100\right) \qquad (11)$$

where $x^{(0)}(k)$ is defined as in (1) and (7), while $\hat{x}^{(0)}(k)$ as in (9), and α ∈ (0,1] (Javed and Cudjoe, 2022). For a more detailed discussion on DGM (1,1,α) the interested reader might refer, among others, to Javed and Cudjoe (2022).

4.3.2.6. EGM (1,1,α,θ)

The EGM (1,1,α,θ) – the even form of a grey model with a first-order differential equation containing one variable, and weighted background value containing conformable fractional accumulation – time-response function of $X^{(0)}$ (i.e., the formula that provides the forecasts) is (Javed *et al*., 2022)

$$\hat{x}^{(0)}(k) = k^{1-\alpha}(1-e^{a})\left(x^{(0)}(1) - \frac{b}{a}\right)e^{-a(k-1)}, k = 1,2,\dots,n \qquad (12)$$

in which $\hat{x}^{(0)}(1) = x^{(a)}(1) = x^{(0)}(1)$

To estimate the parameters a and b, an Ordinary Least Square (OLS) approach can be adopted (Javed *et al*., 2020), namely

$$[\mathrm{a}, \mathrm{b}]^{T} = [\mathrm{B}^{T}\mathrm{B}]^{-1}\mathrm{B}^{T}Y \qquad (13)$$

with

$$\mathrm{B} = \begin{bmatrix} -z^{(1)}(2) & 1 \\ -z^{(1)}(3) & 1 \\ \vdots & \vdots \\ -z^{(1)}(n) & 1 \end{bmatrix} \text{and } \mathrm{Y} = \begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix}, \text{where } z^{(1)}(k) = \theta x^{(\alpha)}(k) + (1-\theta)x^{(\alpha)}(k-1).$$

θ ∈ (0,1].

α and θ can be identified by minimizing the forecasting error. In particular, according to Javed *et al*. (2020), this can be done by solving the following optimization problem

$$\min\left(\frac{1}{n}\sum_{k=1}^{n}\left|\frac{x^{(0)}(k)-\hat{x}^{(0)}(k)}{x^{(0)}(k)}\right| \times 100\right) \qquad (14)$$

where $x^{(0)}(k)$ is defined as in (1) and (7), while $\hat{x}^{(0)}(k)$ as in (12), α ∈ (0,1], and θ ∈ (0,1] (Javed *et al*., 2020). For a more detailed discussion on EGM (1,1,α,θ) the interested reader might refer, among others, to Javed *et al*. (2020).

4.3.3. Forecasting performance evaluation

To evaluate the forecasting performance of the four models we resorted to the Mean Absolute Percentage Error (MAPE) defined as follows:

$$MAPE(\%) = \frac{1}{n}\sum_{k=1}^{n}\left|\frac{x(k)-\hat{x}(k)}{x(k)}\right| \times 100 \qquad (15)$$

where $x(k)$ and $\hat{x}(k)$ represent, respectively, the actual observation and the predicted (forecasted) value.

MAPE is one of the most widely adopted measures of goodness-of-fit and has been already used in different contexts (see for example Ikram *et al*., 2021, 2019; Javed *et al*., 2020). According to the Lewis scale (Lewis, 1982), MAPE values can be considered as follows (Table 9).

Table 9: Lewis scale for MAPE evaluation

MAPE (%)	**Forecast accuracy**
Lower than 10%	Highly accurate forecast
Between 10% and 20%	Good forecast
Between 20% and 50%	Reasonable forecast
Higher than 50%	Inaccurate forecast

4.3.4. Growth analysis and doubling time

To complement our analyses, two additional indicators were used: the Relative Growth Rate (RGR) and the Doubling time (Dt). The first was employed to shed light on the country-wise relative growth of ISO/IEC 27001 certificates; the second to understand the time needed to double the number of ISO/IEC 27001 certificates. Previous adoption of these indexes can be found, among others, in Javed and Liu (2018).

RGR is defined as (Javed and Liu, 2018):

$$RGR = \frac{(ln\ N_2 - ln\ N_1)}{(t_2 - t_1)} \quad (16)$$

where N_2 and N_1 are the cumulative numbers of ISO/IEC 27001 certifications in years t_2 and t_1. By considering (t_2-t_1) equal to 1 year, the above equation can be written as (Javed and Liu, 2018):

$$RGR = (ln\ N_2 - ln\ N_1) \quad (17)$$

Moving to the Doubling time (Dt), the underlying equation is given as (Javed and Liu, 2018):

$$Dt = (t2 - t1)\ln\left(\frac{2}{\ln N_2 - \ln N_1}\right) \quad (18)$$

Similarly to the RGR, (t_2-t_1) is equal to one year. Therefore, Dt equation becomes (Javed and Liu, 2018):

$$Dt = \ln\left(\frac{2}{\ln N_2 - \ln N_1}\right) \quad (19)$$

4.4. Results and discussion

This chapter is structured into two sections. The first evaluates the effectiveness of the models in describing current and future trends of ISO/IEC 27001 adoption. The second presents and discusses the findings.

4.4.1. Performance evaluation of the models

Table 10 – 15 report the findings for the six countries under investigation: Japan, China, UK, India, Germany, Italy. For each of them, we first simulated data from 2010 to 2020 and then we predicted the number of issued certificates from 2021 to 2030.

As stated in section 4.3.3., the goodness of fit of the Grey models is evaluated in terms of their MAPE. Results show that EGM (1,1,α,θ) always outperforms (i.e., its MAPE shows lower values) DGM (1,1,α), EGM (1,1), and DGM (1,1) exhibiting highly accurate (UK, India) or good (Japan, China, Germany, Italy) estimates. Accordingly, in the following section, findings presentation and discussion will build on EGM (1,1,α,θ) predictions.

As a side note, it is particularly interesting to highlight that the accuracy improvement in moving from EGM (1,1), DGM (1,1,α), and DGM (1,1) to EGM (1,1,α,θ) is far more relevant in countries with higher growth rates. For instance, in China the accuracy improves by almost 40% with a MAPE that goes from 27.02% (DGM (1,1)) to 15.30% (EGM (1,1,α,θ)).

Table 10: ISO/IEC 27001 growth for Japan

Year	Actual data	EGM (1,1,α,θ)	EGM (1,1)	DGM (1,1,α)	DGM (1,1)	Cumulative data	RGR	RGR mean	Dt	Dt mean
2010	6237	6237	6237	6237	6237	6237				
2011	6914	4859	5000	5060	5060	13151	0.746	0.285	0.986	2.072
2012	7199	5545	5721	5784	5784	20350	0.437		1.522	
2013	7140	6328	6546	6611	6611	27490	0.301		1.895	
2014	7171	7221	7490	7557	7557	34661	0.232		2.155	
2015	8240	8240	8571	8638	8638	42901	0.213		2.238	
2016	8945	9403	9807	9873	9873	51846	0.189		2.357	
2017	9161	10730	11222	11285	11285	61007	0.163		2.509	
2018	12145	12245	12841	12899	12899	73152	0.182		2.399	
2019	16848	13973	14693	14744	14744	90000	0.207		2.267	
2020	18103	15945	16813	16853	16853	108103	0.183		2.390	
2021		18195	19238	19263	19263	18195				
2022		20763	22014	22018	22018	38958	0.761	0.330	0.966	1.912
2023		23694	25189	25167	25167	62652	0.475		1.437	
2024		27038	28823	28766	28766	89690	0.359		1.718	
2025		30854	32980	32880	32880	120544	0.296		1.912	
2026		35208	37738	37583	37583	155752	0.256		2.055	
2027		40178	43182	42958	42958	195930	0.229		2.165	

2028		45848	49411	49101	49101	241778	0.210		2.253	
2029		52319	56539	56123	56123	294097	0.196		2.323	
2030		59704	64695	64150	64150	353801	0.185		2.381	
a; β1		-0.13203	-0.13475	1.14302	1.14302					
b; β2		3722.141	3829.922	4168.496	4168.496					
α		1		1						
θ		0.67579								
MAPE (%)		11.68%	12.28%	12.32%	12.32%					

Table 11: ISO/IEC 27001 growth for China

Year	Actual data	EGM (1,1,α,θ)	EGM (1,1)	DGM (1,1,α)	DGM (1,1)	Cumulative data	RGR	RGR mean	Dt	Dt mean
2010	509	509	509	509	509	509				
2011	664	459	604	371	635	1173	0.835	0.441	0.874	1.556
2012	790	668	857	624	902	1963	0.515		1.357	
2013	965	965	1216	965	1282	2928	0.400		1.610	
2014	1210	1389	1725	1441	1821	4138	0.346		1.755	
2015	1469	1994	2447	2111	2588	5607	0.304		1.885	
2016	2618	2858	3471	3056	3676	8225	0.383		1.652	
2017	5069	4091	4923	4387	5224	13294	0.480		1.427	
2018	7612	5849	6983	6261	7422	20906	0.453		1.486	
2019	8357	8357	9905	8892	10545	29263	0.336		1.783	
2020	12489	11933	14050	12583	14983	41752	0.355		1.728	
2021		17029	19930	17754	21289	17029				
2022		24292	28270	24989	30247	41321	0.886	0.485	0.814	1.459
2023		34640	40100	35100	42977	75961	0.609		1.189	
2024		49380	56880	49216	61063	125341	0.501		1.385	
2025		70372	80682	68904	86760	195713	0.446		1.501	
2026		100263	114444	96342	123272	295976	0.414		1.576	
2027		142819	162335	134551	175149	438795	0.394		1.625	
2028		203399	230266	187720	248857	642194	0.381		1.658	
2029		289624	326624	261663	353585	931818	0.372		1.681	
2030		412338	463303	364432	502386	1344156	0.366		1.697	
a; β1		-0.35019	-0.34957	1.37186	1.42083					
b; β2		188.415	326.972	181.652	420.702					
α		0.93717		0.70528						
θ		0.92309								
MAPE (%)		15.30%	22.74%	18.30%	27.02%					

Table 12: ISO/IEC 27001 growth for UK

Year	Actual data	EGM (1,1,α,θ)	EGM (1,1)	DGM (1,1,α)	DGM (1,1)	Cumulative data	RGR	RGR mean	Dt	Dt mean
2010	1157	1157	1157	1157	1157	1157				
2011	1464	1443	1552	1380	1560	2621	0.818	0.341	0.894	1.874
2012	1701	1708	1811	1701	1820	4322	0.500		1.386	
2013	1923	2013	2114	2038	2124	6245	0.368		1.693	
2014	2253	2368	2467	2414	2479	8498	0.308		1.871	
2015	2790	2781	2879	2841	2893	11288	0.284		1.952	
2016	3367	3263	3361	3330	3377	14655	0.261		2.036	

2017	4503	3826	3922	3892	3941	19158	0.268		2.010	
2018	4723	4483	4578	4539	4599	23881	0.220		2.206	
2019	5251	5251	5343	5286	5368	29132	0.199		2.309	
2020	5897	6148	6236	6148	6265	35029	0.184		2.384	
2021		7197	7278	7144	7312	7197				
2022		8423	8494	8295	8533	15620	0.775	0.345	0.948	1.855
2023		9855	9914	9623	9959	25475	0.489		1.408	
2024		11528	11571	11159	11623	37003	0.373		1.679	
2025		13484	13505	12932	13565	50487	0.311		1.862	
2026		15769	15762	14981	15832	66256	0.272		1.996	
2027		18439	18396	17347	18477	84695	0.246		2.097	
2028		21559	21471	20081	21564	106254	0.227		2.177	
2029		25205	25059	23238	25167	131459	0.213		2.240	
2030		29465	29247	26884	29372	160924	0.202		2.291	
a; β1		-0.15443	-0.15455	1.15102	1.16709					
b; β2		1123.561	1256.080	1204.810	1366.185					
α		0.96497		0.90072						
θ		1								
MAPE (%)		3.94%	5.87%	4.43%	6.16%					

Table 13: ISO/IEC 27001 growth for India

Year	Actual data	EGM (1,1,α,θ)	EGM (1,1)	DGM (1,1,α)	DGM (1,1)	Cumulative data	RGR	RGR mean	Dt	Dt mean
2010	1281	1281	1281	1281	1281	1281				
2011	1427	1356	1372	1380	1380	2708	0.749	0.323	0.983	1.920
2012	1611	1585	1607	1616	1616	4319	0.467		1.455	
2013	1931	1854	1882	1892	1892	6250	0.370		1.689	
2014	2168	2168	2205	2216	2216	8418	0.298		1.905	
2015	2490	2535	2582	2596	2596	10908	0.259		2.044	
2016	2902	2965	3024	3040	3040	13810	0.236		2.138	
2017	3272	3467	3542	3561	3561	17082	0.213		2.241	
2018	4723	4054	4149	4171	4171	21805	0.244		2.103	
2019	5052	4741	4860	4885	4885	26857	0.208		2.262	
2020	5449	5544	5692	5721	5721	32306	0.185		2.382	
2021		6483	6667	6701	6701	6483				
2022		7581	7809	7848	7848	14064	0.774	0.345	0.949	1.856
2023		8865	9147	9192	9192	22929	0.489		1.409	
2024		10367	10713	10766	10766	33296	0.373		1.679	
2025		12123	12548	12609	12609	45419	0.310		1.863	
2026		14176	14698	14768	14768	59595	0.272		1.996	
2027		16577	17215	17297	17297	76172	0.245		2.098	
2028		19385	20164	20258	20258	95557	0.227		2.177	
2029		22669	23618	23727	23727	118226	0.213		2.240	
2030		26509	27663	27790	27790	144735	0.202		2.291	
a; β1		-0.15648	-0.15810	1.17122	1.17122					
b; β2		1052.006	1063.804	1160.167	1160.167					
α		1		1						
θ		0.56732								
MAPE (%)		4.26%	4.49%	4.57%	4.57%					

Table 14: ISO/IEC 27001 growth for Germany

Year	Actual data	EGM (1,1,α,θ)	EGM (1,1)	DGM (1,1,α)	DGM (1,1)	Cumulative data	RGR	RGR mean	Dt	Dt mean
2010	357	357	357	357	357	357				
2011	424	345	330	338	338	781	0.783	0.364	0.938	1.771
2012	488	444	421	430	430	1269	0.485		1.416	
2013	581	571	536	548	548	1850	0.377		1.669	
2014	634	734	683	699	699	2484	0.295		1.915	
2015	994	943	871	890	890	3478	0.337		1.782	
2016	1338	1212	1110	1135	1135	4816	0.325		1.816	
2017	1339	1558	1415	1446	1446	6155	0.245		2.098	
2018	2003	2003	1803	1843	1843	8158	0.282		1.960	
2019	2095	2575	2298	2349	2349	10253	0.229		2.169	
2020	3367	3309	2928	2993	2993	13620	0.284		1.952	
2021		4254	3732	3815	3815	4254				
2022		5468	4756	4861	4861	9722	0.827	0.409	0.884	1.653
2023		7029	6061	6196	6196	16751	0.544		1.302	
2024		9035	7724	7896	7896	25786	0.431		1.534	
2025		11613	9843	10062	10062	37399	0.372		1.683	
2026		14928	12544	12824	12824	52327	0.336		1.784	
2027		19188	15987	16342	16342	71515	0.312		1.857	
2028		24665	20374	20827	20827	96180	0.296		1.909	
2029		31704	25965	26542	26542	127884	0.285		1.949	
2030		40752	33090	33826	33826	168636	0.277		1.978	
a; β1		-0.25107	-0.24249	1.27441	1.27441					
b; β2		214.279	205.225	239.598	239.598					
α		1		1						
θ		0.35361								
MAPE (%)		10.05%	11.91%	11.29%	11.29%					

Table 15: ISO/IEC 27001 growth for Italy

Year	Actual data	EGM (1,1,α,θ)	EGM (1,1)	DGM (1,1,α)	DGM (1,1)	Cumulative data	RGR	RGR mean	Dt	Dt mean
2010	374	374	374	374	374	374				
2011	425	365	343	357	357	799	0.759	0.362	0.969	1.804
2012	495	465	433	450	450	1294	0.482		1.423	
2013	901	592	546	566	566	2195	0.528		1.331	
2014	969	753	688	713	713	3164	0.366		1.699	
2015	1013	959	867	898	898	4177	0.278		1.974	
2016	1220	1220	1094	1130	1130	5397	0.256		2.055	
2017	958	1553	1379	1422	1422	6355	0.163		2.505	
2018	1818	1976	1738	1791	1791	8173	0.252		2.073	
2019	2513	2515	2191	2254	2254	10686	0.268		2.010	
2020	3324	3201	2762	2837	2837	14010	0.271		1.999	
2021		4074	3482	3572	3572	4074				
2022		5186	4390	4496	4496	9260	0.821	0.402	0.890	1.673
2023		6600	5534	5660	5660	15860	0.538		1.313	
2024		8400	6977	7125	7125	24260	0.425		1.549	
2025		10692	8795	8969	8969	34952	0.365		1.701	
2026		13608	11088	11290	11290	48560	0.329		1.805	
2027		17319	13978	14212	14212	65879	0.305		1.881	

2028		22043	17622	17890	17890	87922	0.289		1.936	
2029		28055	22215	22520	22520	115977	0.277		1.977	
2030		35708	28006	28349	28349	151685	0.268		2.008	
a; β1		-0.24118	-0.23164	1.2588	1.25881					
b; β2		232.813	218.548	260.680	260.680					
α		1		1						
θ		0.31327								
MAPE (%)		15.67%	20.29%	18.22%	18.22%					

4.4.2. Presentation of the findings

As regards data up to 2020 (Table 10 – 15; see Figure 6 – 11 for a graphical representation of the results), Japan (18103 certifications) has recorded the highest number of ISO/IEC 27001 issued certificates followed by China (12489), UK (5897), India (5449), Germany (3367), and Italy (3324). Moving to the EGM (1,1,α,θ) predicted values (2021-2030), the estimates exhibit exponential growth (Figure 6 – 11) in the years to come with China (412338 certificates) that is likely to become the leading country in terms of ISO/IEC 27001 certifications, followed by Japan (59704), Germany (40752), Italy (35708), UK (29465), and India (26509). Based on these results, two interesting findings emerge. On the one hand, with 24292 certificates in 2022 China will overtake Japan (20763) at the top of the chart. On the other, UK is predicted to lose some positions in favour of Germany and Italy.

After shedding light on the (current and future) diffusion trends, we can notice that the countries characterized by the highest amount of ISO/IEC 27001 certificates are also leading as regards the adoption of more mature standards (i.e., ISO 9001, ISO 14001 – ISO, 2021; Ikram *et al*., 2021, 2019). These results can be explained considering the findings of Mirtsch *et al*. (2020), Cots and Casadesús (2015), and Dahlin and Isaksson (2017): firms usually start to implement general standards (i.e., ISO 9001) and then resort to more specific ones. Accordingly, in areas with an established tradition of certifications, many organizations have already validated the quality of their operational processes and therefore they are starting to approach other (more specific) standards like ISO/IEC 27001. In such contexts, ISO/IEC 27001 exhibits two main strengths. On the one hand, the learning process followed for ISO 9001 and ISO 14001 could help firms to adhere more quickly to ISO/IEC 27001 (Podrecca *et al*., 2022a); companies can therefore take advantage of the positive externalities of ISO/IEC 27001 (e.g., streamlined buyer-supplier relationships - Hannigan *et al*., 2019; differentiation effect - Stewart, 2018) without all the burdens faced by firms approaching ISO standards for the first

time. On the other hand, by implementing ISO/IEC 27001 together with other management standards (and by integrating them into a single management system) firms can benefit from the peculiarities of each of them while reducing costs, complexity, and time efforts required to manage common mandatory requirements like documentation, audits, and procedures (Hoy and Foley, 2015; Sampaio *et al*., 2012).

Based on the data up to 2020, the RGR estimates show the following sequence:

$$China_{(0.441)} > Germany_{(0.364)} > Italy_{(0.362)} > UK_{(0.341)} > India_{(0.323)} > Japan_{(0.285)}$$

while Dt results are as follows:

$$Japan_{(2.072)} > India_{(1.920)} > UK_{(1.874)} > Italy_{(1.804)} > Germany_{(1.771)} > China_{(1.556)}$$

The outcomes of these analyses highlight two main findings. First, up to 2020, China has recorded the highest RGR (0.441). Second, after an initial euphoria, the growth rate of Japan has slowed down and the country is currently characterized by the highest Dt (2.072). This evidence is consistent with the dictates of Mastrogiacomo *et al*. (2021): diffusion patterns are not 'synchronous' across different contexts. Some countries exhibit an immediate adoption followed by a reduction of interest (or at least a decrease in the diffusion rate), while in other regions the diffusion processes start more slowly and the sustained growth occurs only at a later stage. These dynamics are generally linked to some peculiar economic and socio-political conditions of each country (Ikram *et al*., 2019). Accordingly – in parallel with their expansion in worldwide markets – Chinese firms may have been asked to achieve ISO/IEC 27001 as a mandatory prerequisite to create some business partnerships (Dionysiou, 2011). On the contrary, the slowdown recorded in Japan might be linked to the issues faced by Japanese firms: both their market shares and their productivity exhibit stagnating trends (e.g., Akram, 2019).

Based on EGM (1,1,α,θ) data (2021-2030) the following sequence is obtained for the RGR:

$$China_{(0.485)} > Germany_{(0.409)} > Italy_{(0.402)} > UK_{(0.345)} > India_{(0.345)} > Japan_{(0.330)}$$

while the Dt is:

$$Japan_{(1.912)} > India_{(1.856)} > UK_{(1.855)} > Italy_{(1.673)} > Germany_{(1.653)} > China_{(1.459)}$$

EGM (1,1,α,θ) predicted data (2021-2030) present higher RGR (and therefore lower Dt) when compared with trends observed up to 2020. For instance, while up to 2020 the RGR of China was 0.441, in the period 2021-2030 the RGR is equal to 0.485. Similarly, Germany moved from 0.364 to 0.409, Italy from 0.362 to 0.402, UK from 0.341 to 0.345, India from 0.323 to 0.345, Japan from 0.285 to 0.330. These data show that, differently from other more mature standards (e.g., ISO 9001, ISO 14001) whose growing trends have recently plateaued

(ISO, 2021), ISO/IEC 27001 is expected to play a significant role in the years to come. This pattern seems to reflect the increasing central position of information technologies in all economic fields (Maganga and Taifa, 2022; Sony *et al*., 2022): nowadays value creation is all about data exchange across organizational boundaries (Rendon-Benavides *et al*., 2022; Wu *et al*., 2022). The relevance of both scope and scale of these interactions poses several new challenges to information system security (Li, 2021; Wong *et al*., 2019); supply chains are increasing their digitalization level, online solutions are connecting a relevant amount of customers and suppliers, cloud-based platforms are leading to massive outsourcing of computing capabilities and data storage. In this new landscape, holistic approaches – such as ISO/IEC 27001 – are a given for worldwide companies and organizations (Rauniyar *et al*., 2022; Vance *et al*., 2020). Moreover, as more and more firms are demanding the external validation of the IS-related processes of their business partners, ISO/IEC 27001 is becoming a common ground to overcome transaction barriers (Villarreal, 2019).

Summing up, while some scholars (e.g., Mirtsch *et al*., 2021) have raised potential concerns regarding ISO/IEC 27001 long-term dissemination, our study shows that such controversial issues will not overshadow the adoption of the standard. As long as information security will remain a hot business topic, ISO/IEC 27001 adoption will continue growing and giving certified organizations the required capabilities to ensure data availability, integrity, and confidentiality together with the chance to present formal evidence of their commitment.

At this point, it is worth acknowledging some factors that may alter the estimates in the years to come. Building on extant research (e.g., Sampaio *et al*., 2009; Corbett and Kirsch, 2001) two macroeconomic aspects appear particularly relevant: the economic development and the export propensity of the different countries. First, as for economic development, previous studies have posited that the greater the development of the country, the higher the number of companies, and the larger the number of issued certificates (e.g., Corbett and Kirsch, 2001). A potential economic slowdown in the years to come (e.g., due to the rising energy prices – We Forum, 2022), could reduce the number of companies interested in adopting ISO/IEC 27001 and thus cause the estimates of this study to be revised downward. Second, as for the export propensity of the companies' home country, firms usually implement international management standards as a response to the coercive pressures of some foreign commercial partners that require formal evidence of their commitment towards a specific topic (e.g., quality assurance, sustainability, social responsibility – Guler *et al*., 2002). Some recent events (e.g., Brexit, US-

China trade war, Russia-Ukraine war) might, however, decrease the economic openness and the export propensity of the countries (e.g., Goulard, 2020) potentially leading to a reduction in the number of issued certificates in the years to come. To conclude, in addition to the macroeconomic factors emerging from the literature, other relevant aspects such as the enactment of incentives aimed at fostering the adoption of ISO/IEC 27001 and modifications in the dictates underpinning this certification scheme might further modify the adoption patterns.

Figure 6: Graphical representation of Japan data

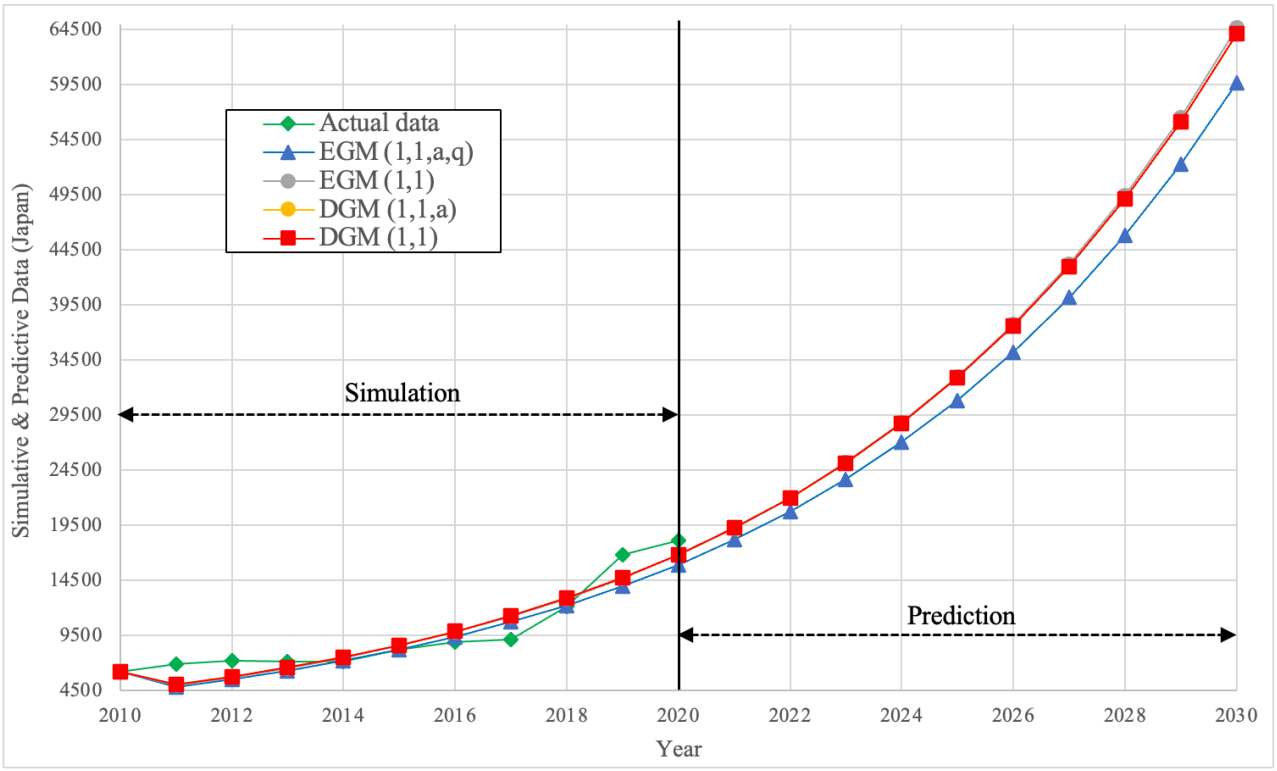


Figure 7: Graphical representation of China data

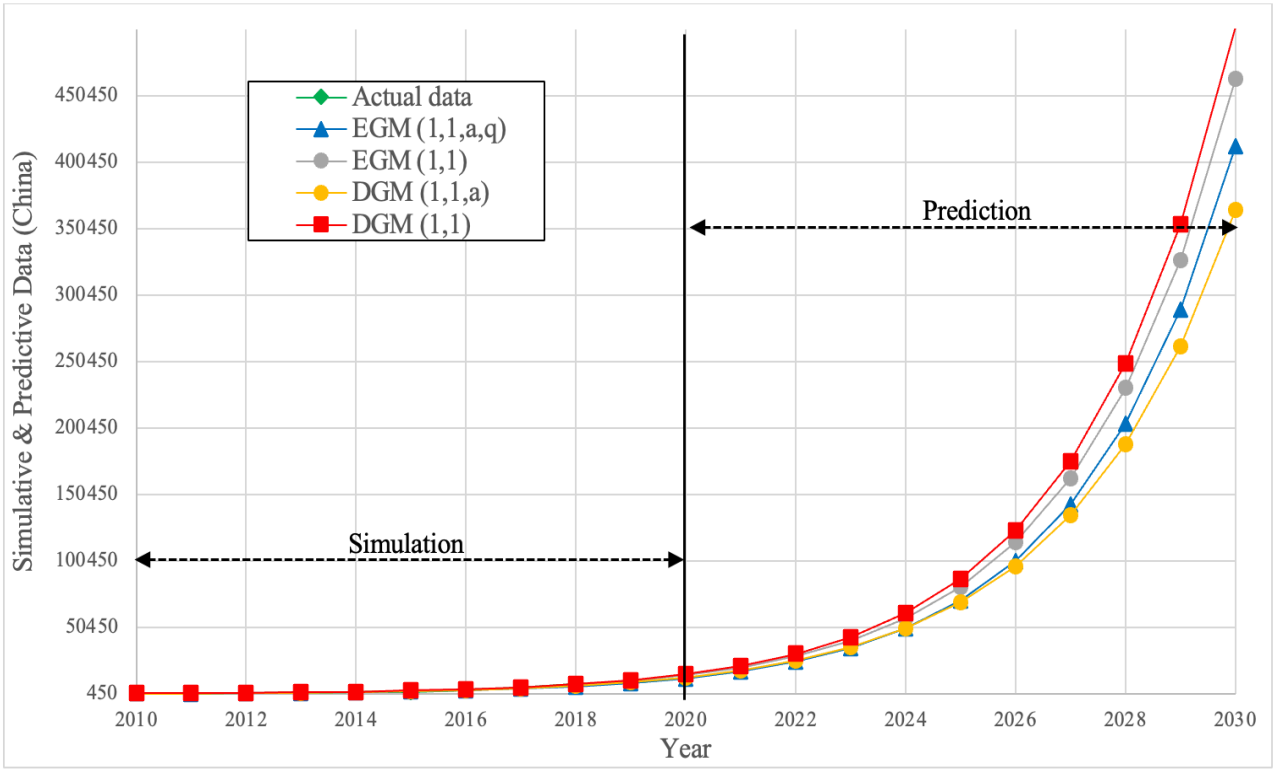


Figure 8: Graphical representation of UK data

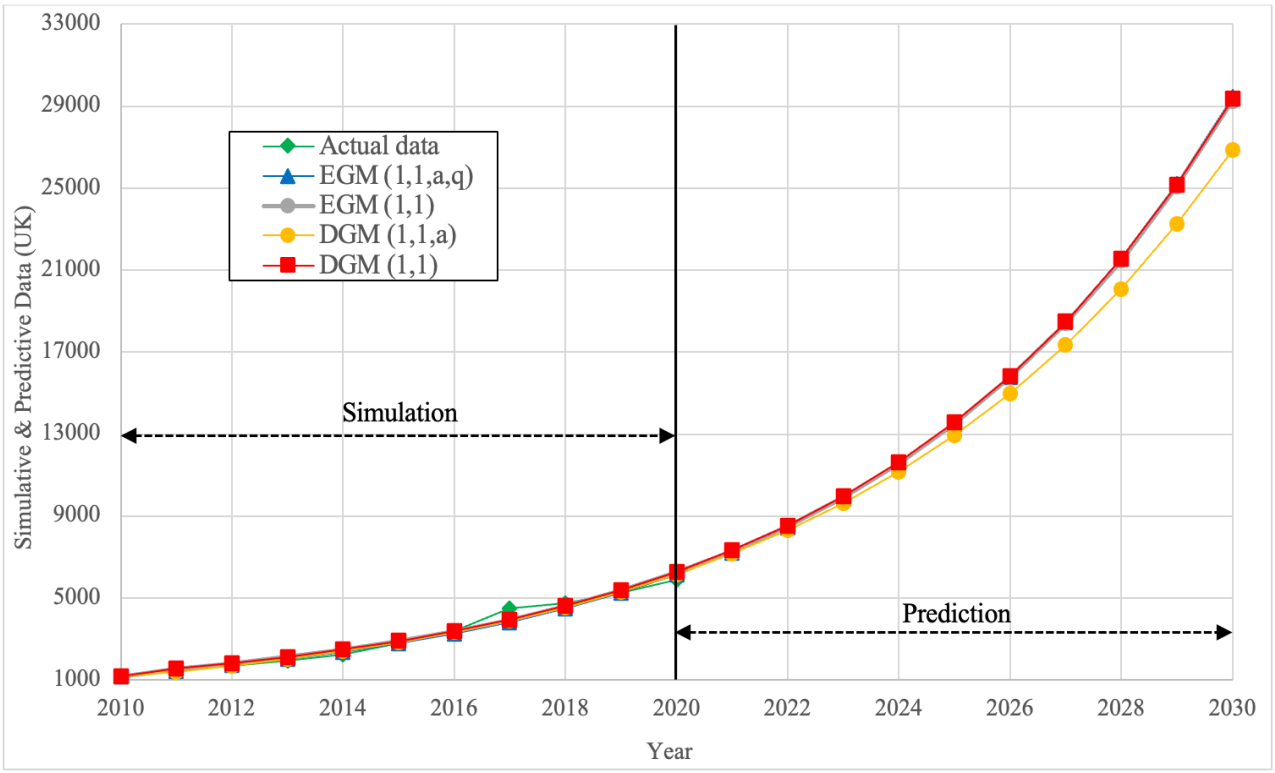


Figure 9: Graphical representation of India data

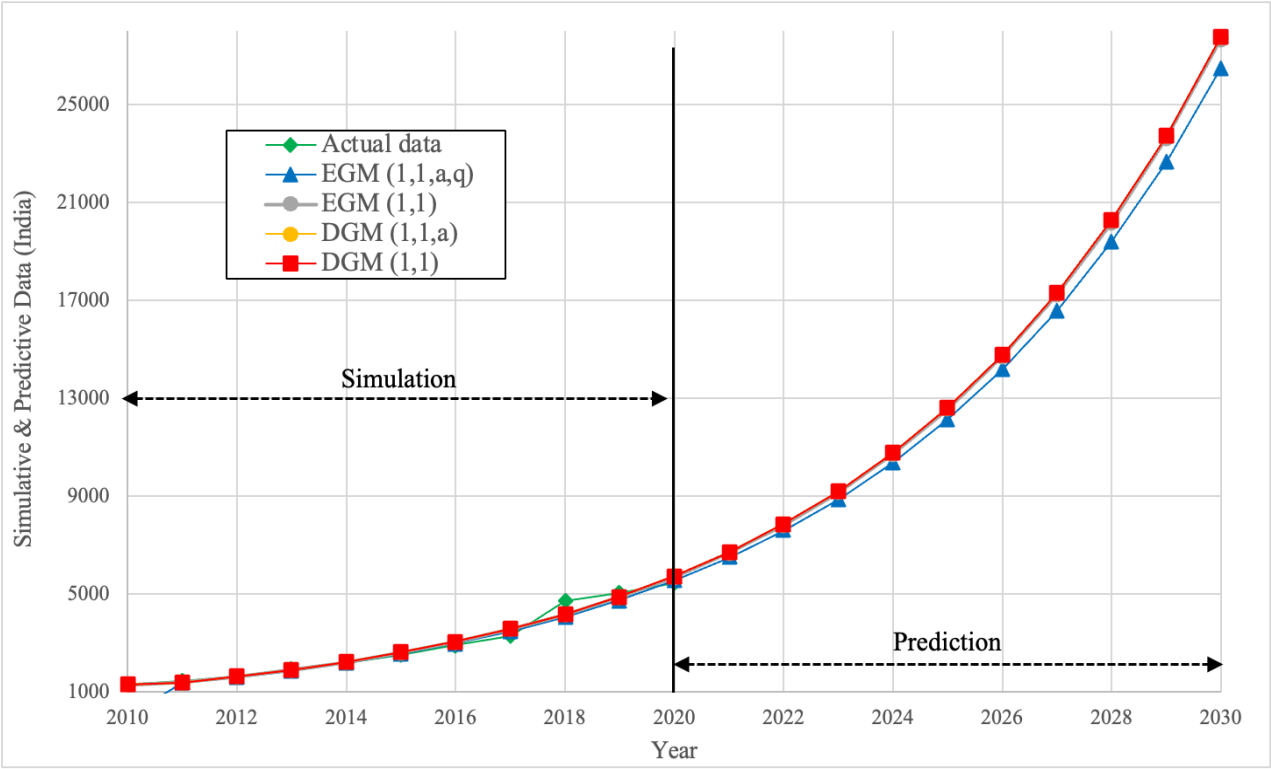


Figure 10: Graphical representation of Germany data

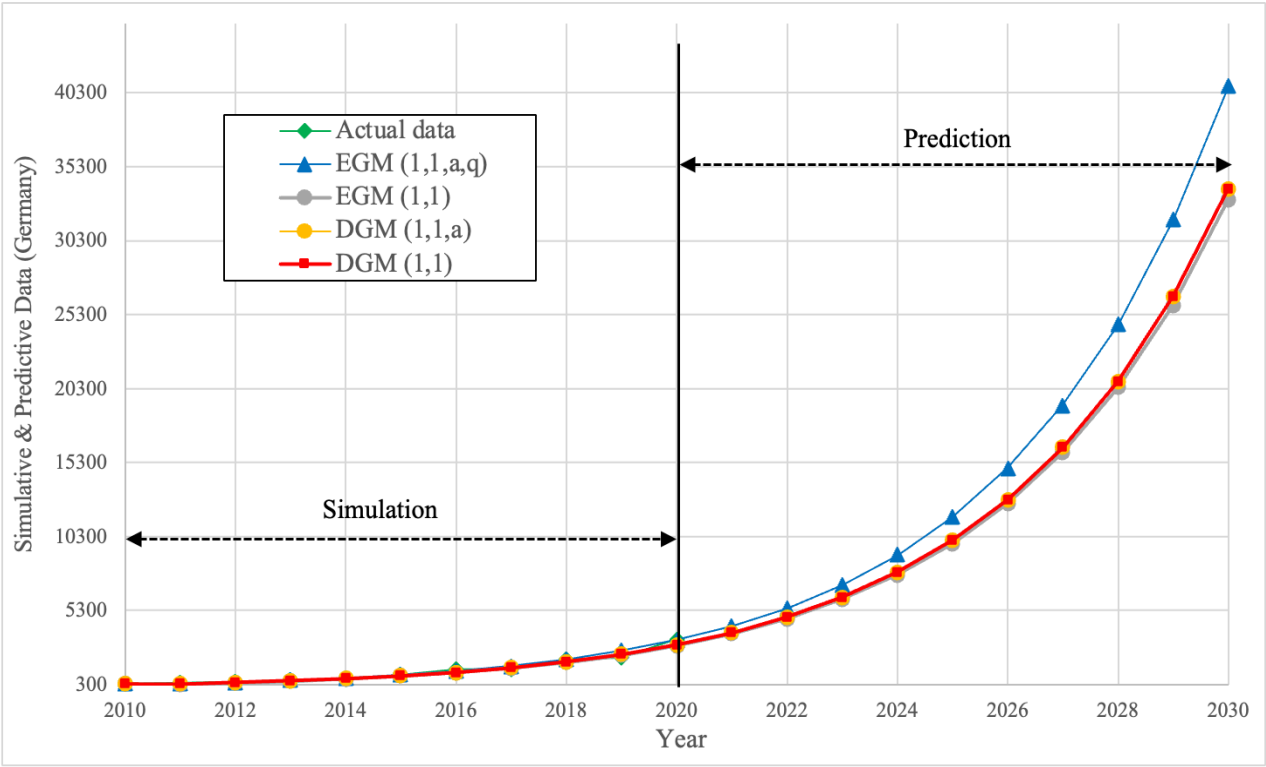
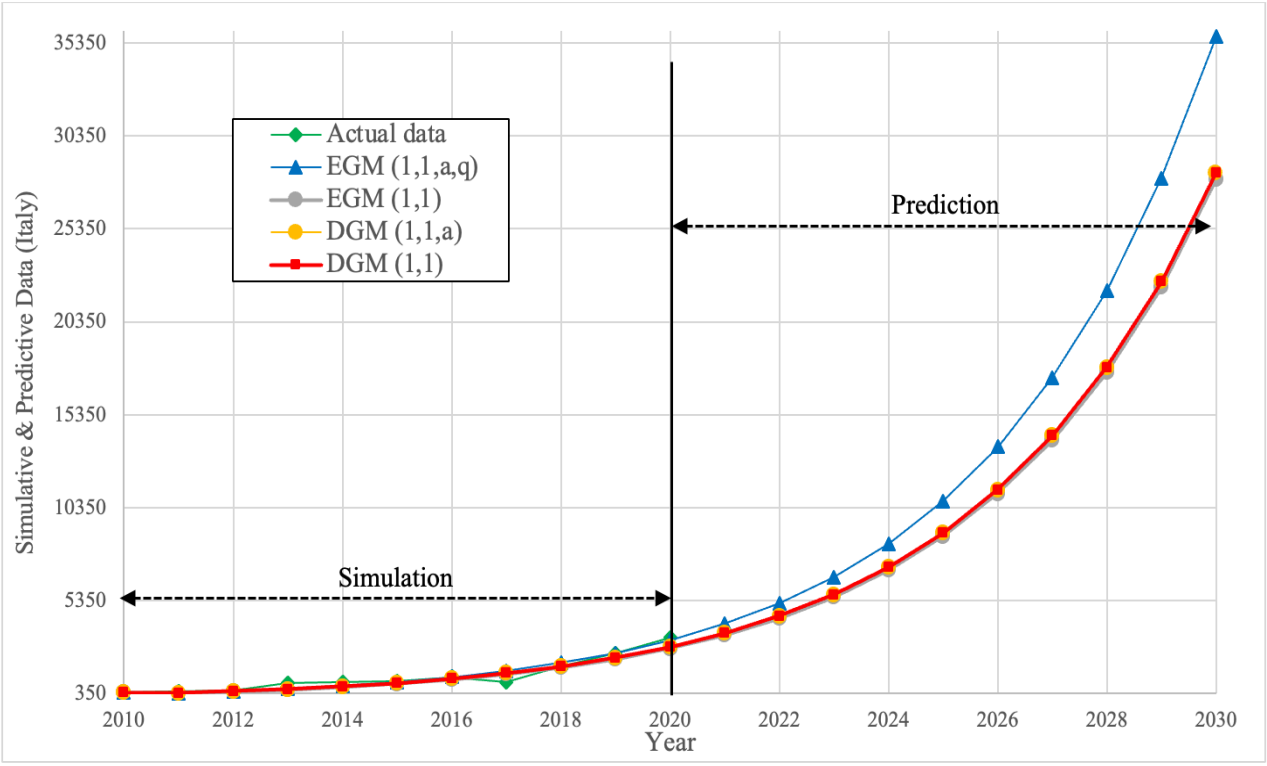


Figure 11: Graphical representation of Italy data



CHAPTER 5. PERFORMANCE IMPLICATIONS OF ISO/IEC 27001 CERTIFICATION

5.1. Purpose

This chapter analyses the relationship between the attainment of the ISO/IEC 27001 certification and firms' financial performance. More specifically, we performed an event study complemented by an ordinary least squares regression on a dataset of 143 US-listed companies.

5.2. Literature background

In light of a high and growing number of ISO/IEC 27001 certified companies, the debate on the topic has been gaining traction in the last few years. Initially, the studies were mostly of a technical nature, i.e., methods for control implementation and harmonization with other standards (e.g., Simić-Draws *et al*., 2013; Pardo *et al*., 2012). Only recently the debate has been intensifying on non-technical outlets (e.g., Mirtsch *et al*., 2021a; Deane *et al*., 2019). This mirrors a new attitude towards IS. There is indeed growing awareness of the fact that IS should be discussed well beyond the walls of IT departments, as it concerns market positioning, organizational practices, and complex trade-off decisions (Bower, 2020; Corallo *et al*., 2020; Burt, 2019).

The managerial research on the standard has been developing in three major research foci (see Chapter 3): *i) motivations* to certify; *ii) certification process*; *iii) performance implications* for certified firms. In addition to that, several studies have been focusing on *iv) contextual factors*.

As far as *i) motivations* are concerned, drawing from the renowned classification of Nair and Prajogo (2009), researchers reported the presence of functionalist and institutionalist motivations. Functionalist motivations reflect the expectations that the norm would support better IS processes and documentation. These are underpinned by the continuous improvement logic (e.g., Smith *et al*., 2010) as well as by the ISO/IEC 27001's pressure toward the acquisition of new IS skills and capabilities (Ku *et al*., 2009). Some papers indicate that firms also foresee better-defined roles and accountabilities (e.g., Kossyva *et al*., 2014; Crowder, 2013). Institutionalist motivations refer mainly to a better corporate image (Liao and Chueh, 2012a; Freeman, 2007) and the opportunity to attract more business (Pardo *et al*., 2012). It has

been also shown that firms certify following explicit requests from the customers, i.e., large private-sector corporations and governmental agencies demand their suppliers to be certified (Barafort *et al*., 2019; Smith *et al*., 2010). The presence of isomorphic dynamics and the global reputation of the ISO standards complete the picture (e.g., Stewart, 2018).

It is relevant to note that – with reference to ISO/IEC 27001 *ii) certification process* – most of the studies underline that the journey can be long and demanding. For instance, companies incur relevant costs in specialized consulting (e.g., Annarelli *et al*., 2020; Gillies, 2011). Organizations moreover need to invest considerable time in activities related to the set-up of the information management system (e.g., analysis, redesign, formalization of processes, and documentation development) (Dionysiou, 2012; van Wessel *et al*., 2011). Finally, it can be expensive to implement and manage the security controls suggested by ISO/IEC 27001 (Montesino *et al*., 2012). These costs and complexities might offset the benefits of the certification (Mirtsch *et al*., 2021b; Stewart, 2018).

Overall, the *iii) performance implications* related to ISO/IEC 27001 are far from being clear; previous studies show contradictory results. In terms of stock market performance and value of certified companies, both Deane *et al*. (2019) and Park *et al*. (2010) find positive effects, whereas Hsu *et al*. (2016), and Tejay and Shoraka (2011) do not confirm any relation. Similarly, Mirtsch *et al*. (2021b) argue that firms perceive ISO/IEC 27001 only as a preventive innovation without any benefit in terms of value creation. Moreover, these studies mostly focus on stock market reactions and therefore do not highlight specific effects on the different performance dimensions (revenues vs. costs). From a methodological standpoint, further limitations arise considering the size of the analysed samples (less than 35 organizations - Hsu *et al*., 2016; Tejay and Shoraka, 2011; Park *et al*., 2010) as well as potential issues in the use of perceptual measures in surveys (Mirtsch *et al*., 2021b; Park *et al*., 2010).

Sparse and conflicting considerations on the effects of ISO/IEC 27001 also emerge from case research and expert opinions. In terms of the certification's impact on firms' bottom line, lower IS risk levels (Freeman, 2007) and improved business continuity (Rezaei *et al*., 2014) have been linked to companies avoiding profit losses (e.g., legal costs resulting from information leakage and misuse - Bakar *et al*., 2015). Lower expenses have been motivated as well by advantageous insurance premiums to certified organizations (Gillies, 2011). Previous research has also indicated that ISO/IEC 27001 can lead to a reduction of redundancies and clearer roles and accountabilities due to a more structured approach to information-related

processes (Crowder, 2013). However, the formalization required by the standard may lead to a loss of flexibility with negative effects on labour productivity and on the capacity to meet clients' requests (van Wessel *et al*., 2011).

The benefits are equally not clear looking at the effects of being certified on the top line. Overall, the literature supposes a positive impact on revenues as customers might prefer firms able to prove a structured approach to IS (e.g., Crowder, 2013). The ISO/IEC 27001 can also represent a "ticket to the market" for exporting companies (Dionysiou, 2012) and contractors operating in offshored countries – e.g., Taiwan, Singapore, and India – because of the need to ensure intellectual property protection to international customers (Ku *et al*., 2009). Notwithstanding these considerations and in contrast with the high credibility of the standard (Hlača *et al*., 2008), it has also been argued that the certification provides a limited reputational advantage by itself. This is because customers are aware that certified firms can have different levels of absorption, namely implementing the norm's requirement only formally without changing their actual practices (e.g., Culot *et al*., 2019).

The literature has also debated *iv) contextual factors* mostly related to industry and geographical idiosyncrasies as well as to the technological profile and previous ISO experience of the certified companies. The studies of Mirtsch *et al.* (2021a), Gillies (2011), and Cots and Casadesús (2015), indicated that there are more certifications in technological industries and in countries where the government has pursued regulatory or promotion activities (as such companies value the benefits of ISO/IEC 27001 higher than firms outside these contexts – Mirtsch *et al*., 2021b). Finally, some studies have questioned the standard effectiveness in guaranteeing IS against more complex and innovative technological environments (e.g., those determined by cloud computing and the Internet of Things), suggesting the integration of other technology-specific standards (Leszczyna, 2019; Ku *et al*., 2009).

To summarize, previous research indicates that the ISO/IEC 27001 certification is pursued not only expecting higher levels of IS but also more cost-efficient processes for information-related activities as well as commercial benefits. Notwithstanding the financial and non-financial resources that are invested to attain the certification, the evidence on ISO/IEC 27001 effects on performance is contradictory and mostly anecdotical. This echoes the previous debate on other certifications such as ISO 9001 (Corbett *et al*., 2005), ISO 14001 (Treacy *et al*., 2019; De Jong *et al*., 2014), OHSAS 18001 (Yang *et al*., 2021; Lo *et al*., 2014), and SA 8000 (Orzes *et al*., 2017). All these papers – which are based on the analysis of secondary data through event

study methods – stemmed from the premise that the absence of hard evidence on the financial effects of certification would ultimately hamper the understanding of their value and opportunities. In this sense, the most investigated financial performance dimensions were profitability, labour productivity, and sales-related metrics. In some cases, also the potential effects of the characteristics of the certified firms or the industry have been investigated in order to assess whether context-specific factors may influence the outcomes of the standard application (Yang *et al*., 2021; Orzes *et al*., 2020, 2017; Lo *et al*., 2014, 2013).

5.3. Research framework

In this section, we formulate a set of research hypotheses related to the effects of ISO/IEC 27001 on firms' financial performance (RQ1) and contextual variables affecting the relationship (RQ2).

As for RQ1, consistently with similar studies on other international standards (e.g., ISO 9001, ISO 14001, SA 8000, UNGC, HACCP, OHSAS 18001 – Corbett *et al*., 2005; De Jong *et al*., 2014; Orzes *et al*., 2017, 2020; Liu *et al*., 2021; Yang *et al*., 2021), the following dimensions are taken into account: profitability, labour productivity, and sales performance. Our reasoning is based on the application of some theoretical frameworks broadly used in the study of management systems (Culot *et al*., 2021; Tuczek *et al*., 2018; Lo *et al*., 2014) which seemed in line with the current scientific knowledge on the standard outlined in the previous section.

Starting with *profitability*, extant research shows that ISO/IEC 27001 is related to IS improvements and avoidance of profit losses. This is supported by the High-Reliability Theory (HRT) (La Porte, 1996; Roberts, 1990). According to the core tenets of the theory, organizations operating high-hazard technological systems – e.g., nuclear power plants, nuclear aircraft carriers, and air traffic control – can prevent accidents by applying solutions and processes that provide guidance against numerous and complex risk factors. As far as management systems standards are concerned, HRT has mainly been applied to workers' safety (Lo *et al*., 2014; Levine and Toffel, 2010). The initial theorization was limited to organizations with peculiar operational needs; however, further elaborations extended the same reasoning to a broader pool of companies, namely "reliability-seeking organizations" that operate in high-hazard environments (Vogus and Welbourne, 2003). These contexts are characterized by

complex, rapidly changing, and tightly coupled organization-environment relations. The challenges posed by digitalization reflect this picture.

As known (e.g., Lezzi *et al*., 2018; Xie *et al*., 2016), in modern organizations IS risk comes not only from an ever-increasing technological complexity and the proliferation of entry points (e.g., in relation to the Internet of Things, cloud computing, system integration), but it is also related to human factors such as malicious behavior and mere inattention (e.g., in password storage and response to phishing attacks). In such contexts, the formalization required by ISO/IEC 27001 not only provides targeted instructions at different levels of the organization but also spreads IS know-how throughout the company, thus preventing information-related accidents to happen. Accident prevention means in turn that firms are more likely to avoid financial losses related to business discontinuities, legal fees, compensations, and customer churn. Moreover, against the prospects of the cost of the certification exceeding its benefits, the ISO/IEC 27001 guidelines require IS management systems to be designed accordingly to the profile of the certified organizations. In shaping their ISMS, the flexibility inherent in the standard's guidelines allows companies to avoid unnecessary IS investments and operating expenses by aligning on what is actually needed for their specific situation (e.g., Smith *et al*., 2010). This is consistent with HRT discouraging a one-size-fits-all approach in complex environments. The same line of reasoning is also valid from the perspective of the Resource-Based View (RBV) (Barney, 1991). Consistently with the arguments of Mirtsch *et al*. (2021b) and Culot *et al*. (2021), it is possible to see IS as a strategic resource encompassing both tangible (e.g., specific devices) and intangible (e.g., employee capabilities and awareness) aspects. In this sense – similarly to other management system standards (Orzes *et al*., 2020; Prajogo, 2011) – routines/procedures that stem from the introduction of ISO/IEC 27001 may help organizations to build internal capabilities and select the most appropriate technological investments. At the same time, the impact of ISO/IEC 27001 is that of a "preventive innovation" (Mirtsch *et al*., 2021b; Rogers, 2002; Rogers, 1988), whose purpose is namely to avoid unwanted consequences. We thus posit that:

H1. There is a significant positive relationship between ISO/IEC 27001 certification and profitability.

The same theoretical perspectives can be applied to formulate a relationship between certification and *labour productivity*. Previous case-based research and expert studies indicate

improvements due to higher process efficiency in information-related activities across the organization (Kossyva *et al*., 2014; Crowder, 2013). From an HRT perspective (e.g., Cantu *et al*., 2020; Sawyerr and Harrison, 2019; Faraj and Xiao, 2006), the presence of formal coordination practices – such as protocols and knowledge-sharing processes – can create clarity around what needs to be done and thus reduce redundant efforts. Theory, moreover, suggests that formalization does not prevent organizations from innovating through individual efforts. On the other way round, HRT indicates that companies need to work on routinizing constant minor modifications in their processes and procedures to achieve excellence. This seems related to the continuous improvement logic that underpins ISO/IEC 27001. Similar arguments can be formulated based on the RBV, which has been mostly used as a basis to posit the internal impacts of certifications in terms of more efficient operational practices (e.g., Orzes *et al*., 2020). Therefore, it can be assumed that:

H2. There is a significant positive relationship between ISO/IEC 27001 certification and labour productivity.

As far as *sales performance* is concerned, the prospect of higher revenue opportunities for ISO/IEC 27001 certified firms is mentioned in the literature. This is consistent with the presence of institutionalist motivations underpinning firms' decisions to certify (Mirtsch *et al*., 2021a; Culot *et al*., 2021): companies seek the certification to prove their reliability to external stakeholders – first of all, their customers – who are not in the position to verify firsthand internal procedures and controls. The Signaling Theory (ST) (Connelly *et al*., 2011; Spence, 1978) seems appropriate to explain this dynamic as it clarifies that social selection often occurs under conditions of imperfect information. Such theoretical perspective has been extensively used in the field of international management standards (e.g., Delmas and Montiel, 2009; Terlaak and King, 2006; King *et al*., 2005; Orzes *et al*., 2020). In particular, drawing from the central tenets of ST, extant research indicates that certification provides a practical tool to "signal" to the market that the organization adopts a proven approach. ST has been also adopted in the context of IS (Lansing *et al*., 2019) showing, however, that recipients decompose certifications into a set of more fine-grained signals that are differently weighted to evaluate certifications. Overall, we assume that customers prefer companies sending such signals, thus the following hypothesis is formulated:

H3. There is a significant positive relationship between ISO/IEC 27001 certification and sales performance.

As far as RQ2 is concerned, previous research on other standards indicates that the relationship certification-performance can be affected by industry- and/or firm-specific elements (Yang *et al*., 2021, Orzes *et al*., 2017; Lo *et al*., 2014, 2013). *Contextual factors* have been mentioned in the literature on ISO/IEC 27001 as well (Culot *et al*., 2021); their relevance has been tested in relation to the standard diffusion (e.g., Mirtsch *et al*., 2021a; Gillies, 2011). We thus posit that also the relationship between the ISO/IEC 27001 certification and financial performance might be affected by the specific situation of the certified firm. Overall, our hypotheses on contextual factors are based on the Contingency Theory, which postulates that there is no best way to manage a company as strategies and actions depend upon the situation of the firm, both in terms of internal and external factors (Donaldson, 2001). The theory has been applied also to other standards (e.g., Orzes *et al*., 2017; Narasimhan *et al*., 2015) to explain the different performance effects resulting from the attainment of a certification in different contexts.

The first factor that may affect the relationship between ISO/IEC 27001 certification and financial performance is related to the level of internationalization of the certified firm (i.e., the extent to which the firm sells its products/services abroad rather than in the domestic market – Chakrabarty and Wang, 2012). This is motivated by two considerations. On the one hand, ISO/IEC 27001 acts as *lingua franca* of IS: it enables internationalized firms to implement an overarching approach incorporating different local requirements and it provides guidance independently from local specificities (Simić-Draws *et al*., 2013). On the other hand, the strength of the "ISO brand" seems particularly relevant to qualify firms in international markets, not to mention the governmental initiatives launched in different countries in its support (e.g., Culot *et al*., 2021). We, therefore, assume that:

H4. The effect of ISO/IEC 27001 certification on financial performance is significantly affected by the degree of internationalization of the certified firm.

The second factor refers to the technological context in which the norm finds application. Although ISO/IEC 27001 is by design applicable irrespective of the firm adopting any information or data processing technology (ISO/IEC 27001:2013), it has been noted that its relevance is perceived mainly in highly digitalized contexts (Crowder, 2013). In this sense, the

different levels of adoption depending on the industry might also be related to information being handled in digital forms and thus potentially subject to attacks (Heston and Phifer, 2011; Mukhtar and Ahmad, 2014). Moreover, even though the literature (e.g., Park and Lee, 2014) highlights that more specific standards are needed to face the challenges represented by emerging technologies – e.g., cloud computing and the Internet of Things – it has also been argued that ISO/IEC 27001 could serve as the backbone on which these standards can be integrated (e.g., Leszczyna, 2019). Overall, it can be assumed that firms operating in environments with higher technological intensity would not only be more inclined to invest in a substantial internalization of the ISO/IEC 27001 dictates, but also extract the most value out of the certification. Therefore, we posit that:

H5. The effect of ISO/IEC 27001 certification on financial performance is significantly affected by the level of technological intensity of the industry.

5.4. Methodology

To test the research hypotheses, we resorted to the longitudinal event-study methodology (RQ1) complemented by an ordinary least squares (OLS) regression (RQ2). Based on the analysis of publicly available financial data, this combination enables the detection of the abnormal performance resulting from the specific event under investigation (in our case the attainment of the ISO/IEC 27001 certification), as well as the identification of the factors affecting the relationship. We decided for this approach for three reasons. First, it is the most robust and widely acknowledged statistical procedure to study the performance implications of management standards; previous contributions have adopted it to investigate, among the others, ISO 9001 (e.g., Corbett *et al*., 2005), OHSAS 18001 (e.g., Yang *et al*., 2021), ISO 14001 (e.g., De Jong *et al.*, 2014), and SA 8000 (e.g., Orzes *et al*., 2017). Second, by comparing the performance of certified and similar non-certified organizations before and after the event (certification), the event study allows to establish a connection between the certification and the investigated performance dimensions (Treacy *et al*., 2019: Lo *et al*., 2014). Third, the performance benefits can be tracked and measured quantitatively through reliable secondary data sources (i.e., financial statements) avoiding potential issues related to the perceptual measures adopted in surveys (e.g., De Jong *et al*., 2014).

In this study, we focused on US-listed public companies. The choice was motivated by the need to identify a broad set of certified firms – listed companies give publicity to the attainment

of internationally recognized certifications – and to retrieve and compare reliable accounting data.

As there is no publicly available full list of ISO/IEC 27001 companies (ISO does not collect firm-level information from the certification bodies), the sample was built in three steps drawing from previous contributions on the topic (e.g., Deane *et al*., 2019; Podrecca *et al.,* 2021). First, we searched in Factiva and Business Wire databases for announcements of ISO/IEC 27001 certified firms between 2005 (ISO/IEC 27001 publication year) and 2018. As a second step, we screened the announcements, performed an additional news search (for each firm) with Factiva, Business Wire, and Google search engines, and double-checked firms' official websites and Twitter pages to verify that: *i.* the announcing firm had actually certified and the exact date of certification; *ii.* there were no other events within the same timeframe influencing identified firms' performance, following the suggestions of McWilliams and Siegel (1997) to look for "confounding events". Finally, we combined our initial firm list with financial data from the Thomson Reuters Eikon database.

The final dataset consisted of 143 firms. Table 16 shows the distribution of the sampled firms by industry and by certification year. If compared with the ISO survey for the period under examination (i.e., certified firms up to 2018 - ISO, 2018), our dataset displays a good representation of the population of ISO/IEC 27001 certified organizations with available industry information (ISO provides this data for approximately one-third of the firms). For instance, firms operating in ICT/IT related industries represent the 65% of the overall population, while they account for the 67% of our data (96 out of 143 total companies). Similarly:

- Service firms (non-ICT/IT related) are the 13% of the population and the 12% of the dataset (17 companies).
- Non-ICT/IT related manufacturing companies represent the 7% of the whole certified companies and account for the 10% of the dataset (14 companies).
- Wholesale & retail trade companies are the 3% of the population and constitute the 2% of the dataset (3 companies).

The distribution is also consistent with previous large-scale empirical studies on ISO/IEC 27001 (Mirtsch *et al*., 2021a; Deane *et al*., 2019).

Table 16: Dataset breakdown by industry and by ISO/IEC 27001 certification year

Industry	SIC code	Number of companies
Manufacturing	20-39	48
(of which ICT/IT related)		*34*
Transportation and public utilities	40-49	11
(of which ICT/IT related)		*9*
Wholesale & retail trade	50-59	3
Finance, Insurance, and Real Estate	60-67	11
Services	70-89	70
(of which ICT/IT related)		*53*
TOTAL		**143**

Year	Frequency	Year	Frequency
2005	5	2012	6
2006	11	2013	5
2007	5	2014	8
2008	16	2015	15
2009	10	2016	14
2010	8	2017	23
2011	5	2018	12

In order to test hypotheses H1, H2, and H3 we employed the event-study approach to detect whether the 143 sampled ISO/IEC 27001 certified companies presented a significant abnormal performance against a set of similar control firms (ISO/IEC 27001 non-certified). We set the event period as the year the certification was obtained (year t) and the year preceding the certification (t-1), as the process to certify according to ISO/IEC 27001 dictates is reported to last between 6 and 18 months (van Wessel *et al*., 2011). Year t-2 was considered the base year (i.e., the year free from the event – Treacy *et al*., 2019) and used to determine the control firm sample. Year t-3 was taken into account to control for endogeneity issues; this way verifying whether the impact of ISO/IEC 27001 on a firm's performance was actually driven by the certification (Orzes *et al*., 2017; Lo *et al*., 2014).

The three performance measures under investigation – *profitability* (H1), *labour productivity* (H2), and *sales performance* (H3) – were operationalized following previous event studies on international management standards (e.g., Podrecca *et al.,* 2021; Orzes *et al*., 2020, 2017; Lo *et al*., 2014). Specifically, we resorted to the return on assets (ROA) for *profitability* (*H1*); the ratio of operating income to the number of employees for *labour productivity* (*H2*); year-over-year sales growth for *sales performance* (*H3*).

The control set of ISO/IEC 27001 non-certified firms was identified consistently with Orzes *et al*. (2017) and Hendricks *et al*. (2007). For each certified firm and for each performance measure under investigation we created a distinct control portfolio. The portfolio creation process followed the three criteria defined by Barber and Lyon (1996): industry (certified and control firms should have the same two-digit SIC code), size (control firms should have total assets ranging between 50% and 200% of the certified firm in the base year) and performance comparability (control firms should show data ranging between 90% and 110% of the certified firm's considered performance – *profitability*, *labour productivity*, *sales performance* – in the base year). Should no firm match, the first criterion was changed to one-digit SIC code and then dropped (Orzes *et al*., 2020; Barber and Lyon, 1996).

On average each certified company matched with 7.30 control firms; similar ratios have been found in Orzes *et al*. (2017) and Treacy *et al*. (2019), among others.

Abnormal performance (AP) of the certified organizations was defined as follows:

$$AP_{(t+b)} = PS_{(t+b)} - EP_{(t+b)}$$

$$EP_{(t+b)} = PS_{(t+a)} + (PC_{(t+b)} - PC_{(t+a)})$$

where EP is the expected performance, PS is the actual performance of the sampled firms, PC is the median performance of control firms, t is the year of certification, a is the starting year of comparison (-3, -2, - 1, 0, 1), and b is the ending year of comparison (-2, - 1, 0, 1, 2). Given that our data were not normal (Shapiro-Wilk Tests), we tested whether AP differed significantly from zero through non-parametric tests. These were selected for their proven robustness in evaluating paired data of event studies both for symmetric – Wilcoxon signed-rank test (WSR) – and skewed distributions – sign test (De Jong *et al*., 2014; Barber and Lyon, 1996). For the sake of completeness, in presenting the results, we also reported the outcomes of the parametric t-tests.

To investigate *H4* and *H5,* we performed an OLS regression on the abnormal ROA between t-2 to t+2. We decided to focus on ROA as this measure is representative of the overall financial effectiveness of management system standards (Lo *et al*., 2014). A similar approach was already adopted for SA 8000 (Orzes *et al*., 2017), OHSAS 18001 (Lo *et al*., 2014; Yang *et al*., 2021), and ISO 9001 (Lo *et al*., 2013). As for the independent variables, H4 assumes the effect of ISO/IEC 27001 on financial performance to be affected by the degree of internationalization of the certified firm. Consistently we included the variable *internationalization* operationalized as the ratio of firm foreign sales to its total sales in the base year (Yang *et al*., 2021; Chakrabarty

and Wang, 2012). H5 suggests that the effect of ISO/IEC 27001 on financial performance is affected by the technology intensity of the industry in which the certified firms operate. Hence, we followed Kile and Phillips (2009) high-tech industries categorization and included a dummy variable (*high-tech*) having value "1" for firms operating in the following industries (defined at the three-digit SIC code level): 283 – Drugs, 357 – Computer and Office Equipment, 366 – Communication Equipment, 367 – Electronic Components and Accessories, 382 – Laboratory, Optic, Measure, Control Instruments, 384 – Surgical, Medical, Dental Instruments, 481 – Telephone Communications, 482 – Miscellaneous Communications Services, 489 – Communication Services, NEC, 737 – Computer Programming, Data Processing, 873 – Research, Development, Testing Services.

To ensure the rigorousness of our model, we also controlled for several industry- and firm-level variables that could impact the sample firms' abnormal performance:

- *ISO experience* (dummy: previous ISO 9001 certification – Orzes *et al*., 2017) to account for organizational learning dynamics. Firms already having standardized managerial practices may get less benefits from the certification (Swink and Jacobs, 2012); however, experienced organizations possess greater abilities to acquire, evaluate and assimilate the new routines (Culot *et al*., 2021);
- *year* (year of certification) as motivations and outcomes may differ between early and late certified firms (Lo *et al*., 2014);
- *age* (years since the firm foundation at the time of ISO/IEC 27001 certification – Jacobs *et al*., 2015) as accumulated experience may help firms in achieving higher benefits from certifications (Wang and Zhao, 2020);
- *pre-certification ROA* (ROA in the base year) since firms with higher initial performance may experience a lower degree of improvement (Orzes *et al*., 2020);
- *firm size* (natural logarithm of firm total assets in the base year – Dong *et al*., 2020). Larger firms have more resources (De Zoysa *et al*., 2021) but smaller firms tend to be more focused and agile, easing the introduction of new management philosophies (Malik and Abdallah, 2020);
- *capital intensity* (ratio of assets by revenues in the base year – Su *et al*., 2015) as more capital-intensive firms may get higher benefits from the certification (Culot *et al*., 2021);

- *industry size* (natural logarithm of industry total assets in the base year, the industry is defined by two-digit SIC code – Lo *et al*., 2013) as companies operating in large industries may be subject to higher scrutiny (Terlaak and King, 2006);
- *industry efficiency* (industry median ROA in the base year, the industry is defined by two-digit SIC code – Lo *et al*., 2013) as the impact of the certification in terms of process improvements might be lower for firms operating in contexts characterized by higher efficiency (Lo *et al*., 2013);
- *industry competitiveness* (1-Herfindahl index in the base year, the industry is defined by two-digit SIC code – Podrecca *et al*., 2021) as international management standards may provide less advantages in highly competitive contexts (Podrecca *et al*., 2021).

Table 17 provides the correlation matrix.

Table 17: Correlation matrix

	Internationalization	*High-Tech*	*ISO Experience*	*Age*	*Year*	*Firm Size*	*Industry Competitiveness*	*Industry Size*	*Industry Efficiency*	*Capital Intensity*	*Pre-certification ROA*
Internationalization	1										
High-Tech	0.14+	1									
ISO Experience	0.07	0.10	1								
Age	0.05	-0.02	-0.06	1							
Year	-0.02	-0.13	-0.11	0.02	1						
Firm Size	0.03	-0.19*	-0.04	0.28***	-0.04	1					
Industry Competitiveness	0.12	-0.12	0.19*	-0.01	0.25**	0.05	1				
Industry Size	0.06	0.05	0.07	0.08	0.12	0.26**	0.65***	1			
Industry Efficiency	-0.08	-0.03	0.14+	0.08	-0.42***	0.07	-0.08	-0.16+	1		
Capital Intensity	-0.04	-0.14+	-0.20*	-0.06	-0.01	0.18*	0.05	0.19*	-0.05	1	
Pre-certification ROA	0.02	-0.17*	0.13	0.12	-0.07	0.40***	-0.06	0.02	0.09	-0.04	1

Note: +p<0.1, *p<0.05, ** p<0.01, *** p<0.001

5.5. Results

5.5.1. Event study

The performance implications of ISO/IEC 27001 on certified firms were studied investigating the presence of abnormal performance between certified and similar non-certified companies on three indicators – profitability, labour productivity, and sales performance. The results are reported in Table 18. For each indicator and considering different time intervals, the table includes the characteristics of the distribution (normality and skewness), the number of observations, the mean (AP mean) and the median (AP median) of the abnormal performance, and the results of the tests. As stated in the methodology section, in case of symmetric distribution we referred to the WSR test, while if data were skewed the sign test was taken into account.

In terms of profitability, we found statistically significant and positive differences between certified and non-certified firms from years t+1 to t+2, t to t+2, t-2 to t+1, and t-2 to t+2 (H1 is supported).

For labour productivity, the results showed significant positive abnormal performance from years t+1 to t+2, t to t+2, and t-2 to t+2 (H2 is supported). This finding is particularly interesting: firms achieve relevant productivity benefits only when they have completely assimilated/internalized the new practices related to ISO/IEC 27001 (i.e., in year t+2).

Finally, in terms of sales, significant positive abnormal performance emerged from years t-2 to t-1, t-2 to t, t-2 to t+1, and t-2 to t+2. These results show that sales performance improvements are mainly achieved along the certification pathway, rather than in the post-certification period (H3 is only partially supported).

Consistently with the methodological approach of Orzes *et al*. (2017) and Lo *et al*. (2014), we also verified the absence of abnormal changes before the certification (t-3 to t-2). This test examined whether the impact of ISO/IEC 27001 was actually driven by the certification or whether firms were already achieving superior performance. The results included in Table 18 indicate no significant abnormal performance between t-3 and t-2. Performance changes appeared only after the firms entered the event period (t-1 onwards). This allows us to exclude the presence of systematic biases between sample and control firms thus confirming the robustness of our findings and the relationship certification-performance.

Table 18: Results of the event-study analysis

	Period	Normality	Skewness	N	AP Mean	AP Median	p-value (t-test)	p-value (WSR)	p-value (sign test)
Profitability (return on assets)									
Single-year periods	t-3 to t-2	NO		137	0.52%	0.26%	0.245	0.190	0.366
	t-2 to t-1	NO	S	139	1.34%	0.28%	0.122	0.213	0.249
	t-1 to t	NO	S	139	-0.45%	0.04%	0.637	0.464	0.433
	t to t+1	NO		138	0.67%	0.46%	0.257	0.193	0.222
	t+1 to t+2	NO	S	138	2.47%	1.20%	0.005**	0.001***	0.000***
Multi-year periods	t-2 to t (certification window)	NO	S	139	0.90%	0.75%	0.222	0.329	0.154
	t to t+2 (post-certification window)	NO	S	138	3.14%	1.29%	0.010**	0.004**	0.011*
	t-2 to t+1 (first-year post-certification)	NO		138	1.61%	0.97%	0.049*	0.024*	0.011*
	t-2 to t+2 (full event window)	NO	S	138	4.08%	1.55%	0.002**	0.000***	0.000***
Labour productivity (operating income/number of employees)									
Single-year periods	t-3 to t-2	NO	S	132	2461.25	1450.45	0.385	0.338	0.271
	t-2 to t-1	NO		137	2966.60	587.90	0.300	0.367	0.197
	t-1 to t	NO	S	135	3976.80	2583.57	0.315	0.084+	0.151
	t to t+1	NO	S	134	6830.55	388.49	0.199	0.302	0.466
	t+1 to t+2	NO	S	134	17805.79	3964.59	0.034*	0.002**	0.001***
Multi-year periods	t-2 to t (certification window)	NO		135	6320.63	553.17	0.215	0.376	0.365
	t to t+2 (post-certification window)	NO	S	134	24636.34	5744.78	0.058+	0.003**	0.010**

	t-2 to t+1 (first-year post-certification)	NO	S	134	13253.82	1673.79	0.039*	0.284	0.398
	t-2 to t+2 (full event window)	NO	S	134	31059.61	8304.21	0.009**	0.002**	0.015*

Sales performance (yearly sales change)

Single-year periods	t-3 to t-2	NO	S	132	-7.42%	-3.32%	0.986	0.966	0.966
	t-2 to t-1	NO	S	136	8.93%	4.52%	0.002**	0.001***	0.006**
	t-1 to t	NO		136	-0.32%	0.36%	0.536	0.556	0.334
	t to t+1	NO		135	-2.57%	-2.06%	0.794	0.819	0.635
	t+1 to t+2	NO	S	134	4.24%	0.70%	0.089*	0.102	0.333
Multi-year periods	t-2 to t (certification window)	NO	S	136	8.61%	3.79%	0.001**	0.002**	0.016*
	t to t+2 (post-certification window)	NO	S	134	1.88%	0.07%	0.314	0.387	0.466
	t-2 to t+1 (first-year post-certification)	NO	S	135	6.23%	3.70%	0.006**	0.015*	0.029*
	t-2 to t+2 (full event window)	NO	S	134	10.54%	4.89%	0.000***	0.000***	0.002**

Note: + p<0.1, *p<0.05, ** p<0.01, *** p<0.001

5.5.2. Ordinary least squares regression

Table 19 presents the results of the OLS regression performed to shed light on the possible factors affecting the financial outcomes of ISO/IEC 27001 certification. The model did not present multicollinearity issues, as the variance inflation factors (VIF) were beyond the threshold for all the parameters (VIF<10) (Allison, 1998). See Table 17 for the correlation matrix.

The findings show a significant and positive effect of the internationalization degree of the certified firms (H4 is supported). On the other hand, the technological level of the industry has no effect (H5 is not supported). Moving to the control variables, the outcomes are negatively affected by the certification year and the previous performance of the certified firm.

As the results of the OLS regression do not support H5, we repeated the analysis using two alternative measures. First, we used the same dummy variable (*high-tech*) as in the main analysis but with high-tech industries defined at two-digit rather than three-digit SIC code level. Second, we operationalized technology intensity (at the firm level) as the ratio of R&D expenses to the firm sales in the base year (Lo *et al*., 2013). The outcomes are qualitatively the same as in the main analysis (i.e., negative sign and not significant).

Table 19: Results of the OLS analysis

Dependent variable=**ROA**	OLS (n=138)		
	Estimated coefficients (Standard errors)	Statistical significance	VIF
Explanatory variables			
Internationalization	0.111 (0.051)	0.0320*	1.071
High-Tech	-0.048 (0.032)	0.1362	1.236
Control variables			
ISO Experience	0.041 (0.029)	0.1518	1.182
Age	-0.001 (0.001)	0.5491	1.125
Year	-0.008 (0.004)	0.0326*	1.374
Pre-certification ROA	-0.296 (0.102)	0.0043**	1.284
Firm Size	0.007 (0.007)	0.3242	1.505
Capital Intensity	-0.003 (0.010)	0.8045	1.165
Industry Size	-0.009 (0.016)	0.5814	2.202
Industry Efficiency	0.482 (0.932)	0.6057	1.328
Industry Competitiveness	0.105 (0.420)	0.8035	2.195
R^2	15.82%		

Note: +p<0.1, *p<0.05, ** p<0.01, *** p<0.001

5.6. Discussion

Starting from a theory-based research framework, this study provides solid empirical evidence on the impact of ISO/IEC 27001 on the financial performance of certified companies. We developed a long-term event study on a dataset of 143 certified firms whose profitability, labour productivity, and sales performance were compared with those of a control set (7.30 firms on average) of non-certified organizations. Possible affecting factors were identified in the literature and tested through an OLS approach.

Regarding RQ1, the common understanding of IS is that of a purely defensive/preventive investment, whose value is mainly related to the ability to avoid potential future damage (Mirtsch *et al*., 2021b; Deane *et al*., 2019; Radanliev *et al*., 2018). In this sense, the ISO/IEC 27001 might not bear direct financial benefits, being these effects somehow related to the probability of an IS issue to occur. Moreover, previous studies also indicated that the formalization required by the norm might create excessive bureaucracy and a potential loss of flexibility, ultimately impacting the bottom line of certified firms (e.g., Annarelli *et al*., 2020; van Wessel *et al*., 2011). Our findings show that the benefits of ISO/IEC 27001 outweigh these potential drawbacks. Through the analysis of large-scale empirical evidence, we show in fact that there is a significant positive relationship between the certification, profitability (H1) and labour productivity (H2). By comparing these outcomes with the results for the most widespread international management standards (i.e., ISO 9001, ISO 14001, OHSAS 18001), both similarities and differences emerge. In line with ISO 9001 and OHSAS 18001 (e.g., Corbett *et al*., 2005; Lo *et al*., 2014), but in contrast with ISO 14001 (Wang and Zhao, 2020), our analysis indicates that ISO/IEC 27001 is related to improvements in the financial performance for certified firms (H1 and H2). However, while for ISO 9001 and OHSAS 18001 the positive effects on labour productivity are almost immediate (Corbett *et al*., 2005; Lo *et al*., 2014), in the case of ISO/IEC 27001 abnormal performance changes appear only after some years after the certification.

Consistently with the HRT perspective, our results can be explained by the ISO/IEC 27001 enabling a clearer definition of roles and responsibilities as well as raising employees' awareness and capabilities. By the same token, from the RBV standpoint, this is also related to the adoption of a process-based approach underpinned by a continuous improvement logic. In fact, ISO/IEC 27001 requirements support firms in reducing managerial uncertainty related to complex interactions, like those implied by information-related processes. The impact of this – in a business environment characterized by an increasing relevance of data – spans well beyond the boundaries of IT departments for at least three reasons. First, regular audits and meetings help organizations review and redefine their organizational practices and enhance the use of budget, resources, and personnel (Crowder, 2013). Second, the standard allows companies in selecting among the various technological solutions for information management currently available (Leszczyna, 2019). Third, the presence of the certification makes individual

customers' on-site audits unnecessary with a consequent reduction of times for contracting (Kossyva *et al*., 2014).

As far as sales performance is concerned (H3), in contrast with ISO 14001 and OHSAS 18001 (De Jong *et al*., 2014; Lo *et al*., 2014) for which positive sales effects appeared only after the formal attainment of the certification, our evidence shows that ISO/IEC 27001 certified firms outperform the control ones mainly in the pre-certification period. As it takes on average between 6 and 18 months for companies to get certified (van Wessel *et al*., 2011), the motivation might be twofold. On the one hand, ISO/IEC 27001 could be a requirement placed by customers to initiate business relationships. On the other, potential benefits related to the streamlining of buyer-supplier relationships (Hannigan *et al*., 2019) could start before the formal certification. Drawing from ST (Connelly *et al*., 2011; Spence, 1978), the result can be explained in terms of the strength of the signal (King *et al*., 2005) as well as the relative importance of the kind of signal (Lansing *et al*., 2019). In particular, despite the diffusion of ISO/IEC 27001 is on a growing trajectory, the relevant number of issued certificates may have modified the role of the standard; from a source of competitive differentiation in the market to a prerequisite to conduct business.

As far as RQ2 is concerned, we were able to specify that ISO/IEC 27001 performance implications are affected by the degree of internationalization (H4). This result is consistent with the role of ISO/IEC 27001 as *lingua franca* for IS. Contrary to our initial assumptions, technological intensity plays no role in affecting ISO/IEC 27001 impact on performance (H5). This confirms the general applicability of the standard, regardless of the technological profile of the certified organization (ISO/IEC 27001: 2013). However, it is also important to acknowledge that more technologically advanced organizations might also resort to ISO/IEC 27001 as a baseline for IS, integrating other more specific standards and controls (e.g., Pardo *et al*., 2012).

CHAPTER 6. CONCLUDING REMARKS

6.1. Synopsis

Information Security is no longer an issue reserved for a technical audience only but has become de facto one of the major managerial challenges of the current decade (Corallo *et al*., 2022; Bower, 2020; Boyes *et al*., 2018). The challenges posed by the new technological developments as well as the acceleration of digital-first approaches have increased the need for a better understanding by corporate decision-makers (Hopkins, 2021; Boehm *et al*., 2020).

In this doctoral thesis, we aimed at achieving four main objectives: (1) to provide an overview of the main information security issues in the context of Industry 4.0; (2) to develop a systematic literature review on ISO/IEC 27001; (3) to shed light on the diffusion patterns of ISO/IEC 27001; and (4) to investigate the performance implications of ISO/IEC 27001 adoption.

As for the first point (Chapter 2), by discussing with ten senior information security professionals and executives, we outlined the reasons why information security is not a (purely) technical topic. Moreover, we also questioned the effectiveness of current frameworks and standards in facing current challenges and we lay out some emerging approaches to provide a guideline to specialists and managers with a non-information technology background.

Moving to the second point (Chapter 3), we analysed 96 contributions related to ISO/IEC 27001 composed of peer-reviewed journal articles, books, and book chapters. In terms of descriptive statistics, we highlighted their time distribution, methodology, focus of the empirical studies, publication outlet (disciplinary area), and author's affiliation (department and home institution). As for the content of the included contributions, five research foci have been identified (i.e., relationships between ISO/IEC 27001 and other standards/frameworks, motivations for the adoption, implementation path, outcomes of the adoption, and contextual factors). We outlined some critical points of extant research on the topic; a paucity of empirical studies on ISO/IEC 27001 and a limited debate addressing the topic from a managerial point of view. Against this background, we proposed a research agenda which provides both suggestions for further research at the single-firm level as well as some directions to move beyond organizational boundaries by considering a system-based perspective.

In Chapter 4, we resorted to Grey models to investigate the diffusion patterns of ISO/IEC 27001 certifications up to 2030 for the six countries with the highest number of adherents (i.e.,

Japan, UK, India, China, Germany, Italy). The findings show that a generalized growing trend is likely to be expected in the years to come and that China will lead as regards the number of issued certificates.

To conclude (Chapter 5), we developed a set of theory-grounded hypotheses on the impact of ISO/IEC 27001 on a firm's performance and tested them through a long-term event study complemented by an ordinary least squares regression on a dataset of 143 US-listed companies. The results indicate that ISO/IEC 27001 adoption is associated with improvements in profitability, labour productivity, and (partially) sales performance. The impact appears affected by the level of internationalization of the certified firm.

6.2. Contribution

6.2.1. Contribution to theory

This thesis contributes to the Operations Management and Quality Management literature in some significant ways.

First, Chapter 2 conceptualizes the main information security challenges in the context of Industry 4.0. In particular, it highlights that many of them should be addressed through managerial/organizational practices. This outlines the need for a step change in the academic research on information security; the main wisdom is that of a purely technical argument. The findings thus promote the development of a managerial debate on the topic.

Second, Chapter 3 provides an overview of the current knowledge on ISO/IEC 27001, highlighting emerging themes and open issues, thereby providing solid foundations for future research on the topic. Moreover, it explicitly indicates a set of research opportunities, considering ISO/IEC 27001 as part of a system of standards and practices and in the context of networks of business relations. Drawing from Seuring *et al*. (2021) indications, this chapter borrowed three theories related to social systems thinking to read the results of the analysis through new lenses. This enabled to problematize the assumption behind ISO/IEC 27001 research as a firm-level phenomenon; this way providing the springboard for interdisciplinary research on the matter, including quality, supply chain and operations and human resource management.

Third, Chapter 4, highlights the relevance that ISO/IEC 27001 is likely to have in the years to come; it shows that a rising trend in the number of adherents is likely to be expected in the future. This finding is particularly relevant considering the concerns posed by extant research

as regards the usefulness of this international management standard and the competition it might suffer from other general and context-specific standards. Furthermore, it contributes to the literature on management systems and voluntary standards, also enabling comparisons among them; the number of ISO/IEC 27001 issued certificates will approach that of more mature standards such as ISO 9001 and ISO 14001. The use of Grey models also shows an analytical methodology that, with the exception of Ikram *et al*. (2021, 2019), has been rarely employed to shed light on the diffusion of international management standards and which may apply to other voluntary standards as well.

To conclude, Chapter 5 highlights the relevance of proactive investments in IS and shows that structured approaches such as ISO/IEC 27001 pay off. This chapter points out that the value of the standard is not only related to the fulfillment of customer requests and/or to what can be communicated to external stakeholders, but resides also in significant implications for profitability and labour productivity. Overall, the findings of this chapter are especially relevant considering the inherent difficulties in assessing the impact of IS investments (Wang and Franke, 2020; Chai *et al*., 2011). Moreover, the findings contribute to the literature on management systems and voluntary standards shedding light on ISO/IEC 27001 performance implications, also enabling comparisons among them. Differences with other widespread international management system standards emerge as regards ISO/IEC 27001 impact on sales and labour productivity. In particular, the inherent complexity of dealing with information-related activities results in longer internalization times and therefore in lagged labour productivity-related effects. On the other hand, sales-related findings show that the attainment of ISO/IEC 27001 probably streamlines buyer-supplier relationships already during the certification process.

6.2.2. Contribution to practice

The study delivers some implications for policymakers and corporate managers.

Starting with Chapter 2, it emerges that it is not possible to protect companies from all possible cyberattacks: the real question is about risk prioritization and mitigation. Information security should become a cross-functional strategic platform where corporate leader involvement and cross-functional collaboration are essential. Moreover, the results show that information security could be a lever for value creation, yet companies find it difficult to communicate this value to business customers and to the consumer. Internally companies are

piloting new tools for assessing and communicating cyber risks to non-technical managers. Similar tools are needed for client engagement.

As for Chapter 3, the literature review provides a comprehensive overview of 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 these results to inform promotion and regulatory activities aimed at sustaining the diffusion of the standard.

Moving to Chapter 4, the findings assist companies in improving their awareness of the potential values of ISO/IEC 27001 and in taking more informed decisions as regards its potential adoption: findings can help firms to align their strategy with global requirements (which are increasingly oriented towards internationally recognized management standards – Granja *et al*., 2021) and to strengthen their business by planning, developing, and communicating practices related to information security. Moreover, the outcomes of the analyses could be also useful for the certification body itself (ISO) by highlighting the current dissemination status and by providing forecasts that can be used to understand how the ISO/IEC 27001 market will develop in the years to come, anticipate demands, refine medium-term strategic planning, guide promotional strategies, and understand eventual areas of improvement where to prioritize efforts. Policymakers may find the results relevant as well; in particular, to develop promotional and regulatory activities aimed at sustaining the diffusion of the standard.

To conclude (Chapter 5), as new technologies and investments in IS require cross-functional decision-making (Castelo-Branco *et al*., 2022; McKinsey, 2019), the results can help managers to overcome concerns as to the impact of IS management systems on flexibility and productivity. Moreover, although the standard might be initially introduced upon customers' requirements, it has far-reaching consequences on financial performance across multiple dimensions.

6.3. Limitations and future research

The results of this doctoral dissertation should be viewed in light of some main limitations.

First, the qualitative approach adopted in Chapter 2, is based on a reduced sample size (10 companies). Despite qualitative research doesn't have inferential aims (Stuart *et al*., 2002), it

should be acknowledged that the findings cannot be generalized to a wider population of companies. Further contributions could address such aspects by performing a survey on wider and more structured samples.

Second, the systematic literature review presented in Chapter 2 summarizes the academic body of knowledge on ISO/IEC 27001 up to November 2020. Since then, the research has made some progress widening the understanding of ISO/IEC 27001. In addition, although the decision to exclude conference papers vouched for the quality and the rigor of the included contributions, the most recent development of the topic may not have been taken into account.

Third, as for Chapter 4, only a small number of countries exhibiting a high number of issued certificates have been considered. Future studies could extend our findings to different settings (e.g., regions, countries, industries); specific diffusion patterns might appear depending on institutional and legal factors, the relevance of IT/IS for the considered context, and the existence of alternative standards/approaches. Moreover, despite Grey models (1,1) provide robust and reliable results both in terms of explaining past trends and predicting the future diffusion of ISO/IEC 27001, this forecasting technique can only take into account endogenous factors of growth and does not consider the effects of exogenous factors such as those related to the global economic situation, enactment of incentives aimed at fostering the adoption of ISO/IEC 27001, and modifications in the dictates underpinning this certification scheme. Should these variations occur, it would be advisable to repeat the analyses. This would allow, on the one hand, to obtain updated forecasts; on the other, to understand the specific effect of the discontinuity on the diffusion trends of ISO/IEC 27001. Further research could also resort to Grey models to shed light on the joint adoption of multiple management standards (e.g., ISO 9001 and ISO 14001; ISO 9001 and ISO/IEC 27001; ISO 9001, ISO 14001, and ISO/IEC 27001). Moreover, in light of the managerial challenges posed by information security, further studies could investigate the diffusion patterns of other management standards aimed at helping firms to cope with the risks posed by new technologies (e.g., ISO 27700).

Moving to Chapter 5, as the performance implications of the ISO/IEC 27001 adoption have been evaluated through secondary data, it has been possible to analyse only financial dimensions and not the direct effects of ISO/IEC 27001 on the IS levels of certified firms. This issue is, however, difficult to overcome as the bulk of research on IS highlights the lack of external sources and companies' reluctance to disclose vulnerabilities and security breaches (Kotulic and Clark, 2004). Moreover, by including only publicly US-listed companies, it has

been possible to analyse reliable and comparable information about their financial statements. This choice, however, restricts the generalizability of the results. The implications for sales performance can be particularly affected by different geographical settings considering regulatory initiatives supporting the standard diffusion (Culot *et al*., 2021; Gillies, 2011). There are opportunities for future research to overcome these limitations, e.g., with a cross-country study, with specific deep dives on private companies, extending the timeframe of the analysis. Surveys can also support a better understanding of the direct impact of ISO/IEC 27001 on IS and the relationship between the motivations for certification, internalization of the practices, and performance. In addition, as recent technological developments trigger new ways of sharing data with business partners (Romero and Vernadat, 2016; Porter and Heppelmann, 2015, 2014) – researchers might be interested in exploring IS no longer at the firm level but considering the network structures (e.g., customers, suppliers) in which individual organizations are embedded in.

To conclude, we hope that by showing the increasing central role that ISO/IEC 27001 is likely to assume in the years to come as well as the significant implications it might have for firms' performance our study will lead more scholars to consider this certification scheme; for instance, by investigating how the motivations for the adoption, the implementation challenges, and the effectiveness differ when considering different contexts and by shedding light on the role of some country-specific factors (e.g., culture, trade relations, development level) in influencing/explaining national differences in the number of ISO/IEC 27001 issued certificates (e.g., Abdelzaher *et al*., 2019).

References

Abdelzaher, D., Fernandez, W. D., and Schneper, W. D. (2019). Legal rights, national culture and social networks: Exploring the uneven adoption of United Nations Global Compact. *International Business Review*, Vol. 28 No. 1, pp. 12-24.

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

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.

Akram, T. (2019). The Japanese economy: Stagnation, recovery, and challenges. *Journal of Economic Issues*, Vol. 53 No. 2, pp. 403-410.

Al-Karaki, J. N., Gawanmeh, A., and El-Yassami, S. (2022). GoSafe: on the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University-Computer and Information Sciences*, Vol. 34 No. 6, pp. 3079-3095.

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

Allison, P. D. (1998). *Multiple regression: A primer*. Pine Forge Press, New York.

Almeida, L., and Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, Vol. 27 No. sup1, pp. 173-180.

Ancarani, A., and Di Mauro, C. (2018). Reshoring and Industry 4.0: how often do they go together?. *IEEE Engineering Management Review*, Vol. 46 No. 2, pp. 87-96.

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

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

Ardito, L., Petruzzelli, A. M., 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, Ş. D., Vintilă, G., and Gherghina, Ş. C. (2017). A cross-country empirical study towards the impact of following ISO management system standards on Euro-area economic confidence. *Amfiteatru Economic Journal*, 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 & 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. 1, 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 & 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 & 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.

Barber, B. M., and Lyon, J. D. (1996). Detecting abnormal operating performance: The empirical power and specification of test statistics. *Journal of Financial Economics*, Vol. 41 No. 3, pp. 359-399.

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.

BCG (2017). Report from Davos: Board oversight of cyberresilience. Retrieved from: https://www.bcg.com/it-it/publications/2017/technology-digital-report-davos-board-oversight-cyberresilience.aspx [Accessed on: 06/10/2019].

BCG (2019). Are you spending enough on cybersecurity?. Retrieved from: https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity.aspx [Accessed on: 06/10/2019].

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, 36.

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. (2020). Using machine learning to assist with the selection of security controls during security assessment. *Empirical Software Engineering*, Vol. 25 No. 4, pp. 2550-2582.

Bititci, U., Garengo, P., Dörfler, V., and Nudurupati, S. (2012). Performance measurement: challenges 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*. Retrieved from: 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 on: 20/04/2020].

Boehm, J., Kaplan, J., Sorel, M., Sportsman, N., and Steen, T. (2020). Cybersecurity tactics for the coronavirus pandemic, *McKinsey Quarterly*. Retrieved from: 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 on: 12/04/2022].

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. In*ternational Journal of Management Reviews*, Vol. 20 No. 2, pp. 411-432.

Boulding, K. E. (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 & Interfaces*, Vol. 62, pp. 98-118.

Bower, T. (2020), Boost Your Resistance to Phishing Attacks. *Harvard Business Review*, Vol. 98 No. 5, pp. 17-21.

Boyes, H., Hallaq, B., Cunningham, J., and Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, Vol. 101, pp. 1-12.

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*. Retrieved from: https://hbr.org/2019/03/cybersecurity-is-putting-customer-trust-at-the-center-of-competition [Accessed on: 07/01/2022].

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.

Cabecinhas, M., Domingues, P., Sampaio, P., and Arezes, P. (2020). Diffusion, drivers and trends on integrated management systems evolution among Portuguese companies. *International Journal of Occupational and Environmental Safety*, Vol. 4 No. 1, pp. 15-36.

Cabecinhas, M., Domingues, P., Sampaio, P., Bernardo, M., Franceschini, F., Galetto, M., Gianni, M., Gotzamani, K., Mastrogiacomo, L. and Hernandez-Vivanco, A. (2018), Integrated management systems diffusion models in South European countries. *International Journal of Quality & Reliability Management*, Vol. 35 No. 10, pp. 2289-2303.

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. 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. 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. Calder, A. (Eds.), *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. 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. 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. 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.

Cantu, J., Tolk, J., Fritts, S., and Gharehyakheh, A. (2020). High Reliability Organization (HRO) systematic literature review: Discovery of culture as a foundational hallmark. *Journal of Contingencies and Crisis Management*, Vol. 28 No. 4, pp. 399-410.

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

Casadesús, M., Marimon, F., and Heras-Saizarbitoria, I. (2008). ISO 14001 diffusion after the success of the ISO 9001 model. *Journal of Cleaner Production*, Vol. 16 No. 16, pp. 1741-1754.

Castelo-Branco, I., Oliveira, T., Simões-Coelho, P., Portugal, J., and Filipe, I. (2022). Measuring the fourth industrial revolution through the Industry 4.0 lens: The relevance of resources, capabilities and the value chain. *Computers in Industry*, Vol. 138, 103639.

Castka P., and Corbett C.J. (2015). Management Systems Standards: Diffusion, Impact and Governance of ISO 9000, ISO 14000, and Other Standards. *Foundations and Trends in Technology and Operations Management*, Vol. 7 No. 3–4, pp. 161-379.

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.

Chai, S., Kim, M., and Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, Vol. 50 No. 4, pp. 651-661.

Chakrabarty, S., and Wang, L. (2012). The long-term sustenance of sustainability practices in MNCs: A dynamic capabilities perspective of the role of R&D and internationalization. *Journal of Business Ethics*, Vol. 110 No. 2, pp. 205-217.

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.

Connelly, B. L., Certo, S. T., Ireland, R. D., and Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, Vol. 37 No. 1, pp. 39-67.

Contieri, P. G. S., Anholon, R., and De Santa-Eulalia, L. A. (2022). Industry 4.0 enabling technologies in manufacturing: Implementation priorities and difficulties in an emerging country. *Technology Analysis & Strategic Management*, Vol. 34 No. 5, pp. 489-503.

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.

Corallo, A., Lazoi, M., Lezzi, M., and Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, Vol. 137, 103614.

Corbett, C. J., and Kirsch, D. A. (2001). International diffusion of ISO 14000 certification. *Production and Operations Management*, Vol. 10 No. 3, pp. 327-342.

Corbett, C.J., Montes-Sancho, M.J., and Kirsch, D.A. (2005). The financial impact of ISO 9000 certification. *Management Science*, Vol. 51 No. 7, pp. 1046-1059.

Cots, S., and Casadesús, M. (2015). Exploring the service management standard ISO 20000. Total Quality Management & Business Excellence, Vol. 26 No. 5-6, pp. 515-533.

Cowan, D. (2011). External pressure for internal information security controls. *Computer Fraud & 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., Nassimbeni, G., Podrecca, M., and Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, Vol. 33 No. 7, pp. 76-105.

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.

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.

Dahlin, G., and Isaksson, R. (2017). Integrated management systems–interpretations, results, opportunities. *The TQM Journal*, Vol. 29 No. 3, pp. 528-542.

Dang, H. S., Nguyen, T. M. T., Wang, C. N., Day, J. D., and Dang, T. M. H. (2020). Grey system theory in the study of medical tourism industry and its economic impact. *International Journal of Environmental Research and Public Health*, Vol. 17 No. 3, 961.

Dang, Y., Liu, S. and Liu, B. (2005), The GM models that x(n) be taken as initial value, *Chinese Journal of Management Science*, Vol. 13 No. 1, pp. 132-134.

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

De Jong, P., Paulraj, A., and Blome, C. (2014). The financial impact of ISO 14001 certification: top-line, bottom-line, or both?. *Journal of Business Ethics*, Vol. 119 No. 1, pp. 131-149.

De Zoysa, A., Takaoka, N., and Zhang, Y. (2021). Impact of corporate social responsibility (CSR) awareness, affordability and management system sophistication on CSR performance. *Industrial Management & Data Systems*, Vol. 121 No. 7, pp. 1704-1722.

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.

del Mar Alonso-Almeida, M., Marimon, F., Casani, F., and Rodriguez-Pomeda, J. (2015). Diffusion of sustainability reporting in universities: current situation and future perspectives. *Journal of Cleaner Production*, Vol. 106, pp. 144-154.

del Mar Alonso-Almeida, M., Llach, J., and Marimon, F. (2014). A closer look at the 'Global Reporting Initiative'sustainability reporting as a tool to implement environmental and social policies: A worldwide sector analysis. *Corporate Social Responsibility and Environmental Management*, Vol. 21 No. 6, pp. 318-335.

del Mar Alonso-Almeida, M., Marimon, F., and Bernardo, M. (2013). Diffusion of quality standards in the hospitality sector. *International Journal of Operations & Production Management*, Vol. 33 No. 5, pp. 504-527.

Delmas, M., and Montiel, I. (2009). Greening the supply chain: when is customer pressure effective?. *Journal of Economics & Management Strategy*, Vol. 18 No. 1, pp. 171-201.

Deloitte (2020). COVID-19's Impact on Cybersecurity. Retrieved from: https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html [Accessed on: 21/05/2020].

Deng, J. (2004). On IAGO Operator, *Journal of Grey System*, Vol. 16 No. 3, pp. 242-272.

Dhillon, G., Syed, R., and de Sá-Soares, F. (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/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. *Information & 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 No. 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. Khosrow-Pour M. (Ed.), *Standards and Standardization: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, pp. 994-1017.

Donaldson, L. (2001). *The contingency theory of organizations*. Sage, New York.

Dong, Y., Skowronski, K., Song, S., Venkataraman, S., and Zou, F. (2020). Supply base innovation and firm financial performance. *Journal of Operations Management*, Vol. 66 No. 7-8, pp. 768-796.

Dos Santos Ferreira, R., Frogeri, R. F., Coelho, A., and Piurcosky, F. (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, e2018005

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.

ENISA - European Union Agency for Network and Information Security (2018). Good Practices for Security of Internet of Things in the context of Smart Manufacturing. Retrieved from: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot [Accessed on:06/10/2019].

Erkonen, S. (2008). ISO Standards Draft Content. Tipton, H. F. and Krause, M. (Eds.), *Information Security Management Handbook*, Auerbach Publications, Boca Raton, pp. 265-272

Ernst & Young. (2008). Global Information Security Survey: Moving Beyond Compliance. Retrieved from: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/2008_E&YWhitePaper_GlobalInfoSecuritySurvey.pdf [Accessed on: Dec. 19, 2019].

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

Faraj, S., and Xiao, Y. (2006). Coordination in fast-response organizations. *Management Science*, Vol. 52 No. 8, pp. 1155-1169.

Faruq, B. A., Herlianto, H. R., Simbolon, S. P. H., Utama, D. N., and Wibowo, A. (2020). Integration of ITIL V3, ISO 20000 & 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., Chen, 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.

Franceschini, F., Galetto, M., and Cecconi, P. (2006). A worldwide analysis of ISO 9000 standard diffusion: Considerations and future development. *Benchmarking: An International Journal*, Vol.13 No.4, pp.523-541.

Franceschini, F., Galetto, M., and Gianni, G. (2004). A new forecasting model for the diffusion of ISO 9000 standard certifications in European countries. *International Journal of Quality & Reliability Management*, Vol. 21 No. 1, pp. 32-50.

Franceschini, F., Galetto, M., Maisano, D. A., and Mastrogiacomo, L. (2011). ISO/TS 16949: analysis of the diffusion and current trends. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, Vol. 225 No. 5, pp. 735-745.

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

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

Fuentes, C., Lizarzaburu, E. R., and Vivanco, E. (2011). Norms and International Standards related to reduce risk management: a literature review. *Risk governance & control: Financial Markets & 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 No. 3-4, pp. 228-238.

Gartner (2018). Cybersecurity and digital risk management: CIOs Must engage and prepare, *Gartner Research*. Retrieved from: https://www.gartner.com/en/doc/3846477-cybersecurity-and-digital-risk-management-cios-must-engage-and-prepare [Accessed on: 02/05/2020]

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.

Goulard, S. (2020). The impact of the US–China trade war on the European Union. *Global Journal of Emerging Market Economies*, Vol. 12 No. 1, pp. 56-68.

Granja, N., Domingues, P., Cabecinhas, M., Zimon, D., and Sampaio, P. (2021). ISO 22000 certification: Diffusion in Europe. *Resources*, Vol. 10 No. 10, 100.

Greitzer, F. L., Purl, J., Leong, Y. M., and Sticha, P. J. (2019). Positioning your organization to respond to insider threats. *IEEE Engineering Management Review*, Vol. 47 No. 2, pp. 75-83.

Guler, I., Guillén, M. F., and Macpherson, J. M. (2002). Global competition, institutions, and the diffusion of organizational practices: The international spread of ISO 9000 quality certificates. *Administrative Science Quarterly*, Vol. 47 No. 2, pp. 207-232.

Gurbaxani, V. (1990). Diffusion in computing networks: The case of BITNET. *Communications of the ACM*, Vol. 33 No. 12, pp. 65-75.

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*. Retrieved from: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 [Accessed on: 21/05/2020].

Hendricks, K. B., Singhal, V. R., and Stratman, J. K. (2007). The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations. *Journal of Operations Management*, Vol. 25 No. 1, pp. 65-82.

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 Trillig, 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/Journal of Maritime Studies*, 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 & 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.

Hopkins, J. L. (2021). An investigation into emerging industry 4.0 technologies as drivers of supply chain innovation in Australia. *Computers in Industry*, Vol. 125, 103323.

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 & Business Excellence*, Vol. 26 No. 5-6, pp. 690-702.

Hsu, C., Wang, T., and Lu, A. (2016). The impact of ISO 27001 certification on firm performance. *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii.

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: How machine intelligence changes the rules of business, *Harvard Business Review*, Vol. 98, pp. 60-67.

Ikram, M., Mahmoudi, A., Shah, S. Z. A., and Mohsin, M. (2019). Forecasting number of ISO 14001 certifications of selected countries: Application of even GM (1, 1), DGM, and NDGM models. *Environmental Science and Pollution Research*, Vol. 26 No. 12, pp. 12505-12521.

Ikram, M., Zhang, Q., and Sroufe, R. (2021). Future of quality management system (ISO 9001) certification: novel grey forecasting approach. *Total Quality Management & Business Excellence*, Vol. 32 No. 15-16, pp. 1666-1693.

ISO (2019). The ISO Survey of Management System Standard Certifications 2018. Retrieved from: https://www.iso.org/the-iso-survey.html [Accessed on: 12/01/2020].

ISO (2021). *The ISO survey of management system standard certifications 2020*. Retrieved from: https://www.iso.org/the-iso-survey.html [Accessed on: 12/04/2022].

ISO (2021). *The ISO survey of management system standard certifications 2021*. Retrieved from: https://www.iso.org/the-iso-survey.html [Accessed on: 09/11/2022].

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 & 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.

Jacobs, B. W., Swink, M., and Linderman, K. (2015). Performance effects of early and late Six Sigma adoptions. *Journal of Operations Management*, Vol. 36, pp. 244-257.

Javed, S. A., and Liu, S. (2018). Predicting the research output/growth of selected countries: application of Even GM (1, 1) and NDGM models. *Scientometrics*, Vol. 115 No. 1, pp. 395-413.

Javed, S. A., Zhu, B., and Liu, S. (2020). Forecast of biofuel production and consumption in top CO2 emitting countries using a novel grey model. *Journal of Cleaner Production*, Vol. 276, 123997.

Jbair, M., Ahmad, B., Maple, C., and Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, Vol. 137, 103611.

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.

Ji, P., Huang, W., and Hu, X. (2001). Study on the characteristic of grey prediction model. *Systems Engineering Theory & Practice*, Vol. 21 No. 9, pp. 105-109.

Jie, C., and Bo, Z. (2012). Study on parameters characteristics of NGM (1, 1, k) prediction model with multiplication transformation. *Grey Systems: Theory and Application*, Vol. 2 No. 1, pp. 24-35.

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

Katz, D. and Kahn, R.L. (1978). *The Social Psychology of Organizations*. John Wiley & Sons, 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.

Kile, C. O., and Phillips, M. E. (2009). Using industry classification codes to sample high-technology firms: Analysis and recommendations. *Journal of Accounting, Auditing & Finance*, Vol. 24 No. 1, pp. 35-58.

King, A. A., Lenox, M. J., and Terlaak, A. (2005). The strategic use of decentralized institutions: Exploring certification with the ISO 14001 management standard. *Academy of Management Journal*, Vol. 48 No. 6, pp. 1091-1106.

Koohang, A., Anderson, J., Nord, J. H., and Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, Vol. 120 No. 1, pp. 231-247.

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.

Kotulic, A. G., and Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, Vol. 41 No. 5, pp. 597-607.

Ku, C. Y., Chang, Y. W., 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.

La Porte, T. R. (1996). High reliability organizations: Unlikely, demanding and at risk. *Journal of Contingencies and Crisis Management*, Vol. 4 No. 2, pp. 60-71.

Lansing, J., Siegfried, N., Sunyaev, A., and Benlian, A. (2019). Strategic signaling through cloud service certifications: Comparing the relative importance of certifications' assurances to companies and consumers. *The Journal of Strategic Information Systems*, Vol. 28 No. 4, 101579.

Legowo, N., and Juhartoyo, Y. (2022). Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001, *Journal of System and Management Sciences*, Vol. 12 No. 3, pp. 181-199.

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

Levine, D. I., and Toffel, M. W. (2010). Quality management and job quality: How the ISO 9001 standard for quality management systems affects employees and employers. *Management Science*, Vol. 56 No. 6, pp. 978-996.

Lewis, C. (1982). *International and Business Forecasting Methods.* Butterworths, London.

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.

Li, B., Zhang, S., Li, W., and Zhang, Y. (2022). Application progress of Grey model technology in agricultural science. *Grey Systems: Theory and Application*. https://doi.org/10.1108/GS-05-2022-0045

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.

Liu, F., Rhim, H., Park, K., Xu, J., and Lo, C. K. (2021). HACCP certification in food industry: Trade-offs in product safety and firm performance. *International Journal of Production Economics*, Vol. 231, 107838.

Liu, S., Yang, Y., and Forrest, J. (2017). *Grey data analysis*. Springer, Berlin.

Liu, S., Yang, Y., Xie, N., and Forrest, J. (2016). New progress of grey system theory in the new millennium. *Grey Systems: Theory and Application*, Vol. 6 No. 1, pp. 2-31.

Liu, S., Zeng, B., Liu, J., Xie, N., and Yang, Y. (2015). Four basic models of GM (1, 1) and their suitable sequences. *Grey Systems: Theory and Application*, Vol. 5 No. 2, pp. 141-156.

Llach, J., Marimon, F., and Bernardo, M. (2011). ISO 9001 diffusion analysis according to activity sectors. *Industrial Management & Data Systems*, Vol. 111 No. 2, pp. 298-316.

Llach, J., Marimon, F., and del Mar Alonso-Almeida, M. (2015). Social Accountability 8000 standard certification: analysis of worldwide diffusion. *Journal of Cleaner Production*, Vol. 93, pp. 288-298.

Lo, C. K., Pagell, M., Fan, D., Wiengarten, F., and Yeung, A. C. (2014). OHSAS 18001 certification and operating performance: The role of complexity and coupling. *Journal of Operations Management*, Vol. 32 No. 5, pp. 268-280.

Lo, C. K., Wiengarten, F., Humphreys, P., Yeung, A. C., and Cheng, T. C. E. (2013). The impact of contextual factors on the efficacy of ISO 9000 adoption. *Journal of Operations Management*, Vol. 31 No. 5, pp. 229-235.

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 & Management*, Vol. 4 No. 2, pp. 1-8.

Lowry, P. B., Dinev, T., and Willison, 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.

Ma, X., Wu, W., Zeng, B., Wang, Y., and Wu, X. (2020). The conformable fractional grey system model. *ISA transactions*, Vol. 96, pp. 255-271.

Maganga, D. P., and Taifa, I. W. (2022). Quality 4.0 conceptualisation: an emerging quality management concept for manufacturing industries. *The TQM Journal*. https://doi.org/10.1108/TQM-11-2021-0328

Majernik, 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.

Malik, M., and Abdallah, S. (2020). The relationship between organizational attitude and lean practices: an organizational sense-making perspective. *Industrial Management & Data Systems*, Vol. 120 No. 9, pp. 1715-1731.

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

Marimon, F., Casadesús, M., and Heras-Saizarbitoria, I. (2006). ISO 9000 and ISO 14000 standards: an international diffusion model. *International Journal of Operations & Production Management*, Vol. 26 No. 2, pp. 141-165.

Marimon, F., Casadesús, M., and Heras-Saizarbitoria, I. (2010). Certification intensity level of the leading nations in ISO 9000 and ISO 14000 standards, *International Journal of Quality & Reliability Management*, Vol. 27 No. 9, pp. 1002-1020.

Marimon, F., del Mar Alonso-Almeida, M., del Pilar Rodríguez, M., and Alejandro, K. A. C. (2012). The worldwide diffusion of the global reporting initiative: what is the point?. *Journal of Cleaner Production*, Vol. 33, pp. 132-144.

Marimon, F., Heras, I., and Casadesús, M. (2009). ISO 9000 and ISO 14000 standards: a projection model for the decline phase. *Total Quality Management*, Vol. 20 No. 1, pp. 1-21.

Marimon, F., Llach, J., and Bernardo, M. (2011). Comparative analysis of diffusion of the ISO 14001 standard by sector of activity. *Journal of Cleaner Production*, Vol. 19 No. 15, pp. 1734-1744.

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.

Mastrogiacomo, L., Carrozza, A., Maisano, D. A., and Franceschini, F. (2021). Is 'post-decline'the next phase of the diffusion of ISO 9001 certifications? New empirical evidence

from European countries. *Total Quality Management & Business Excellence*, Vol. 32 No. 11-12, pp. 1384-1403.

Mayring, P. (2000). Quantitative Content Analysis, *Forum: qualitative social research*, Vol. 1 No. 2, pp. 1-10.

McKinsey (2019). Perspectives on transforming cybersecurity. Retrieved from: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx [Accessed on: 17/12/2021].

McWilliams, A., and Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *Academy of Management Journal*, Vol. 40 No. 3, pp. 626-657.

Mele, C., Pels, J., and Polese, F. (2010). A brief review of systems theories and their managerial applications. *Service Science*, Vol. 2 No. 1-2, pp. 126-135.

Mercedes (2021). Special Terms. Retrieved from: https://docmaster.supplier.daimler.com/DMPublic/en/doc/ALD00000454.2019-11.EN.4.pdf [Accessed on: 22/12/2021].

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. 06, 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., Blind, K., Koch, C., and Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security*, Vol. 109, 102383.

Mirtsch, M., Kinne, J., and Blind, K. (2020). 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 & Computer Security, *Information Management & 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 & Applied Information Technology*, Vol. 70 No. 2, pp. 316-323.

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

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

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.

Nair, A., and Prajogo, D. (2009). Internalisation 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.

Ofosu-Adarkwa, J., Xie, N., and Javed, S. A. (2020). Forecasting CO2 emissions of China's cement industry using a hybrid Verhulst-GM (1, N) model and emissions' technical conversion. *Renewable and Sustainable Energy Reviews*, Vol. 130, 109945.

Orzes, G., Jia, F., Sartor, M., and Nassimbeni, G. (2017). Performance implications of SA8000 certification. *International Journal of Operations & Production Management*, Vol. 37 No. 11, pp. 1625-1653.

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.

Orzes, G., Moretto, A. M., Moro, M., Rossi, M., Sartor, M., Caniato, F., and Nassimbeni, G. (2020). The impact of the United Nations global compact on firm performance: A longitudinal analysis. *International Journal of Production Economics*, Vol. 227, 107664.

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., 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.

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

Park, C., Jang, S., and Park, Y. (2010). A study of effect of Information Security Management System [ISMS] certification on organization performance. *IJCSNS International Journal of Computer Science and Network Security*, 10(3), 10-21.

Park, C., Jang, S., and Park, Y. (2010). A study of effect of Information Security Management System [ISMS] certification on organization performance. *International Journal of Computer Science and Network Security*, Vol. 10 No. 3, pp. 10-21.

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

Pearl, R. (1978). *The Biology of Population Growth*. Ayer Publishing, New York.

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

Podrecca, M., Orzes, G., Sartor, M., and Nassimbeni, G. (2021). The impact of abandoning social responsibility certifications: Evidence from the decertification of SA8000 standard. *International Journal of Operations & Production Management*, Vol. 41 No. 13, pp. 100-126.

Podrecca, M., Sartor, M., and Nassimbeni, G. (2022a). United Nations Global Compact: where are we going?. *Social Responsibility Journal*, Vol. 18 No. 5, pp. 984-1003.

Podrecca, M., Culot, G., Nassimbeni, G., and Sartor, M. (2022b). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, Vol. 142, 103744.

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

Porter, M. E., and Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, Vol. 92 No. 11, pp. 64-88.

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. 351-376.

Prajogo, D. I. (2011). The roles of firms' motives in affecting the outcomes of ISO 9000 adoption. *International Journal of Operations & Production Management*, Vol. 31 No. 1, pp. 78-100.

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: An International Journal*, Vol. 17 No. 3, pp. 306-322.

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

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, Vol. 102, 14-22.

Rauniyar, K., Wu, X., Gupta, S., Modgil, S., and de Sousa Jabbour, A. B. L. (2022). Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology. *Industrial Management & Data Systems*. https://doi.org/10.1108/IMDS-04-2021-0235

Rebelo, M. F., Santos, G., and Silva, R. (2014). A generic model for integration of quality, environment and safety management systems. *The TQM Journal*, Vol. 26 No. 2, pp. 143-159.

Rendon-Benavides, R., Perez-Franco, R., Elphick-Darling, R., Plà-Aragonés, L. M., Aleu, F. G., Verduzco-Garza, T., and Rodriguez-Parral, A. V. (2022). In-transit interventions using

real-time data in Australian berry supply chains. *The TQM Journal*. https://doi.org/10.1108/TQM-11-2021-0319

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 Computer Applications*, Vol. 18 No. 8, pp. 4-8.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science*, Vol. 1 No. 2, pp. 160-176.

Rogers, E. M. (2002). Diffusion of preventive innovations. *Addictive Behaviors*, Vol. 27 No. 6, pp. 989-993.

Rogers, E.M (1988). Breakthrough: Emerging New Thinking. *Diffusion of the idea of beyond war*. Walker, New York.

Romero, D., and Vernadat, F. (2016). Enterprise information systems state of the art: Past, present and future trends. *Computers in Industry*, Vol. 79, pp. 3-13.

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. *Academy of Management Annals*, Vol. 2 No. 1, pp. 475-515.

Ruiza, L. C., Amado, M. L., Carrasco, J. R., and Andrade-Arenasa, L. (2022). Implementation of Information Security Audit for the Sales System in a Peruvian Company, *International Journal on Advanced Science Engineering and Information Technology*, Vol. 12 No. 3, pp. 1189-1195.

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

Sampaio, P., Saraiva, P., and Domingues, P. (2012). Management systems: integration or addition?. *International Journal of Quality & Reliability Management*, Vol. 29 No. 4, pp. 402-424.

Sampaio, P., Saraiva, P., and Guimarães Rodrigues, A. (2009). An analysis of ISO 9000 data in the world and the European Union. *Total Quality Management*, Vol. 20 No. 12, pp. 1303-1320.

Sanders, G. L., Upadhyaya, S., and Wang, X. (2019). Inside the insider. *IEEE Engineering Management Review*, Vol. 47 No. 2, pp. 84-91.

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.

Sawyerr, E., and Harrison, C. (2019). Developing resilient supply chains: lessons from high-reliability organisations. *Supply Chain Management: An International Journal*, Vol. 25 No. 1, pp. 77-100.

Schleicher, D. J., Baumann, H. M., Sullivan, D. W., Levy, P. E., Hargrove, D. C., and Barros-Rivera, 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. 182-208.

Schoenherr, T., and Talluri, S. (2012). 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., da Silva, M. M., and Bianchi, I. S. (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: An International Journal*, Vol. 17 No. 5, pp. 544-555.

Seuring, S., Yawar, S. A., Land, A., Khalid, R. U., and Sauer, P. C. (2021). The application of theory in literature reviews–illustrated with examples from supply chain management. *International Journal of Operations & Production Management*, Vol. 41 No. 1, pp. 1-20.

Shackelford, S. J. (2016). Business and cyber peace: We need you!. *Business Horizons*, Vol. 59 No. 5, pp. 539-548.

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 No. 3, 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*. Retrieved from: www.wsj.com/amp/articles/coronavirus-upheaval-triggers-corporate-search-for-supply-chain-technology-11588189553 [20/04/2020].

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.

Sony, M., and Naik, S. S. (2019). Ten lessons for managers while implementing Industry 4.0. *IEEE Engineering Management Review*, Vol. 47 No. 2, pp. 45-52.

Sony, M., Antony, J., and McDermott, O. (2022). The impact of medical cyber–physical systems on healthcare service delivery. *The TQM Journal*, Vol. 34 No. 7, pp. 73-94.

Spence M. (1973). Job Market Signaling, *The Quarterly Journal of Economics*, Vol. 87 No. 3, pp. 355-374.

Spence, M. (1978). Job market signaling. Diamond, P. and Rothschild, M. (Eds.), *Uncertainty in economics*. Academic Press, Cambridge, pp. 281-306).

Spiekermann, S., and Korunovska, J. (2017). Towards a value theory for 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 & 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 (Ed.), *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, pp. 216-238

Su, H. C., Dhanorkar, S., and Linderman, K. (2015). A competitive advantage from the implementation timing of ISO management standards. *Journal of Operations Management*, Vol. 37, pp. 31-44.

Susanto, H., Almunawar, M. N., 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.

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.

Stuart, I., McCutcheon, D., Handfield, R., McLachlin, R., and Samson, D. (2002). Effective case research in operations management: a process perspective, *Journal of Operations Management*, Vol. 20 No. 5, pp. 419-433.

Swink, M., and Jacobs, B. W. (2012). Six Sigma adoption: Operating performance impacts and contextual drivers of success. *Journal of Operations Management*, Vol. 30 No. 6, pp. 437-453.

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., and Shoraka, 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 No. 5-6, pp. 324-343.

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 & Organization*, Vol. 60 No. 4, pp. 579-602.

The Economist (2020). The changes covid-19 is forcing on to business, *The Economist*. Retrieved from: https://www.economist.com/briefing/2020/04/11/the-changes-covid-19-is-forcing-on-to-business [Accessed on: 20/05/2020].

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 & 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.

Treacy, R., Humphreys, P., McIvor, R., and Lo, C. (2019). ISO14001 certification and operating performance: A practice-based view. *International Journal of Production Economics*, Vol. 208, pp. 319-328.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., and Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & 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.

Tuptuk, N., and Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, Vol. 47, pp. 93-106.

Uzumeri, M. V. (1997). ISO 9000 and other metastandards: principles for management practice?. *Academy of Management Perspectives*, 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 & 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 across cultures. *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 realities. *Journal of Information Technology*, Vol. 27 No. 3, pp. 179-197.

Villarreal, A.B. (2019). Keeping an eye on what matters for the economy. Retrieved from: https://www. iso.org/news/ref2428.htm [Accessed on: 10/04/2022].

Vogus, T.J., and Welbourne, T.M. (2003). Structuring for high reliability: HR practices and mindful processes in reliability-seeking organizations. *Journal of Organizational Behavior*, Vol. 24 No. 7, pp. 877-903.

Von Bertalanffy, L. (1956). General System Theory. 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 & Computer Security*, Vol. 7 No. 1, pp. 50-58.

Wang, D. (2018). Building value in a world of technological change: Data analytics and industry 4.0. *IEEE Engineering Management Review*, Vol. 46 No. 1, pp. 32-33.

Wang, J. X., and Zhao, M. Z. (2020). Economic impacts of ISO 14001 certification in China and the moderating role of firm size and age. *Journal of Cleaner Production*, Vol. 274, 123059.

Wang, S. S., and Franke, U. (2020). Enterprise IT service downtime cost and risk transfer in a supply chain. *Operations Management Research*, Vol. 13 No. 1, pp. 94-108.

We Forum (2022). How are rising food and energy prices affecting the economy?. Retrieved from: https://www.weforum.org/agenda/2022/09/inflation-rising-food-energy-prices-economy [Accessed on: 02/11/2022].

Webster, J., and Watson, R.T. (2002). Analyzing the past to prepare for the future: writing a literature review. *MIS 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.

Wong, W. P., Tan, H. C., Tan, K. H., and Tseng, M. L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. *Industrial Management & Data Systems*, Vol. 119 No. 6, pp. 1242-1267.

Wu, X., Li, Y., Liu, H., and Zhang, K. (2022). Influence of IT support on firms' cross-channel integration: the moderating role of institutional environment. *Industrial Management & Data Systems,* Vol. 122 No. 4, pp. 1056-1080.

Xie, M., Huang, W., Yang, L., and Yang, Y. (2016). VOAuth: A solution to protect OAuth against phishing. *Computers in Industry*, Vol. 82, pp. 151-159.

Xie, N. M., and Liu, S. F. (2006). Research on extension of discrete grey model and its optimize formula. *Systems Engineering-Theory & Practice*, Vol. 26 No. 6, pp. 108-112.

Yang, Y., Jia, F., Chen, L., Wang, Y., and Xiong, Y. (2021). Adoption timing of OHSAS 18001 and firm performance: An institutional theory perspective. *International Journal of Production Economics*, Vol. 231, 107870.

Yin, R. K. (2017). *Case study research: Design and methods* Sage, Thousand Oaks.

Zhao, H., Han, X., and Guo, S. (2018). DGM (1, 1) model optimized by MVO (multi-verse optimizer) for annual peak load forecasting. *Neural Computing and Applications*, Vol. 30 No. 6, pp. 1811-1825.

Zimon, D., Madzík, P., Dellana, S., Sroufe, R., Ikram, M., and Lysenko-Ryba, K. (2021). Environmental effects of ISO 9001 and ISO 14001 management system implementation in SSCM. *The TQM Journal*, Vol. 34 No. 3, pp. 418-447.

Funding:

This work was supported by the Regione Autonoma Friuli Venezia Giulia within the specific program 89/2019 – Fondo Sociale Europeo 2014/2020.

Appendix 1

Table A1. Country focus of the empirical studies

Author(s)	Year	Country	Aim
Hlača *et al*.	2008	Croatia	Explore the role of ISO/IEC 27001 on the port of Rijeka security
Ku *et al*.	2009	Taiwan	Introduce the information security policy of the Taiwanese government and its current status
Tarn *et al*.	2009	USA	Perform a gap analysis according to ISO/IEC 27001
Smith *et al*.	2010	Australia	Investigate power relationships during ISO/IEC 27001 implementation in an Australian government organization
Asai and Hakizabera	2010	Rwanda	Investigate the issues arising in implementing ISO/IEC 27001 in foreign companies operating in the East African Community
Ozkan and Karabacak	2010	Turkey	Propose a collaborative risk method for the implementation of ISO/IEC 27001
Park *et al*.	2010	South Korea	Investigate the performance implications of ISO/IEC 27001 adoption in South Korean organizations
van Wessel *et al*.	2011	China, Netherlands, and UK	Explore whether the processes of selection, implementation and use of ISO/IEC 27001 differ between China and Europe
Dionysiou	2011	Cyprus	Investigate ISO/IEC 27001 compliance in Cypriot organizations
Tejay and Shokara	2011	USA	Investigate the performance implications of ISO/IEC 27001 adoption in US companies
Liao and Chueh	2012a	Taiwan	Assess the level of attention provided to information security management by medical personnel in Taiwan
Beckers *et al*.	2013	Germany	Provide a method to ease ISO/IEC 27001 adoption
Crowder	2013	UK	Examine the integration of ISO 9001, ISO 14001, and ISO/IEC 27001 in a local authority from UK
Pardo *et al*.	2013	Spain	Propose a method for the harmonization of multiple reference models
Rezaei *et al*.	2014	Iran	Propose a quantitative/qualitative approach for obtaining the information asset value
Itradat *et al*.	2014	Jordan	Analyse the risks faced by a Jordan university and organize a risk assessment plan
Mesquida *et al*.	2014	Spain	Develop a framework to support the integration of different ISO standards related to IT management
Hoy and Foley	2015	England	Evaluate the effects of integrating ISO 9001 and ISO/IEC 27001 audits
Bakar *et al*.	2015	Malaysia	Evaluate the role played by business continuity management

			factors in enhancing organizational performance
Ţigănoaia	2015	Romania and Bulgaria	Develop guidelines for ISO/IEC 27001 implementation
Başaran	2016	Turkey	Evaluate the effects of ISO standards on the emergence of industrial property rights in Turkey
Armeanu *et al*.	2017	Multiple countries	Examine the impact of ISO standards on the economic sentiment indicator
Khajouei *et al*.	2017	Iran	Prioritize and select effective managerial domains and control objectives in information security controls
Dos Santos Ferreira *et al*.	2018	Brazil	Analyse the factors that influence the staff of the Brazilian Air Force information technology board in relation to the understanding of the application of the information security management practices
Culot *et al*.	2019	Italy	Identify emerging practices to deal with cybersecurity threads posed by Industry 4.0
Deane *et al*.	2019	USA	Investigate the performance implications of ISO/IEC 27001 adoption in US companies
Hannigan *et al*.	2019	Qatar	Implement an integrated management system to a Qatari state-owned organization
Annarelli *et al*.	2020	UK and Italy	Propose a managerial cyber resilience framework
Mirtsch *et al*.	2020	Germany	Explore the factors affecting the adoption of ISO/IEC 27001 in Germany
Mirtsch *et al*.	2021	Germany	Investigate the motives, experienced impacts, and obstacles related to ISO/IEC 27001 implementation in German companies
Al-Karaki *et al*.	2022	UAE	Develop a cybersecurity assessment framework based on ISO/IEC 27001
Antunes *et al*.	2022	Portugal	Propose a generic and client-centered cybersecurity auditing information system
Legowo and Juhartoyo	2022	Indonesia	Conduct a risk assessment and provide recommendations to control the risk level
Ruiza *et al*.	2022	Perù	Implement an audit plan and information security through ISO/IEC 27001 for a sales system
Podrecca *et al*.	2022b	USA	Investigate the performance implications of ISO/IEC 27001 adoption in US companies

Appendix 2

Application of DGM (1,1) and EGM (1,1) to Japan data

According to Table 10, Japan data $X^{(0)}$are as follows: 6237, 6914, 7199, 7140, 7171, 8240, 8945, 9161, 12145, 16848, 18103 (ISO, 2021).

Hence, the 1-AGO sequence $X^{(1)}$is: 6237, 13151, 20350, 27490, 34661, 42901, 51846, 61007, 73125, 90000, 108103.

DGM (1,1)

The B matrix is $\begin{bmatrix} 6237 & 1 \\ 13151 & 1 \\ 20350 & 1 \\ 27490 & 1 \\ 34661 & 1 \\ 42901 & 1 \\ 51846 & 1 \\ 61007 & 1 \\ 73125 & 1 \\ 90000 & 1 \end{bmatrix}$, while Y is $\begin{bmatrix} 13151 \\ 20350 \\ 27490 \\ 34661 \\ 42901 \\ 51846 \\ 61007 \\ 73125 \\ 90000 \\ 108103 \end{bmatrix}$

By resolving $[\beta_1, \beta_2]^T = [\mathrm{B}^T\mathrm{B}]^{-1}\mathrm{B}^T Y$, β_1=1.14302 while β_2=4168.496.

Substituting $\beta_1$and $\beta_2$in the time response function of DGM (1,1) we have:

$$\hat{x}^{(0)}(k) = (1.14302\ -1)\left(x^{(0)}(1) - \frac{4168.496}{1-1.14302}\right)1.14302^{k-2}, k = 2,3,\dots,n$$

For k=2, the equation becomes

$$\hat{x}^{(0)}(2) = (1.14302 - 1)\left(6237 - \frac{4168.496}{1-1.14302}\right)1.14302^{2-2} = 5060$$

For k=3, the equation becomes

$$\hat{x}^{(0)}(3) = (1.14302 - 1)\left(6237 - \frac{4168.496}{1-1.14302}\right)1.1430^{3-2} = 5784$$

For k=4, the equation becomes

$$\hat{x}^{(0)}(4) = (1.14302 - 1)\left(6237 - \frac{4168.496}{1-1.14302}\right)1.1430^{4-2} = 6611$$

and so on.

EGM (1,1)

The sequence of data $z^{(1)}$is: 6237, 9694, 16750.5, 23920, 31075.5, 38781, 47373.5, 56426, 67079.5, 81576, 99051.5.

and the resulting matrix B is $\begin{bmatrix} -9694 & 1 \\ -16750.5 & 1 \\ -23920 & 1 \\ -31075.5 & 1 \\ -38781 & 1 \\ -47373.5 & 1 \\ -56426 & 1 \\ -67079.5 & 1 \\ -81576 & 1 \\ -99051.5 & 1 \end{bmatrix}$, while Y is $\begin{bmatrix} 6914 \\ 7199 \\ 7140 \\ 7171 \\ 8240 \\ 8945 \\ 9161 \\ 12145 \\ 16848 \\ 18103 \end{bmatrix}$

By resolving $[\mathrm{a}, \mathrm{b}]^T = [\mathrm{B}^T\mathrm{B}]^{-1}\mathrm{B}^T Y$, a=−0.13475 while b=3829.922.

Substituting a and b in the time response function of EGM (1,1) we have:

$$\hat{x}^{(0)}(k) = (1 - e^{-0.13475})\left(6237 - \frac{3829.922}{-0.13475}\right)e^{0.13475(k-1)}, k = 2,3, \dots, n$$

For k=2, the equation becomes

$$\hat{\mathrm{x}}^{(0)}(2) = (1 - \mathrm{e}^{-0.13475})\left(6237 - \frac{3829.922}{-0.13475}\right)\mathrm{e}^{0.13475(2-1)} = 5000$$

For k=3, the equation becomes

$$\hat{x}^{(0)}(3) = (1 - e^{-0.13475})\left(6237 - \frac{3829.922}{-0.13475}\right)e^{0.13475(3-1)} = 5721$$

For k=4, the equation becomes

$$\hat{x}^{(0)}(4) = (1 - e^{-0.13475})\left(6237 - \frac{3829.922}{-0.13475}\right)e^{0.13475(3-1)} = 6546$$

and so on.