TU Delft OPEN Publishing

Research article

Journal of Standardisation

Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001 in Finland

Gülfem Özmen [1,2,*], *Jussi Heikkilä* [3], *Ville Ojanen* [1]

[1]LUT School of Engineering Sciences, LUT University, Lappeenranta, Finland

[2]Department of Engineering, Innovation and Intellectual Property Management Laboratory, Centre for Technology Management, Institute for Manufacturing, University of Cambridge, United Kingdom

[3]LUT School of Engineering Sciences, LUT University, Lahti, Finland

Abstract: This study examines the adoption of the ISO/IEC 27001 standard among firms in Finland by analyzing the websites of 97 ICT firms, 35 (36%) of which held certification of this standard. The findings show that certified firms communicate their certification through websites, annual reports, and press releases, and engage in cybersecurity-related activities. The results reveal substantial heterogeneity in how firms communicate certification and signal information security quality. ISO/IEC 27001 certification thus functions not only as a compliance mechanism but also as a signaling tool, the effectiveness of which depends on how firms deploy it across communication channels. A thematic analysis of annual reports and press releases identifies four key themes: resilience to cyberattacks, continuous improvement, regulatory compliance, and building trust and reputation. These findings further suggest that certification reflects not only signaling and institutional dynamics but also underlying organizational capabilities, pointing to additional theoretical dimensions for future research.

Keywords: ISO/IEC 27001, information security, cybersecurity, certification, signaling theory

Highlights:

1. ISO/IEC 27001 adoption remains limited among large information and communication technology (ICT) firms in Finland.
2. Certified firms often disclose certification across websites, annual reports, and press releases.
3. Certified firms vary substantially in how they communicate certification and cybersecurity practices.
4. ISO/IEC 27001 certification functions as both a compliance mechanism and a strategic signaling tool shaped by stakeholder demand and regulatory pressures.
5. Certification also reflects underlying organizational capabilities beyond signaling dynamics.

*Corresponding author:
gulfem.ozmen@lut.fi

Submitted: 14-09-2025
Revised: 15-12-2025, 27-03-2026
Accepted: 27-03-2026
Published: 16-06-2026
Peer review: double blind

DOI:
https://doi.org/10.59490/jos.2026.8368

ISSN: 2772-9249

How to cite: Özmen, G., Heikkilä, J., Ojanen, V. (2026). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001 in Finland. *Journal of Standardisation, 5*.
https://doi.org/10.59490/jos.2026.8368

1 Introduction

The diffusion of 5G has accelerated the growth of licensed cellular Internet of Things (IoT) connections (Edquist et al., 2021). Increased connectivity has led organizations to become more dependent on data and, consequently, more vulnerable to information security breaches and cyber threats. Organizations' ability to prevent and recover from cyberattacks builds trust in societies reliant on digital technologies, such as Finland. According to the Nordic Cyber

Resilience Report 2024 by Tietoevry[1], nearly half (47%) of Finnish respondents reported experiencing a serious security attack in 2023, and 85% believe cybercrime will continue to rise.

Organizations establish an Information Security Management System (ISMS) to mitigate the risk of information security breaches (Mirtsch et al., 2021a). ISO/IEC 27001 standard specifies requirements for organizations to follow when establishing and maintaining an ISMS. ISO/IEC 27001:2022 defines an ISMS as "a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives" (ISO, 2022). Organizations can choose to implement the ISO/IEC 27001 standard and, if desired, seek certification. Standard certifications act as a credible market signal (Riillo, 2025; Fomin et al., 2008; Anderson, 1999) for stakeholders.

Organizations may use ISO/IEC 27001 certification as a signaling mechanism to communicate information security capabilities (Mirtsch et al., 2026; Hsu et al., 2016). However, obtaining an ISO/IEC 27001 certification often requires significant company resources (e.g., time, labor, and financial investment) (Podrecca et al., 2022; Culot et al., 2021). The certification is time-consuming and costly (Mirtsch et al., 2021a). It typically takes 6-18 months for a firm to obtain an ISO/IEC 27001 certificate (Podrecca et al., 2022; Svoboda & Horalek, 2018; Longras et al., 2018), with expenses exceeding €50,000 (Longras et al., 2018). Costs associated with certification include employee training (Montiel et al., 2012), external consultancy services (Podrecca et al., 2022; Svoboda & Horalek, 2018; Longras et al., 2018), and third-party audit fees (Montiel et al., 2012). These costs vary depending on organizational size and complexity, the sector of operation, and the number of employees (Clougherty & Grajek, 2023). To justify these investments, the perceived benefits of certification must outweigh the associated costs (Mirtsch et al., 2021b; Fomin et al., 2008).

Policymakers have been seeking solutions to improve information security and cybersecurity (Mirtsch et al., 2021b), with notable examples including the EU Cybersecurity Act and the Network and Information System 2 (NIS2) Directive in Europe, the National Institute of Standards and Technology (NIST) Cybersecurity Act in the U.S., and the Cybersecurity Law and Data Security Law in China. These laws and regulations foster the diffusion of the ISO/IEC 27001 standard (Culot et al., 2021; Longras et al., 2018; Svoboda & Horalek, 2018). The adoption of the ISO/IEC 27001 also helps firms to comply with regulatory and legal requirements (Mirtsch et al., 2021b; Culot et al., 2021; van Wessel & de Vries, 2013) and improve the quality of their Information Security Management Systems.

There are only a few empirical studies that have investigated stock market reactions to the announcement of the ISO/IEC 27001 certification (Podrecca et al., 2022; Deane et al., 2019; Hsu et al., 2016; Tejay et al., 2011) and information security breaches (Garg et al., 2025). However, to our knowledge, no prior research has examined the signaling of information security quality in ISO/IEC 27001-certified firms. Therefore, we empirically analyze the websites of ISO/IEC 27001-certified firms in Finland to answer the following research questions: What is the extent of ISO/IEC 27001 standard certification among firms in Finland? How do ISO/IEC 27001-certified firms in Finland communicate cybersecurity-related practices on their websites? How do ISO/IEC 27001-certified firms signal information security quality to stakeholders?

[1] A total of 3,059 people aged 18–65 responded to the survey in Finland, Sweden, and Norway. The survey was targeted at employees of various companies and the public sector who could make decisions related to cybersecurity. 1,000 of the respondents were from Finland. The survey was conducted between May and August 2024.

This study contributes to the literature on standardization, information security management, and organizational signaling in four ways. First, it extends the signaling perspective by showing that ISO/IEC 27001 certification reflects not only signaling and institutional dynamics but also underlying organizational capabilities. Second, it enriches stakeholder and institutional perspectives by demonstrating how regulatory pressures (e.g., NIS2 Directive) and stakeholder expectations influence both certification decisions and disclosure strategies. Third, it provides novel empirical evidence from Finland, offering the first systematic analysis of how large ICT firms communicate their certification across websites, annual reports, and press releases. Finally, it introduces a combined content and thematic analysis approach to examine how certified firms signal information security quality across multiple disclosure channels. Together, these contributions provide a more nuanced understanding of how standard certification is not only obtained but also strategically communicated in practice.

The rest of this paper is structured as follows: Section 2 introduces cybersecurity regulations and the ISO/IEC 27001 standard. Section 3 explains the ISO/IEC 27001 standard certification from theoretical perspectives. Section 4 presents the results of the empirical analysis. Section 5 discusses the findings. Section 6 concludes with managerial and policy implications, limitations, and avenues for future research.

2 A review of European cybersecurity regulations and the ISO/IEC 27001 standard

2.1 European cybersecurity regulations

IoT devices continue to grow rapidly (Edquist et al., 2021) and are integrated into the daily operations of individuals and organizations (Parsons et al., 2022). These devices generate, exchange, and process vast amounts of data through various forms of connectivity, including Wi-Fi, Bluetooth, cellular networks, and emerging low-power wide-area technologies. The seamless flow of data between devices enables real-time monitoring, automation, and decision-making across domains ranging from smart homes to industrial systems. However, this interconnected environment also raises significant concerns about data security (Weber & Studer, 2016), as sensitive information frequently travels across distributed networks and cloud infrastructures. The interplay between IoT devices, connectivity, and security measures determines the confidentiality, integrity, and availability of data flowing through the broader IoT ecosystem.

Ensuring data security is an ongoing challenge for ICT specialists (Alexei, 2021). According to the 2024 Cost of a Data Breach report, IBM announced that the average global cost of a data breach increased by 10% in one year, rising from USD 4.45 million to USD 4.88 million in 2023[2]. In addition to financial burdens, information security breaches often lead to decreased customer trust, potential legal liabilities, reputational damage, and short-term and long-term drops in stock prices (Garg et al., 2025; Deane et al., 2019). ISO/IEC 27001 standard certification builds a structured approach to mitigate cybersecurity risks (Mirtsch et al., 2021a) and helps organizations to comply with regulatory and legal requirements (Mirtsch et al., 2021b; Culot et al., 2021; van Wessel & de Vries, 2013).

The increased shift to remote work during and after the pandemic, along with geopolitical uncertainties such as Russia's invasion of Ukraine, has raised concerns about information security breaches and cyber threats in recent years. However, Finland has a longstanding

[2] IBM's Cost of a Data Breach report 2024 consisted of 3,556 interviews with 604 organizations impacted by data breaches between March 2023 and February 2024. These organizations were across 17 industries, in 16 countries and regions.

tradition of adopting a comprehensive approach to security and formalizing this within its legal framework. At the European level, the NIS2 Directive[3] establishes a comprehensive and legally codified approach to cybersecurity and risk management that aligns with Finland's existing practices across various sectors. The NIS2 Directive mandates that organizations in critical sectors (e.g., energy, transport, health, and digital infrastructure) and their suppliers assess and manage risks to their communication networks and information systems and report significant incidents to the National Cyber Security Centre Finland.

The Digital Operational Resilience Act (DORA) (EIOPA, 2026) and the Cyber Resilience Act (CRA) (European Commission, 2025) complement the NIS2 Directive. DORA is tailored to the financial sector to enhance ICT risk management for banks, insurance companies, and investment firms. It establishes cybersecurity and resilience requirements for financial institutions. It also applies to third-party ICT service providers providing services to the financial sector. CRA focuses on information security and the resilience of hardware and software manufacturers. It applies to devices or software that contain a digital element and can be directly or indirectly connected to another device or network. The CRA extends cybersecurity requirements to remote data processing solutions and holds product manufacturers accountable for the special features of IoT devices and cloud solutions.

The General Data Protection Regulation (GDPR) is a European law that governs how organizations handle the personal data of EU residents. GDPR's data handling rules and principles apply to all data controllers and processors operating within the European Economic Area. Adopting ISO/IEC 27001 can help firms demonstrate compliance with the GDPR (Kamil et al., 2023; Mirtsch et al., 2021a; Longras et al., 2018) and national cybersecurity laws (Kitsios et al., 2023; Svoboda & Horalek, 2018). Prior research indicates that organizations compliant with ISO/IEC 27001 are better positioned to meet GDPR requirements (Diamantopoulou et al., 2020; Lopes et al., 2019).

2.2 ISO/IEC 27001 standard

Building on the global success of management system standards for quality (ISO 9001) and environment (ISO 14001), the International Organization for Standardization (ISO) has introduced a series of Information Security Management System standards, including ISO/IEC 27001 (Fomin et al., 20008). The ISO/IEC 27001 standard originated in response to technological threats in the late eighties and early nineties[4]. The United Kingdom Government's Department of Trade and Industry (DTI) created evaluation criteria for system security and a set of security practices in 1991. Two years later, the British Standards Institution (BSI) published a set of security procedures under the British standard BS7799. This standard was divided into two parts (BS7799-1 and BS7799-2) in 1998.

The first part of the standard was published as ISO/IEC 17799 in 2000, following a collaboration between the ISO and the International Electrotechnical Commission (IEC). ISO/IEC 17799 was revised in 2005 and renamed ISO/IEC 27002 in 2007. The second part of the standard was adopted in 2005 as an international standard and labelled ISO/IEC 27001. ISO/IEC 27001:2005 was technically revised to the second edition in 2013 and to the third edition in 2022 to address emerging cybersecurity risks. ISO/IEC 27001:2022 mandates requirements for implementing, monitoring, maintaining, and continually improving the ISMS. It also prescribes a set of best practices, including documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive

[3] NIS2 Directive: securing network and information systems | Shaping Europe's digital future

[4] Prior research (cf. Skopak & Sakanovic, 2016; Svoboda & Horalek, 2018) explained the evolution of this standard in depth.

measures. ISO/IEC 27001 is the only standard in the ISO/IEC 27000 family for which an organization can obtain a certificate.

2.3 Certification of ISO/EC 27001:2022 standard

Organizations meeting the requirements described in ISO/IEC 27001:2022 can seek certification from an accredited certification body. Accreditation bodies, under the supervision of the International Accreditation Forum (IAF), accredit certification bodies (Skopak & Sakanovic, 2016). The national accreditation body of Finland is the Finnish Accreditation Service (FINAS). As of May 2025, ISO/IEC 27001 standard certificates can be obtained from six certification bodies[5], accredited by FINAS (FINAS, 2025). Only certificates issued by accredited certification bodies can be included in the annual ISO Surveys (Mirtsch, 2023).

The certification process for ISO/IEC 27001 begins when an organization purchases the standard and reviews its requirements for an ISMS. To comply with the standard for the first time, organizations typically need to implement or modify their security controls. Organizations also must document each security control they implement. Certification is granted through a two-stage audit process (Mirtsch, 2023; Skopak & Sakanovic, 2016). In the first stage, an external auditor evaluates the organization's documentation, and in the second, the auditor assesses whether the practices align with the ISO/IEC 27001 requirements. If the organization meets the criteria, the certification body issues a certificate, typically valid for three years. During this period, regular surveillance audits are conducted to ensure continued compliance, followed by a recertification audit at the end of the cycle (Mirtsch, 2023; Clougherty & Grajek, 2023).

ISO/IEC 27001-certified firms regularly test their systems to identify vulnerabilities and maintain a disaster recovery plan to minimize losses and resume operations quickly after an incident. This proactive approach fosters risk awareness and helps firms to identify and address weaknesses before they are exploited (Kitsios et al., 2023; Fomin et al., 2008). As a result, certified firms are better positioned to mitigate the negative impacts of data breaches, including legal consequences and financial losses (Garg et al., 2025; Kitsios et al., 2023; Culot et al., 2021).

ISO/IEC 27001 certification builds trust between organizations and their stakeholders by ensuring that security controls are in place to protect sensitive customer and business information (Kamil et al., 2023; Longras et al., 2018; Disterer, 2013). Therefore, stakeholders may request their suppliers to obtain certification (Kamil et al., 2023; Podrecca et al., 2022; van Wessel & de Vries, 2013). The ISO/IEC 27001 certification signals a firm's commitment to quality (Mirtsch, 2023; Disterer, 2013) and information security (Hsu et al., 2016; Skopak & Sakanovic, 2016). By demonstrating such commitment, the ISO/IEC 27001 certification can enhance an organization's reputation (Kitsios et al., 2023; Kamil et al., 2023; Mirtsch, 2023), strengthen its corporate image (Culot et al., 2021; Hudson & Orviska, 2013; van Wessel & de Vries, 2013), and ultimately, contribute to increased profitability and market share (Kitsios et al., 2023; Deane et al., 2019).

The scope of certification can range from a single local office to an entire corporation. Thus, organizations may obtain multiple standard certificates for different branches or organizational

[5] Accredited certification bodies providing the ISO/IEC 27001 standard certificates in Finland are Kiwa Sertifiointi Oy, SGS Fimko Oy, Bureau Veritas Certification Finland, KPMG IT Sertifiointi Oy, Nixu Certification Oy, and Into Certification Oy (Information was gathered on 8 May 2025 from the official website of FINAS).

units (Mirtsch et al., 2021a; Hsu et al., 2016). This research focuses on firms certified to the ISO/IEC 27001 standard in Finland.

2.4 Prior empirical research on the adoption of the ISO/IEC 27001 standard

Prior empirical research on the ISO/IEC 27001 standard has mainly focused on the motives and obstacles to its adoption (cf. Mirtsch et al., 2021b; Longras et al., 2018; Svoboda & Horalek, 2018; Skopak & Sakanovic, 2016), while only a few studies have analyzed stock market reactions to to ISO/IEC 27001 certification announcements (Podrecca et al., 2022; Deane et al., 2019; Hsu et al., 2016; Tejay et al., 2011) and to information security breach announcements (Garg et al., 2025). These studies have adopted various data collection methods, such as analyses of public financial reporting databases (Garg et al., 2025; Podrecca et al., 2022; Deane et al., 2019; Hsu et al., 2016; Tejay et al., 2011) and firm-level surveys (Mirtsch, 2023; Mirtsch et al., 2021b; Hsu et al., 2016). Overall, the findings remain mixed.

Tejay and Shoraka (2011) investigated stock market reactions to ISO/IEC 27001 certification announcements among 32 U.S. companies. Their analysis found no statistically significant impact, suggesting that the certification does not yield substantial financial benefits. Similarly, Hsu et al. (2016) examined 25 ISO/IEC 27001-certified firms in Europe and the United States, analyzing publicly available certificates and press releases. By comparing the stock market performance of these firms with that of non-certified firms in the same sectors, they also found no evidence of a positive impact. They concluded that ISO/IEC 27001 serves more as a regulatory compliance measure than a source of competitive advantage.

In contrast, Deane et al. (2019) analyzed 111 public announcements to assess the impact of ISO/IEC 27001 certification on firm market value. Their findings showed that such announcements led to positive stock market reactions, suggesting that investors view the certification as a signal of reduced risk from information security breaches. This perception positions ISO/IEC 27001 as a competitive advantage. Reinforcing this view, Podrecca et al. (2022) examined 143 U.S.-listed firms and found that ISO/IEC 27001 certification is associated with measurable financial performance gains, especially in profitability and labor productivity. The study also noted improved sales performance, particularly for international firms.

Garg et al. (2025) examined the relationship between information security breaches and the risk of stock price crashes among U.S.-listed firms. The study compared firms that experienced breaches with those that did not and assessed the likelihood of crash events. It also analyzed whether ISO/IEC 27001 certification could mitigate these risks. The results indicated that although certification does not entirely prevent stock price crashes, it signals strong governance and risk management. This might positively influence market reactions to security breaches.

Mirtsch (2023) analyzed the adoption of the ISO/IEC 27001 standard in Germany by comparing certified firms with those implementing the standard without certification. The survey revealed that firms adopt the standard primarily to ensure legal compliance, increase employee awareness, and mitigate the risk of information security breaches. However, many firms reported no intention to pursue ISO/IEC 27001 certification, citing a lack of pressure from customers, legislators, and top management. Notably, the study found that organizations with ISO/IEC 27001 certification experienced fewer security breaches.

Mirtsch et al. (2021a) used web mining to analyze the websites of 2,664 German firms and identified references to the ISO/IEC 27001 standard. These references were categorized into firms with certification, firms adopting the standard without certification, firms referring to certified partners, and those offering consultancy or certification services. Their analysis revealed that larger and more innovative ICT service firms are more likely to obtain ISO/IEC 27001 certification. Building on this dataset, Mirtsch et al. (2021b) surveyed 125 ISO/IEC

27001-certified firms in Germany to explore why adoption remains low outside the ICT sector. The findings showed that ICT firms are more driven by customer demand, market access, and corporate image, whereas non-ICT firms adopt the standard mainly for legal compliance. The study concluded that limited short-term economic benefits, such as increased sales or cost savings, and low institutional pressure hinder the broader adoption of ISO/IEC 27001 beyond the ICT industry.

3 Theoretical framework

We employed theoretical triangulation of signaling theory, stakeholder theory, and institutional theory to examine how competition, stakeholder demand, and regulatory pressures impact the diffusion of the ISO/IEC 27001 certification in Finland. Strategic decisions are often characterized by information asymmetries between supplier firms and their (potential) stakeholders (Bergh et al., 2014). Information asymmetries increase transaction costs associated with market transactions (Montiel et al., 2012). Signaling theory (Spence, 1973) provides a mechanism to resolve information asymmetry by transferring information to these stakeholders (Mirtsch et al., 2026; Podrecca et al., 2022; Delmas & Montiel, 2009). Firms typically know their characteristics better than their stakeholders do. Therefore, stakeholders incur search and monitoring costs to identify suppliers with desirable traits. These transaction costs are reduced if firms signal that they possess these characteristics (Montiel et al., 2012). Costly signals are observable actions that provide information about the unobservable characteristics of supplier firms (Spence, 1973).

Firms can signal unobservable characteristics to stakeholders through standard certification (Mirtsch et al., 2026; Montiel et al., 2012; King et al., 2005). Standard certificates serve as a strategic tool (Podrecca et al., 2022; Hsu et al., 2016) to reduce information asymmetry and transaction costs between suppliers and stakeholders (Mirtsch et al., 2026; Delmas & Montiel, 2009; Fomin et al., 2008; Terlaak & King, 2006), thus enabling supplier firms to distinguish themselves from uncertified competitors (Anderson et al., 1999; Spence, 1973). These certificates may lead to improved reputation (Kitsios et al., 2023; Kamil et al., 2023; Mirtsch, 2023), increased sales, and enhanced performance (Mirtsch, 2023; Delmas & Montiel, 2009; Anderson et al., 1999) for firms that maintain certification (Clougherty & Grajek, 2023). Firms that obtain such certifications benefit from signaling higher quality to the market (Hudson & Orviska, 2013).

Signaling theory (Spence, 1973) helps to distinguish between high- and low-quality firms based on observable signals (Clougherty & Grajek, 2023; Bergh et al., 2014). High-quality firms typically incur lower certification costs because they are more likely to meet the standard's requirements already (Clougherty & Grajek, 2023; Montiel et al., 2012). In contrast, low-quality firms face higher expenses due to necessary organizational changes, such as employee training (Montiel et al., 2012; Delmas & Montiel, 2009). Therefore, high-quality firms are more inclined to pursue certification, as the perceived benefits outweigh the associated costs (Mirtsch et al., 2021b; Bergh et al., 2014; Fomin et al., 2008).

The ISO/IEC 27001 standard certification is primarily driven by stakeholder pressures (Kamil et al., 2023; Podrecca et al., 2022; Culot et al., 2021), regulatory pressures (Mirtsch, 2023; Culot et al., 2021), and export markets (Clougherty & Grajek, 2023; Mirtsch et al., 2021a; Hudson & Orviska, 2013). Stakeholder theory (Freeman, 1984) helps to examine the impact of stakeholder pressures on the diffusion of the ISO/IEC 27001 standard (Kamil et al., 2023; Culot et al., 2021). ISO/IEC 27001 serves not only as an international governance tool but also as an external signal of trust and reliability, particularly in globalized and digitally connected markets (Mirtsch et al., 2026). Large private and public sector firms often mandate their suppliers to be

certified to the ISO/IEC 27001 standard (Culot et al., 2021; Alexei, 2021) to signal to their (foreign) partners that they know how to mitigate cybersecurity risks (Kitsios et al., 2023; Mirtsch et al., 2021a; Alexei, 2021). Standard certifications serve as a tool (Podrecca et al., 2022; Hsu et al., 2016) to signal information security quality to stakeholders. Prior empirical research indicates that the stock market responds positively to ISO/IEC 27001 certifications (Garg et al., 2025; Podrecca et al., 2022; Deane et al., 2019).

Institutional theory (DiMaggio & Powell, 1983; Meyer & Rowan, 1977) has been applied in information security research to examine the interplay between compliance, regulatory pressures (Göransson Ording et al., 2022; Uwizeyemungu & Poba-Nzaou, 2015), and the adoption of the ISO/IEC 27001 standard (Culot et al., 2021; Mirtsch et al., 2021b). Regulations as external pressures foster the diffusion of the ISO/IEC 27001 standard (Culot et al., 2021; Longras et al., 2018; Svoboda & Horalek, 2018) and, concurrently, the adoption of the ISO/IEC 27001 standard helps firms to demonstrate compliance with regulatory and legal requirements (Mirtsch et al., 2021b; Culot et al., 2021; van Wessel & de Vries, 2013). The ISO/IEC 27001 standard certification enhances trust (Kamil et al., 2023; Mirtsch et al., 2021b) and confidence of foreign partners (Alexei, 2021). It also serves as a "ticket to the European market" (Dionysiou et al., 2015). International firms are more likely to adopt and certify standards when operating in export markets shaped by EU regulations (Clougherty & Grajek, 2023; Mirtsch et al., 2021a; Hudson & Orviska, 2013).

While signaling theory frames certification as a mechanism for communicating information security capability (Mirtsch et al., 2026), prior research on the adoption of the ISO/IEC 27001 standard shows that firms may implement standards for reasons that extend beyond signaling. Firms may choose to implement the standard internally to improve information security processes and increase employee awareness without bearing the time and cost of certification (Mirtsch et al., 2021a; Hsu et al., 2016). ISO/IEC 27001 is not only a standard but also a strategic tool signaling reliability, competence, and organizational maturity (Mirtsch et al., 2026). Nevertheless, firms with strong alternative signals, such as established brand reputation, extensive patent portfolios, or dominant market position, may not need certification to convey ICT competence or information security capabilities. Thus, these firms may have limited additional benefit from certification. However, adopting a standard without third-party certification does not provide a credible market signal to stakeholders (Riillo, 2025; Montiel et al., 2012). Without credible information security signals, even trustworthy firms may be treated with suspicion or excluded from sensitive supply chains (Mirtsch et al., 2026; Moore, 2010).

4 Empirical analysis

4.1 Method

Our empirical analysis focuses on Finland during the period 2020–2025. This timeframe allows us to examine the impact of geopolitical uncertainties, such as Russia's attack on Ukraine, as well as evolving regulatory frameworks, including the NIS2 Directive, the NIST Cybersecurity Framework, the Digital Operational Resilience Act, and the Cyber Resilience Act, on the adoption of ISO/IEC 27001. Finland is recognized as a leader in digitalization and the adoption of digital technologies (European Commission, 2022). It consistently ranks among the most innovative countries and invests heavily in intellectual property (Dutta et al., 2024). Despite being a frontrunner in digitalization and innovation, Finland, as a small economy, relies heavily on international trade, making it a compelling case for studying the adoption of ISO/IEC 27001.

To understand the national diffusion of the standard, we first analyzed the ISO Annual Surveys, which compile data from accredited certification bodies worldwide. These surveys provide the

number of certificates issued by country and by sector. The results of ISO Annual Surveys (IAF, 2025) between 2021 and 2025 show that ISO/IEC 27001 was the fourth most widely adopted management system standard in Finland, following ISO 9001 for quality management (first), ISO 14001 for environmental management (second), and ISO 45001 for occupational health and safety (third).

Our analysis focuses primarily on ICT firms. ISO began publishing sectoral data in 2006 (Mirtsch et al., 2026). Data from the ISO Annual Surveys (IAF, 2025) show that the ICT sector is the dominant adopter of the ISO/IEC 27001 standard. Consistent with this, Mirtsch et al. (2021a) observed in Germany that nearly half of certified firms offer ICT services and are over three times larger than non-certified firms. ICT firms face strong pressures from stakeholders (Kamil et al., 2023; Podrecca et al., 2022; Culot et al., 2021), regulators (Mirtsch, 2023; Culot et al., 2021), and export markets (Clougherty & Grajek, 2023; Mirtsch et al., 2021a; Hudson & Orviska, 2013) to obtain ISO/IEC 27001 certification – pressures that are less pronounced in non-ICT sectors (Mirtsch et al., 2021b). These industry-specific motivations distinguish ICT firms from other adopters and shape the signaling dynamics observed in this study.

We identified our sample using the ORBIS database, which offers comprehensive cross-country firm-level data on private and publicly listed companies (Kalemli-Özcan et al., 2024). We applied the following criteria: (1) classified under NACE 2 divisions 26 and 58-63[6] (ICT sector), (2) located in Finland, (3) classification as "very large" firms[7], and (4) having an active operational status. This search initially yielded 114 firms. After removing firms without websites and excluding subsidiaries when their parent company was already included, our final sample consisted of 97 firms.

We conducted an online content analysis of these firms' websites to identify which firms held ISO/IEC 27001 certification and how they disclosed it. Content analysis allows systematic and replicable inferences from textual data (Krippendorff, 2019), and online content analysis adapts this approach to web-based sources. Following Mirtsch et al. (2021a), we assumed that "all firms certified to ISO/IEC 27001 would announce this on their websites." Data collection was carried out between April and May 2025.

We then expanded our analysis to explore how firms communicate information security quality to stakeholders. First, we extracted and compiled relevant sections referring to ISO/IEC 27001 certification from firms' annual reports (Ramírez et al., 2022; Nieuwesteeg et al., 2022; Ibrahim et al., 2021) and press releases (Meissner et al., 2025; Ferrigno et al., 2023). Combining these two disclosure channels enabled us to assess the consistency of firms' information security signals across multiple platforms.

The data were analyzed using NVivo 15 qualitative data analysis software (Lumivero, 2025), which was employed for systematic data management and coding. The coding process was driven by the authors and followed an iterative thematic analysis. Thematic analysis enables researchers to identify and interpret patterns of meaning in corporate disclosures (Beattie et al., 2004; Thomas, 1997). In detail, initial codes were generated inductively through repeated readings of the data, capturing recurring patterns in how firms communicate information security practices and certification. These codes were then iteratively refined, merged, and

[6] Orbis database utilizes NACE 2 classification for economic activities. Division 26 is the manufacture of computer, electronic, and optical products. Divisions 58-63 are part of the Information and Communication section (Section J). Division 58 is publishing activities; 59 is motion picture, video, and television program production, sound recording, and music publishing; 60 is programming and broadcasting activities; 61 is telecommunications; 62 is computer programming, consultancy, and related activities; and 63 is information service activities.

[7] Companies on Orbis Europe are considered very large when they match at least one of the following conditions: (1) Operating revenue ≥ 100 million EUR, (2) Total assets ≥ 200 million EUR, (3) Employees ≥ 1000.

grouped into higher-level categories. Finally, the categories were consolidated into four overarching themes that reflect how firms signal the quality of their information security to stakeholders. Throughout the process, the coding scheme was continuously reviewed and applied consistently across documents to ensure coherence in interpretation.

4.2 Results

Our analysis primarily focuses on ISO/IEC 27001-certified firms within the sample. Out of 97 firms, 35 held ISO/IEC 27001 certification. Over half of these firms (51%) had published their certificates online. From the publicly available certificates, we collected additional details, including the initial certification date, certification validity, recertification status, and scope of coverage. Firms that did not publish certificates online often disclosed certification-related information in press releases or annual reports. Most certified firms (71%) had been recertified, while nine firms (26%) obtained certification for the first time between 2024 and 2025. Table 1 summarizes the adoption of the ISO/IEC 27001 standard among ICT firms in Finland. If no evidence of certification was found—such as a certificate listing Finland among certified sites (Hsu et al., 2016), references to certification in a 2024 annual report, or press releases issued in 2024–2025—the firm was classified as "not certified" or "not recertified."

Table 1: The adoption of the ISO/IEC 27001 standard among the ICT firms in Finland

Sectors	Number of firms	Certified firms	Certificate available on the website	Recertification	Adopt the standard without a certificate	Do not adopt the standard in Finland*
Manufacture of computer, electronic and optical products	19	3	2	2	1	15
Publishing activities	15	6	2	4	1	8
Motion picture, video, and television programme production, sound recording and music publishing activities	1	0	0	0	0	1
Programming and broadcasting activities	2	0	0	0	0	2
Telecommunications	10	5	2	4	0	5
Computer programming, consultancy and related activities	45	18	11	12	5	22
Information service activities	5	3	1	3	0	2
Total	**97**	**35**	**18**	**25**	**7**	**55**

Notes: Information was collected from company websites between April and May 2025. We identified six firms in Finland that had been certified to ISO/IEC 27001 in recent years. As no documents confirming recertification were available, we classified these firms as no longer certified. We also considered a firm to have adopted the standard without certification when it announced that it was under audit for ISO/IEC 27001. *Some firms were certified to the ISO/27001 standard outside Finland.

We next examined the cybersecurity activities of certified firms. The findings suggest variation in how certified firms communicate and signal information security quality across stakeholder channels. Certified firms commonly use sub-websites, press releases, and blog posts to communicate their cybersecurity efforts and demonstrate regulatory compliance to investors and other stakeholders. Among the 35 certified firms, 16 (46%) were highly active across different communication channels, 4 (11%) were moderately active, and 15 (43%) were largely

or entirely inactive. Cybersecurity-related press releases were the most used communication channel among 20 (57%) certified firms, followed by cybersecurity events, such as webinars and podcast series, by 15 (43%) firms. We also observed that 14 (40%) of firms had dedicated cybersecurity sub-websites. However, public disclosures rarely addressed cybercrime incidents or data breaches (Garg et al., 2025; Mirtsch et al., 2021b). Consistent with ISO/IEC 27001:2022 standard requirements, 25 (71%) firms reported that employees receive mandatory data protection and information security training, either on their websites, in annual reports, or both. Table 2 illustrates the cybersecurity activities of certified firms.

Table 2: Cybersecurity activities of certified firms

	Cybersecurity activities			
Firms	**Sub-website dedicated to cybersecurity**	**Press releases on cybersecurity**	**Cybersecurity events (e.g., webinars and podcast series)**	**Training employees in data protection and information security**
F1	X	X	X	X
F2	X	X	X	X
F3				X
F4	X	X	X	X
F5	X	X	X	X
F6	X	X	X	X
F7		X		X
F8		X	X	X
F9				X
F10		X		X
F11	X	X	X	X
F12	X	X	X	X
F13	X	X	X	X
F14		X	X	X
F15		X	X	X
F16	X	X		X
F17	X	X		X
F18			X	
F19	X	X	X	X
F20				
F21				
F22				
F23	X	X		X
F24		X		X
F25				
F26	X		X	X
F27				X
F28				
F29				X
F30	X			
F31		X		X
F32		X	X	
F33				X
F34				

F35				
Total	**14**	**20**	**15**	**25**

Notes: Information was collected from company websites between April and May 2025.

We interpreted the variation in communication practices of certified firms presented in Table 2. In digital markets, information security quality is difficult for external stakeholders to observe directly (Mirtsch et al., 2026). Thus, some certified firms use their communication channels to more actively signal their information security quality and reduce information asymmetries (Mirtsch et al., 2026; Montiel et al., 2012). Furthermore, differences in communication channels may reflect varying stakeholder orientations, with disclosures targeting investors through annual reports, customers through websites and press releases, and broader audiences through events. Lastly, the observed heterogeneity may indicate that firms respond differently to regulatory pressures, resulting in strategic differentiation rather than uniform communication practices.

We also analyzed how certified firms signal information security quality to their stakeholders in annual reports and press releases. While annual reports are mandatory for publicly listed firms, some private firms publish them voluntarily. Out of the 35 certified firms, 20 (57%) mentioned their certification in their 2024 annual reports. We also found 46 press releases announcing ISO/IEC 27001 certification. We extracted relevant sections from these documents, compiled them in Excel, and imported them into NVivo 15 for thematic analysis. Table 3 illustrates the four themes we identified based on the codes derived from the annual reports and press releases: (1) ability to prevent and recover from cyberattacks, (2) continuous improvement of information security, (3) compliance with laws, regulations, and industry best practices, and (4) building customer trust and reputation.

Information security breaches often cause legal liabilities, reputational damage, and loss of customer trust (Garg et al., 2025; Deane et al., 2019). ISO/IEC 27001 certification provides a structured framework for mitigating these risks (Mirtsch et al., 2021a). Investors interpret the certification as a signal of reduced risk (Deane et al., 2019). Accordingly, certified firms use their annual reports and press releases to highlight their resilience to cyber threats and commitment to information security.

Table 3: Qualitative themes and selected quotes

Theme	Codes derived from annual reports and press releases	Selected Quotes
Ability to prevent and recover from cyberattacks	security awareness, mitigate cybersecurity threats, prevent data breaches, identify potential security risks, resilience to cyber attacks, responses to evolving security threats	"With cyber-attacks and data security incidents on the rise, organisations are utilising an increasing amount of their own and their partners' resources to mitigate risks. From a customer's perspective, an internationally recognised certification renewed annually through audits that confirm stringent information security measures remain in place makes F6 a safer partner." (F6, press release) "Trust is critical in the cybersecurity industry. Therefore, we recognize that there is a risk that cybersecurity attacks negatively impact our reputation and business, while working with external suppliers and partners can introduce layers of vulnerabilities. This has led to the decision to improve our product-related vulnerability management processes and develop secure software, as well as overall protection against cyber attacks by successfully running and completing ISO27001 certification that further improved the maturity of our security practices across the company." (F15, annual report) "The standard is used as a baseline for ensuring that F15's customer data and products are protected against modern security threats." (F15, annual report)

Continuous improvement of information security	information security culture, employee training on data protection and information security, proactive security monitoring, regularly conducting security audits	"The certification proves to customers that their ICT solutions are secure, that we handle their data in accordance with information security guidelines, and that we are committed to the continuous development of information security within our organisation." (F6, press release) "The security of our customers and stakeholders is of paramount importance to us, and this recognition reflects our long-term commitment to information security. The certificate shows that we are committed to continuously improving our information security practices and ensuring the continuous development of our services." (F23, press release) " ... the certificate is an important testament to the quality of its services. The certificate shows our customers and other stakeholders that our information security management system is at a high level and that we are committed to its continuous improvement." (F17, press release)
Complying with the laws, regulations, and industry best practices	compliance with legal requirements, cybersecurity regulations, and industry best practices	"For our valued customers and partners, our ISO/IEC 27001:2022 certification confirms that their information is handled in secure manner in accordance with industry best practices." (F15, press release) "Through third-party certifications and audits, we provide independent assurance that our security practices are continuously evaluated and aligned with industry's best practices." (F25, press release) "F32's decision to apply for ISO/IEC certification reflects the company's commitment to proactively manage and protect information and assets and to ensure compliance with legal requirements related to information security. Achieving certification is proof that these requirements have been met." (F32, press release)
Building customer trust and reputation	reliable partner, ensure customer trust, demonstrate security capabilities, meet customer demands	"F3 has received the ISO/IC 27001 information security certificate. The certificate is a significant milestone for F3 and emphasises F3's commitment to providing high quality services to our customers." (F3, press release) "ISO/IEC 27001 communicates information security to customers and other stakeholders, that the organization is committed to risk management, and that it is a reliable partner." (F8, press release) "The certified Information Security Management System (ISMS) ensures we systematically protect customer data, intellectual property, and critical business information. This certification provides a substantial competitive advantage, especially in demanding B2B markets, where high levels of security and reliability are essential for investors and customers." (F31, annual report)

Obtaining ISO/IEC 27001 certification demonstrates firms' commitment to the continuous development of information security. The ISO/IEC 27001 certification helps firms comply with regulatory and legal requirements (Mirtsch et al., 2021b; Culot et al., 2021; van Wessel & de Vries, 2013). The findings suggested that certified firms often emphasize their compliance with laws, regulations, and industry best practices. Table 4 presents the regulatory and legal frameworks referenced by the firms. All certified firms, as well as those that had adopted the standard without formal certification, reported compliance with the GDPR. Moreover, 66% (N = 35) of the certified firms indicated compliance with the NIS2 Directive, and nearly all of them published blog posts explaining the directive and providing guidance on how firms can prepare for it.

Table 4: Regulatory and legal compliance of ISO/IEC 27001-certified firms

	Firms refer to compliance		Cybersecurity regulations				
Firms	**Yes**	**No**	**NIS2**	**DORA**	**CRA**	**GDPR**	**NIST**
ISO/IEC 27001 standard-certified	35	0	23	9	5	35	8
Adopt the ISO/IEC 27001 standard without a certification	7	0	3	2	0	7	3
Not certified to the ISO/IEC 27001 standard in Finland*	35	20	10	4	3	34	6

Notes: Information was collected from company websites between April and May 2025. *Some firms were certified to the ISO/27001 standard outside Finland.

ISO/IEC 27001 certification signals a firm's commitment to quality (Mirtsch, 2023; Disterer, 2013) and helps build customer trust and enhance corporate reputation (Kitsios et al., 2023; Kamil et al., 2023; Mirtsch, 2023). ISO/IEC 27001 certification also serves as a credible market signal (Riillo, 2025) of firms' information security capabilities. Several firms explicitly framed certification as evidence of high quality and reliability in their public disclosures. Selected examples include:

"Achieving the ISO 27001 certification is a great milestone for F15 … and it highlights to our customers and partners that we are committed to maintaining a high standard of security." (F15, press release)

"… the certificate is an important testament to the quality of its services." (F17, press release)

"This certificate is a testament to F18's collective effort and dedication to high quality." (F18, press release)

"ISO 27001 allows us to protect critical information and systems while being able to deliver quality products and services to our customers" (F35, press release)

Overall, the results indicate that while the theoretical framework helps structure the empirical analysis, it does not fully account for the observed variation in firms' signaling practices, further elaborated in the discussion.

5 Discussion

This study explored how ISO/IEC 27001-certified ICT firms in Finland adopt and communicate their information security practices, and how certification is used to signal information security quality to stakeholders. By combining website content analysis with thematic analysis of annual reports and press releases, we provided empirical insights into how certified firms differ in their disclosure strategies and signaling behavior.

The interpretation of the findings was guided by the theoretical framework outlined in Section 3. Specifically, signaling theory informed the analysis of how firms communicate certification to reduce information asymmetries (Mirtsch et al., 2026; Delmas & Montiel, 2009; Fomin et al., 2008; Terlaak & King, 2006), while stakeholder and institutional theories shaped the examination of how regulatory pressures (Mirtsch, 2023; Culot et al., 2021) and stakeholder expectations (Kamil et al., 2023; Podrecca et al., 2022; Culot et al., 2021) influence both certification and disclosure practices. This theoretical grounding guided the coding and interpretation of the empirical findings, ensuring that the themes identified in Table 3 were systematically linked to the study's theoretical framework. At the same time, the analysis

allowed inductive insights to emerge from the data, informing the identification of additional patterns that extended beyond the initial theoretical framework.

Our findings showed that many ISO/IEC 27001-certified firms actively engage in signaling activities, while others adopt more selective or limited disclosure practices. Nearly half of the certified firms published their certificates online, and the rest referenced certification primarily through annual reports or press releases. In addition, some firms maintained cybersecurity sub-websites, issued cybersecurity press releases, or organized public events such as webinars and podcasts. These practices suggest that, for some firms, cybersecurity communication extends beyond regulatory compliance and is used strategically to communicate quality to stakeholders. Such behavior aligns with signaling theory, which posits that costly and observable signals such as certification and sustained cybersecurity initiatives can credibly convey otherwise unobservable organizational qualities (Mirtsch et al., 2026; Montiel et al., 2012; Spence, 1973).

The results also revealed heterogeneity in how certification is communicated. A notable share of certified firms displays limited or no public disclosure of certification-related activities, indicating that certification is not uniformly leveraged as a signaling tool. Certified firms were more likely to reference EU cybersecurity regulations, particularly the NIS2 Directive, and to provide public guidance on regulatory compliance. However, these regulatory signals were not consistently emphasized across all certified firms. This uneven pattern reinforces institutional theory's proposition that external pressures shape organizational practices (DiMaggio & Powell, 1983), while also highlighting that firms respond to such pressures in varied and strategic ways depending on sectoral context and stakeholder exposure.

While the theoretical framework informs the results, the empirical findings do not uniformly support ex ante expectations. Despite signaling theory suggesting that certification should be prominently disclosed to reduce information asymmetries (Mirtsch et al., 2026; Terlaak & King, 2006; Spence, 1973), a substantial share of ISO/IEC 27001-certified firms either did not publish their certificates online or made only limited reference to certification in stakeholder channels. Similarly, although institutional theory predicts relatively homogeneous responses under strong regulatory pressure (DiMaggio & Powell, 1983), firms varied considerably in their level of active reference to EU cybersecurity regulations, such as the NIS2 Directive, in their public disclosures (see Table 4). These patterns indicate that strategic, signaling, and institutional incentives operate unevenly across firms and contexts.

The sample also includes seven firms that adopted without seeking certification. Because adoption without third-party certification does not constitute a credible market signal (Riillo, 2025; Montiel et al., 2012), the presence of these firms points to heterogeneity in strategic motives. Some firms may implement the standard primarily to improve internal information security processes or employee awareness without bearing the time, cost, or scrutiny associated with certification (Mirtsch et al., 2021a; Hsu et al., 2016). This finding further reinforces the notion that certification decisions cannot be explained by signaling incentives alone.

Even among certified firms, the strategic use of certification varied. Some firms maintained outdated or minimal references to certification on their websites, potentially weakening the effectiveness of their signaling. This suggests that certification is not always used to achieve competitive differentiation, raising questions about why some firms underutilize a potentially valuable signal.

Overall, the results suggest that ISO/IEC 27001 certification serves as both a compliance mechanism and a strategic signaling tool, but not uniformly. Firms that already align closely with regulatory requirements and stakeholder expectations appear more likely to pursue certification, disclose it prominently, and integrate it into broader cybersecurity communication strategies. At the same time, the observed variation highlights the limits of theoretical

explanations and underscores the importance of accounting for strategic heterogeneity across firms, as further illustrated by the thematic analysis in Table 3.

The themes identified in Table 3 can be interpreted through the theoretical framework of this study, while also pointing to additional theoretical dimensions. The themes of regulatory compliance and alignment with industry standards (Mirtsch et al., 2021b; Culot et al., 2021; van Wessel & de Vries, 2013) closely reflect institutional theory, as they demonstrate firms' responses to regulatory pressures (Göransson Ording et al., 2022; Uwizeyemungu & Poba-Nzaou, 2015). Similarly, the emphasis on building customer trust (Kamil et al., 2023; Mirtsch et al., 2021b) and reputation (Kitsios et al., 2023; Kamil et al., 2023; Mirtsch, 2023) aligns with signaling theory, as firms use certification and related disclosures to communicate information security quality to stakeholders. However, other themes extend beyond these theories. In particular, the themes of continuous improvement and resilience to cyberattacks highlight the role of organizational capabilities, learning processes, and the development of internal competencies. These findings indicate that ISO/IEC 27001 certification is not only a signal of existing quality but is also associated with the development and maintenance of information security capabilities within firms.

Taken together, these results suggest that signaling and institutional theories, while useful, may not fully capture the complexity of ISO/IEC 27001 certification in this context. The findings, therefore, indicate the need for integrating signaling theory with complementary perspectives from strategic management, such as the resource-based view (Barney, 1991; Wernerfelt, 1984) and the dynamic capabilities framework (Eisenhardt & Martin, 2000; Teece et al., 1997), in future research. By highlighting this interplay, the study contributes to a more nuanced understanding of how standard certification functions not only as a market signal but also as part of broader organizational capability development.

6 Conclusion

This study explored the adoption and signaling practices associated with ISO/IEC 27001 certification among large ICT firms in Finland, a country characterized by high levels of digitalization and strong integration into international markets. The findings indicated that ISO/IEC 27001 certification functions both as a compliance mechanism and, for some firms, as a means of communicating information security capabilities and building stakeholder trust.

Analyzing the websites, annual reports, and press releases of 97 large ICT firms, we observed that certified firms are more likely than non-certified firms to reference cybersecurity regulations, communicate employee training and awareness initiatives, and disclose certification-related information through selected stakeholder channels. However, these practices are not uniformly adopted across all certified firms. While some firms actively integrate certification into broader cybersecurity communication strategies, others engage only selectively or maintain minimal public references to certification. The thematic analysis further reveals that, among firms that do communicate certification, disclosures frequently emphasize resilience to cyberattacks, continuous improvement, regulatory compliance, and trust-building.

These findings suggest that ISO/IEC 27001 certification may serve as a market signal of information security quality, but that its signaling function is contingent on firm-specific disclosure strategies and contextual factors. Certification alone does not guarantee active or consistent signaling; rather, its communicative value depends on how firms choose to deploy it across stakeholder channels. This observation underscores the importance of accounting for strategic heterogeneity when examining standard adoption and signaling behavior. This study contributes to the literature on information security standards and organizational signaling by

showing that ISO/IEC 27001 certification functions as a potential market signal whose effectiveness depends on how firms strategically communicate it across channels.

The findings further suggest that ISO/IEC 27001 certification reflects not only signaling and institutional dynamics, but also underlying organizational capabilities, highlighting opportunities for integrating signaling theory with strategic management perspectives, such as the resource-based view (Barney, 1991; Wernerfelt, 1984) and the dynamic capabilities framework (Eisenhardt & Martin, 2000; Teece et al., 1997), in future research. While prior research emphasizes certification as a costly and credible signal of unobservable quality (Mirtsch et al., 2026; Montiel et al., 2012; Terlaak & King, 2006; Spence, 1973), our findings demonstrate that firms vary considerably in whether and how they deploy certification in public disclosures, highlighting a distinction between possessing certification and actively using it to signal information security quality.

For managers, the results highlight that ISO/IEC 27001 certification offers potential value not only as an internal governance tool but also as a strategic communication resource. Firms that proactively disclose certification and related cybersecurity information may strengthen stakeholder trust and reputation, particularly in export- and regulation-oriented markets. For policymakers, the findings suggest that encouraging transparent and consistent disclosure of certification-related practices, rather than certification alone, may enhance the effectiveness of standards-based governance mechanisms.

We recognize several limitations of our study, many of which also suggest promising avenues for future research. This study focuses on the adoption of the ISO/IEC 27001 standard by ICT firms, which are among the most intensive adopters (cf. ISO Annual Surveys, 2021; 2025). While this sector context enables us to observe information security signaling practices in detail, it also limits the generalizability of our findings. Prior research shows that motives for adopting ISO/IEC 27001 differ between ICT and non-ICT sectors. Mirstch et al. (2021b) found that ICT firms are primarily driven by motives such as customer demand, market access (domestic and abroad), competitors being certified, and marketing/image reasons. In contrast, non-ICT firms tend to adopt this standard to increase legal certainty, improve internal processes, and increase employee awareness. Therefore, the signaling mechanisms identified in this study should be interpreted within the ICT sector.

Our empirical analysis primarily examines certification as a mechanism to signal information security quality. However, firms that adopt without certifying may have motives not captured by signaling theory, such as internal improvement and increasing employee awareness (Mirtsch et al., 2021; Hsu et al., 2016). Future research could examine these heterogeneous motives, particularly in technology-intensive sectors where firms possess strong non-certification-based signals. There is also an avenue for future public-sector research on information security governance, as challenges related to data security, cybersecurity, and the protection of critical infrastructure continue to emerge (Magnusson et al., 2025).

Our findings suggest that firms utilize ISO/IEC 27001 certification to communicate information security capabilities to stakeholders (Mirtsch et al., 2026). However, the study examines only the signaling practices of firms that rely on publicly available content (Mirtsch et al., 2021a). It does not assess how stakeholders interpret or judge the credibility of these signals. Future studies can extend our data and further focus on how different stakeholders (e.g., customers, investors, and regulators) interpret ISO/IEC 27001 certification and which factors shape the perceived credibility of this market signal.

Funding (or Grant)

The authors gratefully acknowledge financial support from Business Finland (Technical standards as critical intangible capital for Finnish companies in an era of strategic competition (StandardEdge) project). Heikkilä gratefully acknowledges funding from the Päijät-Häme Regional Fund of the Finnish Cultural Foundation and PHP Säätiö.

Contributor Statement

Gülfem Özmen: Conceptualization, Methodology, Data collection, Formal analysis, Writing-Original Draft, Writing-Review & Editing

Jussi Heikkilä: Supervision, Writing Review & Editing

Ville Ojanen: Supervision, Writing-Review & Editing

Use of AI

During the preparation of this work, the authors used Grammarly in order to check grammar and language. After using this tool, the authors reviewed, edited, made the content their own, validated the outcome as needed, and took full responsibility for the content of the publication.

Acknowledgements

Earlier versions of the paper have been presented at the European Forum for Studies of Policies for Research and Innovation (Eu-SPRI) 2024 conference in Enschede, the R&D Management 2024 conference in Stockholm, and the European Academy for Standardisation (EURAS) 2025 conference in Madrid. We thank Knut Blind, Geerten van de Kaa, Paul Wiegmann, and the conference participants for their helpful comments.

Conflict Of Interest (COI)

There is no conflict of interest.

References

Alexei, A. (2021). Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Science, 4*(1), 84–94. https://doi.org/10.52326/jss.utm.2021.4(1).11

Anderson, S., Daly, D., & Johnson, M. (1999). Why firms seek ISO 9000 certification: Regulatory compliance or competitive advantage? *Production and Operations Management, 8*(1), 28–43. https://doi.org/10.1111/j.1937-5956.1999.tb00059.x

Barney, J. B. (2001). Is the resource-based "view" a useful perspective for strategic management research? Yes. *Academy of Management Review, 26*(1), 41–56. https://doi.org/10.5465/amr.2001.4011938

Beattie, V., McInnes, B., & Fearnley, S. (2004). A methodology for analysing and evaluating narratives in annual reports: A comprehensive descriptive profile and metrics for disclosure quality attributes. *Accounting Forum, 28*(3), 205–236. https://doi.org/10.1016/j.accfor.2004.07.001

Bergh, D. D., Connelly, B. L., Ketchen, D. J., Jr., & Shannon, L. M. (2014). Signaling theory and equilibrium in strategic management research: An assessment and a research agenda. *Journal of Management Studies, 51*(8), 1334–1360. https://doi.org/10.1111/joms.12097

Clougherty, J. A., & Grajek, M. (2023). Decertification in quality-management standards by incrementally and radically innovative organizations. *Research Policy, 52*, 104647. https://doi.org/10.1016/j.respol.2022.104647

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and research agenda. *The TQM Journal, 33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security announcements on the market value of the firm. *Information Technology Management, 20*(3), 107–121. https://doi.org/10.1007/s10799-018-00297-3

Delmas, M., & Montiel, I. (2009). The diffusion of voluntary international management standards: Responsible Care, ISO 9000, and ISO 14001 in the chemical industry. *Policy Studies Journal, 36*(1), 65–93. https://doi.org/10.1111/j.1541-0072.2007.00254.x

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls. *Information and Computer Security, 28*(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

Dionysiou, I., Kokkinaki, A., Magirou, S., & Iacovou, T. (2015). Adoption of ISO 27001 in Cyprus enterprises: Current state and challenges. In *Standards and standardization: Concepts, methodologies, tools, and applications* (pp. 994–1017). IGI Global. https://doi.org/10.4018/978-1-4666-8111-8.ch047

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92–100. https://doi.org/10.4236/jis.2013.42011

Dutta, S., Lanvin, B., León, L. R., & Wunsch-Vincent, S. (2024). *Global innovation index 2024: Unlocking the promise of social entrepreneurship*. WIPO.

Edquist, H., Goodridge, P., & Haskel, J. (2021). The Internet of Things and economic growth in a panel of countries. *Economics of Innovation and New Technology, 30*(3), 262–283. https://doi.org/10.1080/10438599.2019.1695941

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11%3C1105::AID-SMJ133%3E3.0.CO;2-E

European Commission. (2022). *The digital economy and society index (DESI)*. https://digital-strategy.ec.europa.eu/en/policies/desi

European Commission. (2025). *Cyber Resilience Act.* https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Insurance and Occupational Pensions Authority (EIOPA). (2026). *Digital Operational Resilience Act (DORA).* https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Ferrigno, G., Di Paola, N., Oguntegbe, K., F., & Kraus, S. (2023). Value creation in the metaverse age: A thematic analysis of corporate press releases. *International Journal of Entrepreneurial Behavior & Research, 29*(8), 1902–1923. https://doi.org/10.1108/IJEBR-01-2023-0039

Finnish Accreditation Service (FINAS). (2025). *Akkreditoidut toimijat*. https://www.finas.fi/toimijat/Sivut/default.aspx#l=1035

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

Freeman, R. E. (1984). *Strategic management: A strategic approach*. Pitman.

Garg, M., Wang, T., & Wikin, C. L. (2025). Impact of reporting information security breaches, accounting quality, and the opportunistic disclosure of good news and bad news. *International Journal of Accounting Information Systems, 56*, 100729. https://doi.org/10.1016/j.accinf.2025.100729

Göransson Ording, L., Gao, S., & Chen, W. (2022). The influence of inputs in the information security policy development: An institutional perspective. *Transforming Government: People, Process and Policy, 16*(4), 418–435. https://doi.org/10.1108/TG-03-2022-0030

Hsu, C., Wang, T., & Lu, A. (2016). The impact of ISO 27001 certification on firm performance. In *49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842–4848). IEEE. https://doi.org/10.1109/HICSS.2016.600

Hudson, J., & Orviska, M. (2013). Firms' adoption of international standards: One size fits all? *Journal of Policy Modeling, 35*(2), 289–306. https://doi.org/10.1016/j.jpolmod.2012.04.001

Ibrahim, A. E. A., Elamer, A. A., & Ntim, C. G. (2021). Cybersecurity disclosure and corporate governance: Evidence from UK firms. *International Journal of Accounting & Information Management, 29*(4), 701–724. http://dx.doi.org/10.6007/IJARAFMS/v11-i4/11346

International Accreditation Forum (IAF). (2025). *ISO Survey Results.* https://www.iafcertsearch.org/analytics/iso-survey

International Organization for Standardization (ISO). (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements.* ISO/IEC 27001:2022 (en). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Kalemli-Özcan, Ş., Sørensen, B. E., Villegas-Sanchez, C., Volosovych, V., & Yeşiltaş, S. (2024). How to construct nationally representative firm-level data from the Orbis Global Database: New facts on SME and aggregate implications for industry concentration. *American Economic Journal: Macroeconomics, 16*(2), 1–22. https://doi.org/10.1257/mac.20220036

Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and e-Business Management, 21*, 699–722. https://doi.org/10.1007/s10257-023-00646-y

King, A., Lenox, M. J., & Terlaak, A. K. (2005). The strategic use of decentralized institutions: Exploring certification with the ISO 14001 management standard. *Academy of Management Journal, 48*(6), 1091–1106. https://doi.org/10.5465/amj.2005.19573111

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. *Sustainability, 15*, 5828. https://doi.org/10.3390/su15075828

Krippendorff, K. (2019). *Content analysis: An Introduction to Its Methodology*. SAGE Publications. https://doi.org/10.4135/9781071878781

Longras, A., Pereira, T., Carneiro, P., & Pinto, P. (2018). On the track of ISO/IEC 27001:2013 implementation difficulties in Portuguese organizations. *International Conference on Intelligent Systems (IS)*, 886–890. https://doi.org/10.1109/IS.2018.8710558

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. *Journal of Information Systems Engineering & Management, 4*(2), em0089. https://doi.org/10.29333/jisem/5888

Lumivero. (2025). *NVivo* (Version 15.0) [Computer software]. https://lumivero.com/products/nvivo/

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. *International Journal of Information Security, 24*, 177. https://doi.org/10.1007/s10207-025-01097-x

Meissner, F., Wilke, A. J., & Puikytė, M. (2025). How is cybersecurity discussed across media channels? Exploratory analyses of Twitter content and news reporting. *Journal of Risk Research*, *28*(8), 855–875. https://doi.org/10.1080/13669877.2025.2553079

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. https://doi.org/10.1086/226550

Mirtsch, M., Kinne, J., & Blind, K. (2021a). Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis. *IEEE Transactions on Engineering Management, 68*(1), 87–100. https://doi.org/10.1109/TEM.2020.2977815

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021b). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security, 109*, 102383. https://doi.org/10.1016/j.cose.2021.102383

Mirtsch, M. (2023). Adoption of the information security management system standard ISO/IEC 27001: A study among German organizations. *International Journal for Quality Research, 17*(3), 747–768. https://doi.org/10.24874/IJQR17.03-08

Mirtsch, M., Pohlisch, J., & Blind, K. (2026). Certification as a compensation mechanism for weak regulation? Exploring the diffusion of the international standard ISO/IEC 27001 for information security management. *Computers & Security*, *162*, 104774. https://doi.org/10.1016/j.cose.2025.104774

Montiel, I., Husted, B. W., & Christmann, P. (2012). Using private management standard certification to reduce information asymmetries in corrupt environments. *Strategic Management Journal, 33*(9), 1103–1113. https://doi.org/10.1002/smj.1957

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Nieuwesteeg, B., van Eeten, M., & Bauer, J. M. (2022). An Analysis of Changing Transparency Regarding Cybersecurity in Annual Reports. http://doi.org/10.2139/ssrn.4268272

Parsons, E. K., Panaousis, E., Loukas, G., & Sakellari, G. A. (2023). A survey on cyber risk management for the Internet of Things. *Applied Sciences, 13*, 9032. https://doi.org/10.3390/app13159032

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

Ramírez, Y., Manzaneque, M., & Priego, A. M. (2022). The disclosure of information on cybersecurity in listed companies: Proposal for a cybersecurity disclosure index. *Sustainability, 14*(3), 1390. https://doi.org/10.3390/su14031390

Riillo, C. A. F. (2025). ISO 14001 and innovation: Environmental management system and signal. *Technological Forecasting & Social Change, 215,* 124000. https://doi.org/10.1016/j.techfore.2025.124000

Skopak, A., & Sakanovic, S. (2016). Adoption of standard for information security ISO/IEC 27001 in Bosnia and Herzegovina. In *International Conference on Economic and Social Studies (ICESoS)*, Sarajevo, Bosnia and Herzegovina.

Spence, M. (1973). Job market signaling. *Quarterly Journal of Economics, 87*(3), 355–379. https://doi.org/10.2307/1882010

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

Tejay, G. P. S., & 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*, *11*(5-6), 324-343. https://doi.org/10.1504/IJMDM.2011.043407

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z

Terlaak, A., & King, A. A. (2006). The effect of certification with the ISO 9000 quality management standard: A signaling approach. *Journal of Economic Behavior & Organization, 60*(4), 579–602. https://doi.org/10.1016/j.jebo.2004.09.012

Thomas, J. (1997). Discourse in the marketplace: The making of meaning in annual reports. *Journal of Business Communication, 34*(1), 47–66. https://doi.org/10.1177/002194369703400103

Uwizeyemungu, S., & Poba-Nzaou, P. (2015). Understanding information technology security standards diffusion: An institutional perspective. *International Conference on Information Systems Security and Privacy (ICISSP)*, *1,* 5-16. https://doi.org/10.5220/0005227200050016

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

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, *32*(5), 715–728. https://doi.org/10.1016/j.clsr.2016.07.002

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171–180. https://doi.org/10.1002/smj.4250050207