World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The impact of ISO security standards on enhancing cybersecurity posture in organizations

Adebola Folorunso [1, *], Viqaruddin Mohammed [2], Ifeoluwa Wada [3] and Bunmi Samuel [4]

[1] *School of Business, Technology and Health Care Administration Capella University, Minneapolis, MN, USA 55402.*
[2] *University College of Commerce & Business Management Kakatiya University, Warangal, India.*
[3] *Department of Information Technology Services, Washburn University, Topeka, KS, USA.*
[4] *School of Cybersecurity & Information Technology, University of Maryland Global Campus.*

World Journal of Advanced Research and Reviews, 2024, 24(01), 2582–2595

Publication history: Received on 08 September 2024; revised on 19 October 2024; accepted on 21 October 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.1.3169

Abstract

The increasing frequency and sophistication of cyber threats have made organizations need to adopt robust cybersecurity frameworks. ISO security standards, particularly the ISO/IEC 27000 series, play a critical role in enhancing organizations' cybersecurity posture worldwide. These standards provide a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. ISO/IEC 27001, which focuses on establishing an Information Security Management System (ISMS), is widely recognized for its ability to help organizations identify, manage, and mitigate cybersecurity risks. By adopting ISO standards, organizations benefit from improved risk management, enhanced incident response capabilities, and stronger alignment with regulatory compliance requirements, such as GDPR and HIPAA.

In addition, ISO security standards promote a security-first culture within organizations, fostering greater employee awareness and encouraging the consistent implementation of best practices across departments and regions. The adoption of standards like ISO/IEC 27001 (Information security, cybersecurity and privacy protection), ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors), ISO/IEC 27017 (code of practice for information security controls based on ISO/IEC 27002 for Cloud services), ISO/IEC 27015 (Information security management guidelines for financial services) ISO/IEC 27002 (Information security, cybersecurity and privacy protection - Information security controls), and ISO/IEC 27701 (Security techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – requirements and guidelines) has demonstrated significant improvements in data protection, especially in industries handling sensitive personal or financial data. Despite their benefits, implementing ISO standards poses challenges, such as resource constraints, scalability, and the need for continuous updates. As the threat landscape evolves, ISO security standards will remain integral to developing a proactive cybersecurity strategy, integrating with emerging technologies such as artificial intelligence and IoT. The global adoption of these standards reflects their pivotal role in securing the digital infrastructure of modern organizations.

Keywords: ISO Security; Cybersecurity; Organizations; Standards

1. Introduction

As organizations across the globe become increasingly reliant on digital infrastructure, the volume and complexity of cybersecurity threats have increased dramatically (Djenna *et al*., 2021). Ransomware, phishing, distributed denial-of-service (DDoS) attacks, and data breaches are just a few of the sophisticated assaults that are part of today's threat

* Corresponding author: Adebola Folorunso

landscape. Because cybercriminals are always changing their strategies, it is harder for enterprises to protect themselves from these enduring risks (Pawlicka *et al*., 2020). Recent research indicates that cybercrime is becoming more and more expensive, with yearly global losses predicted to reach trillions of dollars. Cyberattacks have repercussions for enterprises that go beyond monetary losses; these include serious harm to their brand, potential legal issues, and the loss of confidential information (Perera *et al*., 2022). One of the most prominent challenges organizations face is the growing frequency of data breaches. Breaches have become more complex, often involving large volumes of sensitive data being compromised and stolen by attackers. The rise of ransomware attacks also poses a significant threat, as attackers use encryption to lock down critical systems and demand payment to release them (Alaba and Jegede, 2021). Additionally, the increasing sophistication of phishing and social engineering techniques makes it difficult to detect and prevent these attacks.

As organizations continue to digitalize their operations and store sensitive information in cloud environments, their exposure to such threats increases. The digital transformation of businesses, combined with an expanded threat landscape, requires organizations to establish more robust cybersecurity measures (Maddireddy, 2022). Failure to do so could lead to irreversible consequences, impacting business continuity, customer trust, and legal compliance. Organizations are putting more and more effort into strengthening their cybersecurity posture in response to these difficulties (Zimmermann and Renaud, 2019). This includes their defenses' overall strength and their capacity to identify, stop, and neutralize cyberattacks. An organization's cybersecurity posture includes all of the instruments, guidelines, procedures, and technology it uses to safeguard its resources (Melaku, 2023). Organizations can reduce the effect of cyber incidents by anticipating and mitigating possible risks with a solid cybersecurity posture through frequency risk assessment and security reviews such as penetration testing (Diogenes and Ozkaya, 2022). Organizations working in highly regulated sectors, like finance, healthcare, and government, where data protection and regulatory compliance are critical, must have a strong cybersecurity posture. However, a successful cybersecurity posture goes beyond simply deploying security technologies. It involves creating a comprehensive, proactive approach to identifying vulnerabilities, managing risks, and establishing effective incident response and recovery processes (Ahmad *et al*., 2021). Internationally recognized security standards play a significant role in shaping and enhancing an organization's cybersecurity posture. These standards provide a structured and consistent framework for managing information security and protecting sensitive data, ensuring that an organization’s approach to cybersecurity is aligned with industry best practices and legal requirements (Syafrizal *et al*., 2020).

The International Organization for Standardization (ISO) is a global organization that develops and publishes international standards across various industries (Zhao *et al*., 2020). In the realm of cybersecurity, ISO has developed a series of security standards that provide organizations with guidelines and best practices for managing their cybersecurity risks. These standards help organizations establish robust security policies and frameworks, improve risk management, and ensure compliance with regulatory requirements. One of the most widely recognized security standards is ISO/IEC 27001, which provides a comprehensive framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) (Mirtsch *et al*., 2020). ISO/IEC 27001 is designed to help organizations protect their information assets from a wide range of threats and ensure the confidentiality, integrity, and availability of their data. This standard emphasizes a risk-based approach to managing information security, allowing organizations to tailor their security measures to their specific risk environment. Complementing ISO/IEC 27001 is ISO/IEC 27002, which provides best-practice guidelines for implementing security controls. It offers detailed guidance on selecting and implementing specific controls to address various risks identified in an organization’s ISMS (Susukailo *et al*., 2021). These controls cover areas such as access management, encryption, physical security, and incident response. In addition, ISO/IEC 27005 focuses on information security risk management, offering a structured approach to identifying, evaluating, and mitigating information security risks. This standard helps organizations align their risk management strategies with their overall business objectives and the evolving threat landscape. The global adoption of ISO security standards has increased significantly in recent years, as organizations recognize the need for a standardized approach to managing cybersecurity risks (Kitsios *et al*., 2023). Many organizations seek ISO certification to demonstrate their commitment to security and gain a competitive edge in the marketplace. Compliance with ISO security standards not only strengthens an organization’s security posture but also ensures alignment with legal and regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Garbagnati and Wu, 2022). As organizations face an ever-growing array of cybersecurity challenges, the adoption of internationally recognized security standards such as ISO/IEC 27001 is becoming essential for strengthening their cybersecurity posture. These standards provide a structured, risk-based approach to managing information security, helping organizations safeguard their assets and navigate the complex threat landscape of the modern digital world (Maleh *et al*., 2021).

2. Overview of Key ISO Security Standards

Organizations all around the world have resorted to ISO (International Organization for Standardization) security standards as a systematic framework for safeguarding their digital assets in the face of changing cybersecurity threats (Aziz *et al*., 2020). These standards offer thorough instructions for putting security measures in place, mitigating cybersecurity risks, and guaranteeing regulatory compliance. With an emphasis on ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and other pertinent standards like ISO/IEC 27701, ISO/IEC 27017, and ISO/IEC 27018, this gives an overview of the main ISO security standards as explained in figure 1 (Al-Karaki *et al*., 2022; Jedlińska and Jedliński, 2023).

Figure 1 The Family Standards of ISO 2700x. (Al-Karaki *et al*., 2022)

ISO/IEC 27001 is the cornerstone of the ISO 27000 family of standards, outlining the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) (Petrunenko, 2022). The ISMS is a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The purpose of ISO/IEC 27001 is to assist organizations in identifying possible security risks, setting up suitable controls, and putting policies in place to safeguard their information assets against threats, illegal access, and other breaches. A continuous improvement process is encouraged by the Plan-Do-Check-Act (PDCA) paradigm, which forms the foundation of the ISO/IEC 27001 structure (Fauzi and Lubis, 2021). Organizations must comply with the standard. Make a plan by determining the security threats and setting goals. Put in place the required security measures to lessen the risks that have been identified. Verify by keeping an eye on and analyzing the ISMS's performance. Act by consistently enhancing the ISMS depending on the outcomes of monitoring and audits. To become certified in ISO/IEC 27001, an organization must undergo an external audit by an accredited certification body (Podrecca *et al*., 2022). The certification process involves two key stages: a review of the organization's ISMS documentation and an on-site audit to assess the implementation and effectiveness of the security controls. ISO/IEC 27001:2022 certification is highly regarded as it demonstrates an organization’s commitment to robust information security practices. The standard outlines a comprehensive set of 93 key controls across 4 categories -Organizational 37 controls, people 8 controls, physical 14 controls, Technological 34 controls including controls such as access control, cryptography, physical security, and incident response (Sun *et al*., 2022). These controls are designed to address the specific risks and vulnerabilities faced by organizations, enabling them to protect their information assets more effectively.

A companion standard to ISO/IEC 27001, ISO/IEC 27002 provides comprehensive guidance on the choice and application of security controls. It offers a collection of best practices that businesses may use to safeguard their assets and information systems. The standard is meant to serve as a useful reference to assist enterprises in aligning their security procedures with ISO/IEC 27001 criteria, rather than as a means of certification (Alexei, 2021). The controls found in ISO/IEC 27002 fall into the following categories: technical, organizational, and physical measures. Some examples are as follows.

Making certain that information and systems are only accessible to those who are authorized.

Data protection via secure key management procedures and encryption.

Safeguarding tangible assets and spaces to avoid harm or unwanted access. Establishing protocols for security issue detection, reporting, and response. ISO/IEC 27002 emphasizes that the implementation of security controls should be risk-based, meaning that controls should be selected and tailored based on the specific risks an organization faces (Wang and Yongchareon, 2020). This approach ensures that security measures are both effective and cost-efficient, allowing organizations to prioritize resources where they are most needed.

ISO/IEC 27005 focuses specifically on the risk management aspects of information security (Fahrurozi *et al*., 2020). It provides organizations with a structured approach to identifying, evaluating, and mitigating cybersecurity risks. The standard is aligned with ISO/IEC 27001, as risk management is a fundamental part of an ISMS (Ukidve *et al*., 2022). The risk management process in ISO/IEC 27005 involves several key steps. Identifying potential security threats and vulnerabilities. Evaluating the likelihood and impact of each risk. Implementing measures to mitigate or accept risks based on their priority. Continuously monitoring the risk environment and making adjustments to controls as needed. ISO/IEC 27005 helps organizations ensure that their security practices are aligned with their overall business objectives (Rodionova and Utepbergenov, 2020; Ademola, 2021). By prioritizing risks and focusing on critical areas, organizations can efficiently allocate resources and ensure that their security efforts support their strategic goals.

In addition to the core standards of ISO/IEC 27001, 27002, and 27005, several other ISO standards address specific aspects of information security and privacy (Putra *et al*., 2021). Extends ISO/IEC 27001 and ISO/IEC 27002 to address privacy management. It provides a framework for managing personal data in compliance with privacy regulations such as the General Data Protection Regulation (GDPR). ISO/IEC 27701 helps organizations establish, implement, and maintain a Privacy Information Management System (PIMS), which is critical for organizations handling personal data. ISO/IEC 27017, Cloud Security, provides guidelines for implementing security controls in cloud computing environments. It extends the controls in ISO/IEC 27002 to address specific risks associated with cloud services, such as shared responsibility between cloud providers and customers. ISO/IEC 27017 is essential for organizations using cloud infrastructure to ensure their data is protected in the cloud (Drozdova *et al*., 2020). ISO/IEC 27018, Protection of Personal Data in Cloud Environments, focuses on safeguarding personal data in cloud services. It offers additional controls to ensure that cloud service providers implement proper measures to protect personally identifiable information (PII). ISO/IEC 27018 helps organizations ensure compliance with privacy regulations when using cloud services to process personal data (Lachaud, 2020).

Organizations are given a structured method by ISO security standards to manage cybersecurity threats and safeguard confidential data. While ISO/IEC 27002 provides best practices for implementing security measures, ISO/IEC 27001 establishes the framework for an efficient ISMS as explained in Figure 2 (Djebbar and Nordström, 2023).

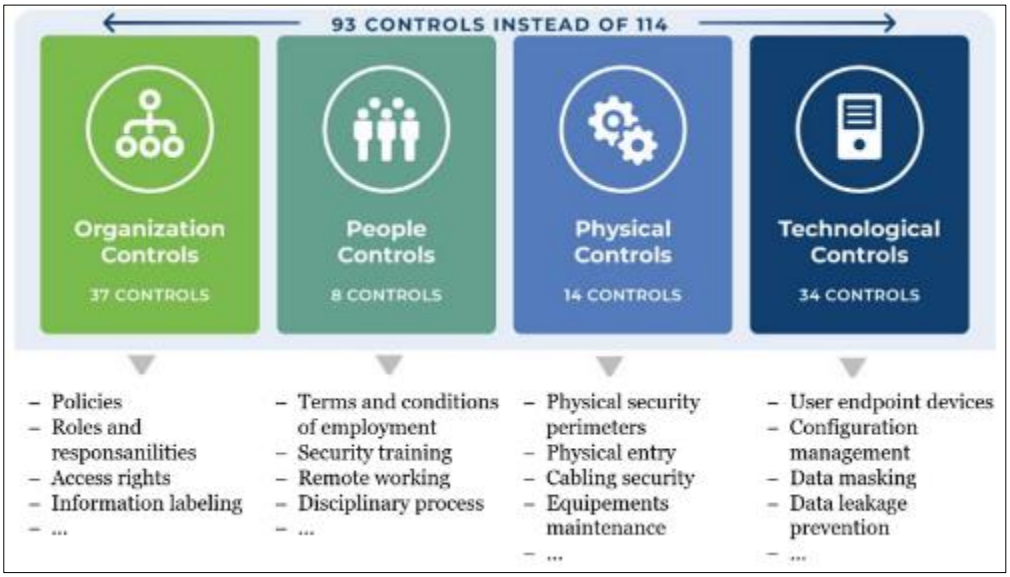

Figure 2 Regions under control in ISO 27001:2022 (Djebbar and Nordström, 2023)

Risk management is made sure to be in line with corporate goals by ISO/IEC 27005. Other standards, such as ISO/IEC 27701, 27017, and 27018, focus on particular issues with cloud security and privacy. When combined, these standards provide a thorough framework for strengthening an organization's cybersecurity posture and guaranteeing adherence to global best practices (Mullet *et al*., 2021).

2.1. Impact of ISO Security Standards on Organizational Cybersecurity Posture

ISO security standards play a critical role in strengthening an organization's cybersecurity posture by providing a structured framework for managing risks, aligning with regulations, fostering a security-conscious culture, and ensuring consistent security practices across multiple locations and supply chains (Onumo *et al*., 2021; Crotty and Daniel, 2021). This explores the key impacts of ISO standards on improving cybersecurity within organizations.

Adopting ISO security standards can increase risk management and threat mitigation, which is one of the main advantages. Risk identification, assessment, and management can be done methodically with the help of ISO standards like ISO/IEC 27005 and ISO/IEC 27001 (Weil, 2020). These standards aid organizations in comprehending their risk environment, evaluating the possibility and possible consequences of threats, and putting in place the necessary controls to lessen those risks. Rather than responding to security events after they happen, this proactive strategy makes sure that protections are in place before they happen. ISO standards encourage organizations to establish a continuous risk management process, where threats are regularly assessed, and controls are updated to address emerging risks (Diop *et al*., 2022). This enables organizations to stay ahead of evolving cyber threats, such as ransomware attacks, phishing, and insider threats, thereby enhancing their overall security resilience.

ISO security standards also enhance security governance by promoting accountability and management involvement in cybersecurity efforts. By requiring senior leadership to be actively engaged in the establishment and maintenance of an Information Security Management System (ISMS), ISO/IEC 27001 ensures that cybersecurity is prioritized at all levels of the organization (Kitsios *et al*., 2022). In addition to governance, ISO standards help organizations align their security practices with legal, regulatory, and industry-specific compliance requirements, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Compliance with these regulations is critical for organizations that handle sensitive data, such as personal information and healthcare records. ISO standards provide a framework for maintaining compliance by addressing key aspects of data protection, access control, and incident response. Adherence to ISO security standards can also improve an organization's standing with regulators, customers, and stakeholders by demonstrating a commitment to maintaining robust security measures and protecting sensitive information (Bicaku *et al*., 2020; Gray *et al*., 2022).

The development of an internal security-first culture within enterprises is one of the major effects of ISO security standards. to guarantee that every employee knows their part in preserving security, ISO standards place a strong emphasis on educating staff members about cybersecurity threats and providing continual training. Employees who have completed training in accordance with ISO/IEC 27001 are guaranteed to be aware of security policies, incident reporting protocols, and secure data handling techniques (Kör and Metin, 2021). Thus, it becomes easier to avoid human errors like using weak passwords or falling for phishing scams, which can result in security breaches. ISO standards encourage enterprises to regularly examine and update their security policies by promoting a culture of continuous development (Gierszewski and Pieczywok, 2020). This ensures that security processes adapt to new threats and technology.

ISO security standards provide organizations with a framework for consistent and standardized implementation of security measures across different locations, departments, and business units as explained in Figure 3 (Karie *et al*., 2021; Al-Karaki *et al*., 2022).

This is particularly important for organizations with a global presence or complex supply chains, where security practices may vary. By adhering to ISO standards, organizations can ensure that security controls are uniformly applied across all locations, reducing the risk of vulnerabilities in one area impacting the entire organization. Additionally, the standardization of security practices facilitates collaboration with suppliers and partners, as ISO standards are widely recognized and adopted across industries. This improves security readiness throughout the supply chain and enhances the organization's overall security posture. ISO security standards also significantly enhance an organization's incident response and recovery capabilities. ISO/IEC 27001 and ISO/IEC 27002 provide guidelines for establishing procedures to detect, report, and respond to security incidents in a timely manner (Ramadhan and Rose, 2022). This ensures that organizations can quickly identify and mitigate the impact of cyberattacks, minimizing the damage caused by data breaches, malware, or system failures. The structured approach to incident response provided by ISO standards includes clear roles and responsibilities, escalation procedures, and post-incident reviews to ensure lessons are learned

and applied (Staves *et al*., 2022). Additionally, ISO standards support faster recovery times by ensuring that business continuity plans are in place, reducing the impact of disruptions on operations. By boosting risk management, fortifying governance, encouraging a security-conscious culture, and guaranteeing uniform security procedures across many locations, ISO security standards are essential in increasing an organization's cybersecurity posture. In an increasingly digital environment, enterprises can secure their operations and reputation by following these standards, which help them better protect their assets, comply with regulations, and lessen the effects of cyber events (Hasan *et al*., 2021).

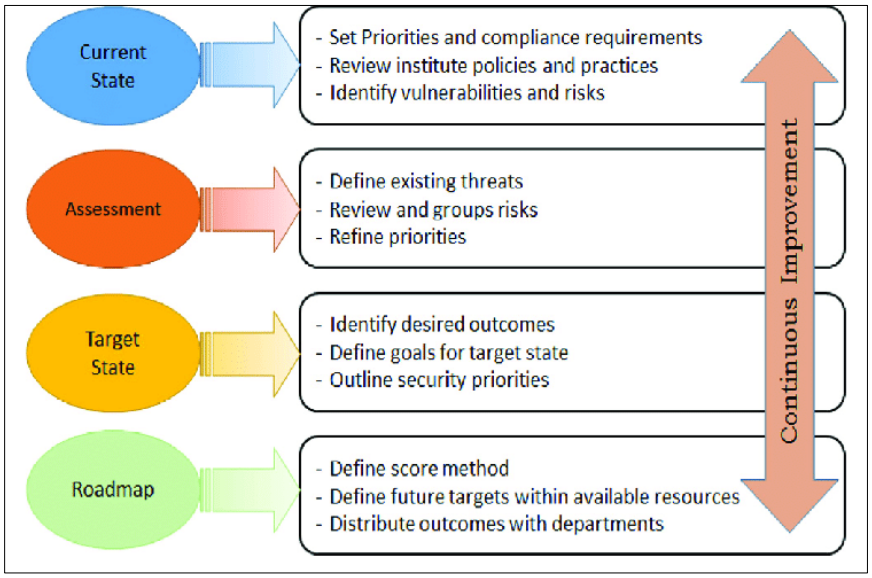

Figure 3 The Methodology for Security Assessment Roadmap (Al-Karaki *et al*., 2020)

2.2. Challenges and Limitations of Implementing ISO Security Standards

ISO security standards, such as ISO/IEC 27001, provide a robust framework for managing information security risks in organizations (Podrecca *et al*., 2022). While these standards are widely recognized for enhancing cybersecurity practices, their implementation presents several challenges and limitations. This examines key obstacles, focusing on resource constraints, scalability and flexibility, continuous maintenance and updates, and resistance to organizational change.

The substantial resource commitment needed to implement ISO security standards is one of the main obstacles. Implementation and certification costs can be unaffordable, particularly for small and medium-sized businesses (SMEs) (Gandhi *et al*., 2021). The auditing process for certification is fee-based and needs to be carried out by third-party organizations with accreditation. Companies also need to budget for the creation and recording of security policies, staff training, and upholding compliance, in addition to direct expenditures. The finances of smaller organizations, which sometimes have fewer financial resources, may be strained by these expenses. Additionally, many firms face additional hurdles due to the specialized knowledge and technologies needed to apply ISO security standards (Zhang *et al*., 2022). ISO/IEC 27001, for instance, requires a comprehensive understanding of risk management, asset protection, and incident response (Koza, 2022). Organizations may need to hire external consultants or invest in internal training to acquire the necessary expertise. These investments in human capital can be costly, particularly in industries where security professionals are in high demand, leading to further strain on organizational resources.

ISO security standards are designed to be broadly applicable across industries and organizational sizes (Breda and Kiss, 2020). However, this universality can lead to challenges in scalability and flexibility. Smaller organizations may struggle to implement all aspects of the standards, as some requirements may seem excessive for their operations. For example, the level of documentation and control required in ISO/IEC 27001 may be too complex for a small company with limited personnel. Conversely, larger organizations may find that the standards do not address all of their unique security needs, requiring additional measures to ensure comprehensive protection (Sobb *et al*., 2020). Adapting ISO standards to fit different industries also presents limitations. While the standards provide a solid foundation for information security, certain sectors, such as healthcare or finance, may require industry-specific security controls that ISO standards do not fully address. Organizations in these industries may need to supplement ISO standards with additional frameworks or regulations to ensure compliance with both industry and regulatory requirements, adding another layer of complexity to the implementation process (Björnsdóttir *et al*., 2022).

Implementing ISO security standards is not a one-time effort; it requires continuous maintenance and regular updates. Organizations must perform regular audits to ensure that they remain compliant with the standards, which can be both time-consuming and costly. These audits often involve reviewing security controls, updating risk assessments, and documenting any changes in the organization's infrastructure or processes (Antunes *et al*., 2022). In many cases, organizations must also invest in ongoing employee training to ensure that personnel stay informed of new security policies and practices. Furthermore, ISO security standards themselves are subject to periodic revisions and updates. Organizations that have already achieved certification may find it challenging to stay up to date with the latest versions of the standards (Villela *et al*., 2021). This requires additional resources to review and implement new guidelines, which can be a significant burden for organizations with limited personnel or budget constraints. Failure to stay current with ISO standards can lead to non-compliance, putting the organization at risk of losing its certification and exposing it to security vulnerabilities (Stevens *et al*., 2020).

Overcoming organizational change resistance presents a key difficulty in the implementation of ISO security standards. The organization's culture and structure must frequently change in order to implement new security procedures and policies (Da Veiga *et al*., 2020). New procedures may be met with resistance by staff members, particularly if they believe they will complicate matters or make their jobs more difficult. In companies where security has previously been a lower concern or where workflows are well-established, this resistance may be especially noticeable (Pennekamp *et al*., 2021). to bring about change, leadership must be important in promoting a security-aware culture and emphasizing the value of upholding the standards. However, it may take some time and work to bring about this cultural change, particularly in companies with poor security awareness. Additionally, structural resistance, such as siloed departments or a lack of collaboration between IT and other business units, can impede the successful implementation of ISO standards (Bakos and Dumitraşcu, 2021).

Although there are of several obstacles involved, implementing ISO security standards gives enterprises an organized method for managing information security (Aleksandrov *et al*., 2021). Resource limitations can be a major obstacle, such as the price of certification and the requirement for specific knowledge. Issues with scalability and flexibility occur when applying the standards to various industry types and sizes of organizations. It takes time and money to spend on frequent upgrades and continuous maintenance. Finally, the effective implementation of these standards depends on overcoming organizational change resistance. Despite these obstacles, businesses can greatly strengthen their cybersecurity posture and better safeguard their assets from emerging threats by successfully implementing ISO security standards (Kuzminykh *et al*., 2021; Chidukwani *et al*., 2022).

2.3. Case Studies: Successful Implementation of ISO Standards

The effective application of ISO security standards in a number of businesses has improved cybersecurity, data protection, and privacy (Wylde *et al*., 2022). By looking at actual cases from the technology, healthcare, and finance industries, we can see how ISO standards give businesses organized frameworks for enhancing security. The three case studies that are highlighted here include a financial institution that is implementing ISO/IEC 27001, a healthcare organization that is employing ISO/IEC 27701, and a technology business that is enhancing cloud security with ISO/IEC 27017.

A leading financial institution faced growing concerns about the security of its customer data amid increasing cyber threats. As a major player in the banking sector, it managed a vast amount of sensitive financial information, making it a prime target for cyberattacks (Pomerleau and Lowery, 2020). To address these risks, the institution decided to implement ISO/IEC 27001, the international standard for information security management systems (ISMS). The institution began by conducting a thorough risk assessment, identifying potential vulnerabilities in its data handling and storage processes (Kandasamy *et al*., 2020). By aligning its security practices with the ISO/IEC 27001 framework, it developed and implemented a comprehensive ISMS. This system included stringent access controls, encryption of sensitive data, and enhanced monitoring of network traffic (Aftab *et al*., 2021). In addition, employees received regular training on information security policies and procedures to promote awareness and compliance throughout the organization. After implementing ISO/IEC 27001, the institution saw a marked reduction in security incidents and data breaches. The enhanced focus on risk management helped the organization identify and mitigate threats more effectively (Fraser *et al*., 2021). Additionally, external audits confirmed the robustness of the ISMS, boosting the institution's credibility and reinforcing customer trust. Ultimately, the adoption of ISO/IEC 27001 not only improved data protection but also minimized the financial and reputational risks associated with cyberattacks, demonstrating the standard's significant value in the financial sector (Aslam *et al*., 2022).

A large healthcare organization, responsible for managing sensitive patient data, sought to enhance its privacy management practices amid tightening regulations such as the General Data Protection Regulation (GDPR). Recognizing

the need for a standardized approach, the organization chose to implement ISO/IEC 27701, a privacy extension to ISO/IEC 27001 that provides guidelines for managing personally identifiable information (PII) (Kurii and Opirskyy, 2022). The healthcare provider's primary challenge was ensuring the confidentiality of patient records while complying with both local and international data privacy regulations. To address this, the organization integrated ISO/IEC 27701 into its existing ISMS, establishing a Privacy Information Management System (PIMS). This system enabled the healthcare provider to clearly define roles and responsibilities for handling PII, ensuring that all patient data was collected, stored, and processed securely. Implementing ISO/IEC 27701 allowed the organization to systematically assess the privacy risks associated with its data management practices. It also introduced new measures such as encryption, anonymization, and role-based access control to safeguard patient information. As a result, the healthcare provider achieved full compliance with privacy regulations while also significantly reducing the likelihood of data breaches. Through ISO/IEC 27701, the organization not only strengthened patient data privacy but also enhanced its ability to respond to regulatory inquiries and audits (Alessi *et al*., 2021). This proactive approach fostered greater patient trust, as individuals became more confident that their sensitive health data was being handled securely and in accordance with stringent privacy standards (Bussone *et al*., 2020; Gille *et al*., 2022).

A global technology company specializing in cloud services faced growing concerns over the security of its cloud infrastructure (Alghofaili *et al*., 2021). With an increasing number of clients relying on its platform to store and process sensitive information, the company needed to bolster its cloud security posture. To address these challenges, it adopted ISO/IEC 27017, an international standard providing security controls specific to cloud services. ISO/IEC 27017 offered the technology company a structured framework to identify and address potential vulnerabilities in its cloud environment. The company implemented key security measures, including enhanced encryption protocols for data at rest and in transit, stricter access control policies, and regular vulnerability assessments (Shukla *et al*., 2022). In addition, the company focused on ensuring the security of client data by incorporating shared responsibility models, which clearly defined the security obligations of both the cloud service provider and its customers. By aligning its practices with ISO/IEC 27017, the technology company successfully mitigated several risks related to cloud computing, including unauthorized access, data leaks, and misconfigurations (Taherdoost, 2022). The implementation of these enhanced security measures not only improved client confidence in the safety of the cloud platform but also attracted new customers who sought robust, compliant cloud services. Furthermore, the certification with ISO/IEC 27017 became a valuable marketing tool, allowing the company to differentiate itself from competitors and demonstrate its commitment to the highest levels of cloud security. The implementation of ISO/IEC 27017 positioned the company as a leader in the cloud services industry, showcasing the importance of industry-specific standards in addressing evolving security challenges (Alaloul *et al*., 2022).

These case studies highlight the major advantages of applying ISO security standards to various sectors. Whereas ISO/IEC 27701 boosted patient data privacy in the healthcare industry, ISO/IEC 27001 enhanced data protection and risk management in the financial sector. ISO/IEC 27017 improved cloud security for the technology organization, highlighting the significance of customized security measures for cloud settings (ISO, 2015). When taken as a whole, these illustrations demonstrate how effective use of ISO standards improves security procedures while also cultivating trust, compliance, and competitive advantage in a number of industries (Stewart, 2022; Sun *et al*., 2022).

2.4. Future Trends and Considerations in ISO Security Standards

ISO security standards need to stay up with the rapid advancements in technology and the dynamic threat landscape as the digital world continues to change (Tornjanski *et al*., 2021). The way business's function is changing due to emerging technologies like blockchain, IoT, and artificial intelligence (AI), which creates new cybersecurity issues. The worldwide scope of cybersecurity also necessitates more cooperation amongst international standards groups.

Emerging technologies such as AI, IoT, and blockchain are transforming industries by improving efficiency, data processing, and connectivity (Aoun *et al*., 2021). However, these technologies also introduce new cybersecurity risks. AI systems, for example, can be vulnerable to adversarial attacks that manipulate algorithms, while IoT devices often suffer from weak security configurations, making them easy targets for cybercriminals. Blockchain, although inherently secure due to its decentralized nature, is not immune to attacks, particularly at the application level. ISO security standards will play a critical role in securing these emerging technologies (Zamani *et al*., 2020; Gourisetti *et al*., 2021). For AI, ISO/IEC is already developing standards to ensure the safety, security, and ethical use of AI systems. Future standards will likely focus on creating frameworks for mitigating risks associated with AI-powered decision-making processes, ensuring that AI systems are resilient against attacks such as data poisoning or algorithm manipulation (Belhadi *et al*., 2022; Judijanto *et al*., 2022). In the realm of IoT, standards like ISO/IEC 27030, which is currently under development, aim to address the specific security requirements of connected devices. These standards will guide organizations in implementing secure protocols, data encryption, and access controls across the growing IoT ecosystem.

Similarly, blockchain technology could benefit from the development of new ISO standards that focus on the security of smart contracts, encryption, and transaction validation processes. By providing clear guidelines, ISO standards will ensure that organizations deploying these technologies can do so in a secure and compliant manner, ultimately reducing their exposure to cyber risks (Viegas and Kuyucu, 2022).

The cyber threat landscape is constantly evolving, with new vulnerabilities and attack vectors emerging as technology advances. Cybercriminals are becoming more sophisticated, utilizing techniques such as advanced persistent threats (APTs), ransomware, and zero-day exploits to breach even the most secure systems. As a result, ISO standards must continuously adapt to address these emerging threats. One of the key challenges in this adaptation is maintaining the relevance of ISO standards in the face of rapidly changing cybersecurity practices (Malatji *et al*., 2022). For instance, as cloud computing and remote work become more prevalent, standards such as ISO/IEC 27001 and ISO/IEC 27017 will need to be updated to reflect the growing importance of securing cloud infrastructure and remote access points. Additionally, the rise of quantum computing poses a significant long-term threat to current encryption methods, necessitating the development of post-quantum cryptography standards. ISO standards must also evolve to address the growing threat of supply chain attacks, which exploit vulnerabilities in third-party vendors and service providers to infiltrate organizations (Boyson *et al*., 2022). Standards that focus on securing the software supply chain, such as ISO/IEC 27036 (Information Security for Supplier Relationships), will need to be expanded to provide more detailed guidance on managing risks across complex, interconnected ecosystems (Yigit *et al*., 2021; Abernathy and Hayes, 2022).

The global nature of cybersecurity requires greater collaboration between international standards organizations. While ISO standards are widely recognized and adopted, other organizations such as the National Institute of Standards and Technology (NIST), the Payment Card Industry Data Security Standard (PCI-DSS), and the European Union's General Data Protection Regulation (GDPR) also play crucial roles in shaping cybersecurity practices (Ramirez *et al*., 2020; Stapleton, 2021). Harmonizing these standards with ISO frameworks can help create a more cohesive global cybersecurity landscape, reducing fragmentation and ensuring that organizations adhere to consistent security practices across borders. One key area of collaboration is in the alignment of standards for critical infrastructure protection. For example, NIST's Cybersecurity Framework is widely used in the United States to secure critical industries such as energy, transportation, and healthcare. By aligning ISO standards with NIST's framework, organizations operating globally can more easily comply with multiple regulatory requirements while ensuring that their cybersecurity practices are consistent and robust (Hamdani *et al*., 2021; Brumfield, 2021). Another important area for collaboration is in the financial sector, where standards such as PCI-DSS govern the security of payment card data. ISO/IEC 27001, which focuses on broader information security management, could be harmonized with PCI-DSS to streamline compliance efforts for organizations that handle payment information. This would help reduce duplication of efforts and ensure that security controls are implemented consistently across different regulatory frameworks.

The need to adjust to a changing cyber threat scenario, the incorporation of emerging technologies, and enhanced international cooperation will all influence the direction of ISO security standards in the future. As blockchain, AI, and IoT technologies develop further, ISO standards will offer crucial foundations for protecting these breakthroughs (Yalcinkaya *et al*., 2021). Furthermore, the constant change in cyber dangers necessitates that ISO standards continue to be flexible and adaptable to new threats. To ensure that businesses can adequately safeguard their assets in an increasingly linked world, a unified worldwide approach to cybersecurity will require improved cooperation between ISO and other international standards organizations (Jarjoui and Murimi, 2021; Dhirani *et al*., 2021).

3. Conclusion

In a variety of industries, ISO security standards have shown to be crucial in improving an organization's cybersecurity posture. These standards assist organizations to detect vulnerabilities, put strong security measures in place, and promote a continuous improvement culture by offering established frameworks and best practices. The implementation of standards such as ISO/IEC 27001, ISO/IEC 27701, and ISO/IEC 27017 has led to increased data protection, regulatory compliance, and general confidence from clients and stakeholders. Businesses that adopt these standards frequently see a decrease in security incidents and an improvement in their capacity to counter new threats.

However, achieving certification is only the first step; ongoing commitment to maintaining and evolving security standards is crucial. As the cyber threat landscape continuously evolves, organizations must regularly review and update their security practices to address new vulnerabilities and compliance requirements. This commitment not only enhances resilience but also instills confidence in clients and partners, further solidifying the organization's reputation in a competitive marketplace.

In the future, ISO security standards will become even more important for negotiating the intricacies of a digital environment that is changing quickly. The emergence of cutting-edge technologies like blockchain, the Internet of Things, and artificial intelligence will make flexible and progressive security standards essential. Moreover, closer cooperation across international standards groups will be necessary to develop a coherent framework that tackles the problems associated with global cybersecurity. The significance of ISO security standards in preserving sensitive data and guaranteeing a secure digital environment cannot be emphasized, especially as enterprises are still confronted with sophisticated cyberattacks. In an interconnected future, proactive standards evolution will be essential to helping enterprises achieve strong cybersecurity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abernathy, R. and Hayes, D.R., 2022. *CISSP cert guide*. Pearson IT certification.

[2] Ademola, E.O., 2021. Towards an Effective Information Assurance and Risk Management (IA&RM) Guide: A Case Study. *Journal of Behavioural Informatics, Digital Humanities and Development Research*, *7*(1), pp.1-12.

[3] Aftab, M.U., Oluwasanmi, A., Alharbi, A., Sohaib, O., Nie, X., Qin, Z. and Ngo, S.T., 2021. Secure and dynamic access control for the Internet of Things (IoT) based traffic system. *PeerJ Computer Science*, *7*, p.e471.

[4] Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T. and Baskerville, R.L., 2021. How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, p.102122.

[5] Alaba, F.A. and Jegede, A., 2021. Ransomware attacks on remote learning systems in 21st century: a survey. *Biomed J Sci Tech Res*, *35*(1).

[6] Alaloul, W.S., Saad, S. and Qureshi, A.H., 2022. Construction sector: IR 4.0 applications. In *Handbook of Smart Materials, Technologies, and Devices: Applications of Industry 4.0* (pp. 1341-1390). Cham: Springer International Publishing.

[7] Aleksandrov, M.N., Vasiliev, V.A. and Aleksandrova, S.V., 2021, September. Implementation of the risk-based approach methodology in information security management systems. In *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 137-139). IEEE.

[8] Alessi, A., Ciccarelli, G., Cipolli, L., Guidotti, L., Marsano, A. and Hanganu, A., 2021. Privacy by design and by default in software development in order to prevent unlawful processing of personal data. Privacy certifications impact on software development and liabilities.

[9] Alexei, A., 2021. Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Sciences*, *4*(1), pp.84-94.

[10] Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A. and Al-Rimy, B.A.S., 2021. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. *Applied Sciences*, *11*(19), p.9005.

[11] 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*, *34*(6), pp.3079-3095.

[12] Antunes, M., Maximiano, M. and Gomes, R., 2022. A client-centered information security and cybersecurity auditing framework. *Applied Sciences*, *12*(9), p.4102.

[13] Aoun, A., Ilinca, A., Ghandour, M. and Ibrahim, H., 2021. A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology. *Computers & Industrial Engineering*, *162*, p.107746.

[14] Aslam, M., Khan Abbasi, M.A., Khalid, T., Shan, R.U., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D.A. and Ahmad, R., 2022. Getting smarter about smart cities: Improving data security and privacy through compliance. *Sensors*, *22*(23), p.9338.

[15] Aziz, B., Doss, R. and Yustianto, P., 2020, October. Digital security reference model: a survey and proposal. In *2020 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 323-328). IEEE.

[16] Bakos, L. and Dumitraşcu, D.D., 2021. Decentralized enterprise risk management issues under rapidly changing environments. *Risks*, *9*(9), p.165.

[17] Belhadi, A., Kamble, S., Fosso Wamba, S. and Queiroz, M.M., 2022. Building supply-chain resilience: an artificial intelligence-based technique and decision-making framework. *International Journal of Production Research*, *60*(14), pp.4487-4507.

[18] Bicaku, A., Tauber, M. and Delsing, J., 2020. Security standard compliance and continuous verification for Industrial Internet of Things. *International Journal of Distributed Sensor Networks*, *16*(6), p.1550147720922731.

[19] Björnsdóttir, S.H., Jensson, P., de Boer, R.J. and Thorsteinsson, S.E., 2022. The importance of risk management: what is missing in ISO standards?. *Risk Analysis*, *42*(4), pp.659-691.

[20] Boyson, S., Corsi, T.M. and Paraskevas, J.P., 2022. Defending digital supply chains: Evidence from a decade-long research program. *Technovation*, *118*, p.102380.

[21] Breda, G. and Kiss, M., 2020. Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. *Procedia Manufacturing*, *46*, pp.580-590.

[22] Brumfield, C., 2021. Cybersecurity risk management: Mastering the fundamentals using the NIST cybersecurity framework. John Wiley & Sons.

[23] Bussone, A., Kasadha, B., Stumpf, S., Durrant, A.C., Tariq, S., Gibbs, J., Lloyd, K.C. and Bird, J., 2020. Trust, identity, privacy, and security considerations for designing a peer data sharing platform between people living with HIV. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), pp.1-27.

[24] Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, pp.85701-85719.

[25] Crotty, J. and Daniel, L., 2021. Lessons from practice: insights on cybersecurity strategy for business leaders, from SMEs to global enterprises. *Milton Keynes: Open University*.

[26] Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M., 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, p.101713.

[27] Dhirani, L.L., Armstrong, E. and Newe, T., 2021. Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, *21*(11), p.3901.

[28] Diogenes, Y. and Ozkaya, E., 2022. Cybersecurity–Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system. Packt Publishing Ltd.

[29] Diop, I., Abdul-Nour, G.G. and Komljenovic, D., 2022. A high-level risk management framework as part of an overall asset management process for the assessment of industry 4.0 and its corollary industry 5.0 related new emerging technological risks in socio-technical systems. *American Journal of Industrial and Business Management*, *12*(7), pp.1286-1339.

[30] Djebbar, F. and Nordström, K., 2023. A comparative analysis of industrial cybersecurity standards. *IEEE Access*.

[31] Djenna, A., Harous, S. and Saidouni, D.E., 2021. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), p.4580.

[32] Drozdova, M., Bridova, I., Uramova, J. and Moravcik, M., 2020, November. Private cloud security architecture. In *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)* (pp. 84-89). IEEE.

[33] Fahrurozi, M., Tarigan, S.A., Tanjung, M.A. and Mutijarsa, K., 2020, October. The use of ISO/IEC 27005: 2018 for strengthening information security management (a case study at data and information Center of Ministry of Defence). In *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)* (pp. 86-91). IEEE.

[34] Fauzi, R. and Lubis, M., 2021. Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM). *International Journal of Advanced Computer Science and Applications*, *12*(10).

[35] Fraser, J.R., Quail, R. and Simkins, B. eds., 2021. Enterprise risk management: Today's leading research and best practices for tomorrow's executives. John Wiley & Sons.

[36] Gandhi, A., Nurcahyo, R. and Gabriel, D.S., 2021, March. Identification of challenges and benefits of product certification on micro, small, and medium enterprises (MSMEs) in Indonesia. In *Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management, Singapore* (pp. 499-509).

[37] Garbagnati, A. and Wu, L., 2022. Creating competitive advantage: privacy and security by design in mhealth and digital health products. *The Health Lawyer*, *34*(4), pp.9-34.

[38] Gierszewski, J. and Pieczywok, A., 2020. Organisational security culture in small enterprises: A case study. *Entrepreneurship and Sustainability Issues*, *8*(2), p.438.

[39] Gille, F., Smith, S. and Mays, N., 2022. Evidence-based guiding principles to build public trust in personal data use in health systems. *Digital Health*, *8*, p.20552076221111947.

[40] Gourisetti, S.N.G., Cali, Ü., Choo, K.K.R., Escobar, E., Gorog, C., Lee, A., Lima, C., Mylrea, M., Pasetti, M., Rahimi, F. and Reddi, R., 2021. Standardization of the distributed ledger technology cybersecurity stack for power and energy applications. *Sustainable Energy, Grids and Networks*, *28*, p.100553.

[41] Gray, J., Ross, J. and Badrick, T., 2022. The path to continual improvement and business excellence: compliance to ISO standards versus a business excellence approach. *Accreditation and Quality Assurance*, *27*(4), pp.195-203.

[42] Hamdani, S.W.A., Abbas, H., Janjua, A.R., Shahid, W.B., Amjad, M.F., Malik, J., Murtaza, M.H., Atiquzzaman, M. and Khan, A.W., 2021. Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR)*, *54*(3), pp.1-36.

[43] Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, p.102726.

[44] International Standard Organization (2015). Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO/IEC 27017:2015, pp30. Available at: https://www.iso.org/standard/43757.html

[45] Jarjoui, S. and Murimi, R., 2021. A framework for enterprise cybersecurity risk management. In *Advances in cybersecurity management* (pp. 139-161). Cham: Springer International Publishing.

[46] Jedlińska, L. and Jedliński, M., 2023. 3D intraoral scan and diagnostic plaster model under General Data Protection Regulation–Legal protection. *Journal of Forensic and Legal Medicine*, *95*, p.102503.

[47] Judijanto, L., Asfahani, A., Bakri, A.A., Susanto, E. and Kulsum, U., 2022. AI-Supported Management through Leveraging Artificial Intelligence for Effective Decision Making. *Journal of Artificial Intelligence and Development*, *1*(1), pp.59-68.

[48] Kandasamy, K., Srinivas, S., Achuthan, K. and Rangan, V.P., 2020. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*, pp.1-18.

[49] Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R., 2021. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, *9*, pp.121975-121995.

[50] Kitsios, F., Chatzidimitriou, E. and Kamariotou, M., 2022. Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in it consulting industry. *Sustainability*, *14*(3), p.1269.

[51] Kitsios, F., Chatzidimitriou, E. and Kamariotou, M., 2023. The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability*, *15*(7), p.5828.

[52] Kör, B. and Metin, B., 2021. Understanding human aspects for an effective information security management implementation. *International Journal of Applied Decision Sciences*, *14*(2), pp.105-122.

[53] Koza, E., 2022. Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security. *Med. Eng. Themes*, *2*, pp.26-39.

[54] Kurii, Y. and Opirskyy, I., 2022. Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013. *NIST Spec. Publ*, *800*(53), p.10.

[55] Kuzminykh, I., Ghita, B. and Such, J.M., 2021, August. The challenges with Internet of Things security for business. In *International Conference on Next Generation Wired/Wireless Networking* (pp. 46-58). Cham: Springer International Publishing.

[56] Lachaud, E., 2020. ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. *Eur. Data Prot. L. Rev.*, *6*, p.194.

[57] Maddireddy, B.R. and Maddireddy, B.R., 2022. Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), pp.270-285.

[58] Malatji, M., Marnewick, A.L. and Von Solms, S., 2022. Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security*, *30*(2), pp.255-279.

[59] Maleh, Y., Sahid, A., Alazab, M. and Belaissaoui, M., 2021. IT governance and information security: Guides, standards, and frameworks. CRC Press.

[60] Melaku, H.M., 2023. A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), pp.327-350.

[61] 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*, *68*(1), pp.87-100.

[62] Mullet, V., Sondi, P. and Ramat, E., 2021. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, *9*, pp.23235-23263.

[63] Onumo, A., Ullah-Awan, I. and Cullen, A., 2021. Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems (TMIS)*, *12*(2), pp.1-29.

[64] Pawlicka, A., Choraś, M. and Pawlicki, M., 2020, August. Cyberspace threats: not only hackers and criminals. Raising the awareness of selected unusual cyberspace actors-cybersecurity researchers' perspective. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-11).

[65] Pennekamp, J., Buchholz, E., Dahlmanns, M., Kunze, I., Braun, S., Wagner, E., Brockmann, M., Wehrle, K. and Henze, M., 2021. Collaboration is not evil: A systematic look at security research for industrial use. *arXiv preprint arXiv:2112.11417*.

[66] Perera, S., Jin, X., Maurushat, A. and Opoku, D.G.J., 2022, March. Factors affecting reputational damage to organisations due to cyberattacks. In *Informatics* (Vol. 9, No. 1, p. 28). MDPI.

[67] Petrunenko, I., 2022. Regulation of CyberSecurity of Ukraine's Critical Infrastructure: Legal Aspects and Standards of Sustainable Protection. *Law, Business and Sustainability Herald*, *2*(3), pp.42-57.

[68] Podrecca, M., Culot, G., Nassimbeni, G. and Sartor, M., 2022. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, p.103744.

[69] Podrecca, M., Culot, G., Nassimbeni, G. and Sartor, M., 2022. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, p.103744.

[70] Pomerleau, P.L. and Lowery, D.L., 2020. Countering Cyber Threats to Financial Institutions. In *A Private and Public Partnership Approach to Critical Infrastructure Protection*. Springer.

[71] Putra, D.S.K., Tistiyani, S. and Sunaringtyas, S.U., 2021, October. The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries. In *2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev)* (pp. 1-6). IEEE.

[72] Ramadhan, N. and Rose, U., 2022. Adapting ISO/IEC 27001 Information Security Management Standard to SMEs.

[73] Ramirez, A., Aiello, A. and Lincke, S.J., 2020, November. A survey and comparison of secure software development standards. In *2020 13th CMI Conference on Cybersecurity and Privacy (CMI)-Digital Transformation-Potentials and Challenges (51275)* (pp. 1-6). IEEE.

[74] Rodionova, Z. and Utepbergenov, I., 2020. The concept of adaptive information security management in digital organizations based on the analysis and monitoring of business processes. *Economic and Social Development: Book of Proceedings*, pp.409-415.

[75] Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data security. In *Data Ethics and Challenges* (pp. 41-59). Singapore: Springer Singapore.

[76] Sobb, T., Turnbull, B. and Moustafa, N., 2020. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), p.1864.

[77] Stapleton, J., 2021. Security without Obscurity: Frequently Asked Questions (FAQ). CRC Press.

[78] Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A. and Hutchison, D., 2022. A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection*, *37*, p.100505.

[79] Stevens, R., Dykstra, J., Everette, W.K., Chapman, J., Bladow, G., Farmer, A., Halliday, K. and Mazurek, M.L., 2020, February. Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards. In *NDSS*.

[80] Stewart, H., 2022. Security versus compliance: an empirical study of the impact of industry standards compliance on application security. *International Journal of Software Engineering and Knowledge Engineering*, *32*(03), pp.363-393.

[81] Sun, N., Li, C.T., Chan, H., Le, B.D., Islam, M.Z., Zhang, L.Y., Islam, M.R. and Armstrong, W., 2022. Defining security requirements with the common criteria: Applications, adoptions, and challenges. *IEEE Access*, *10*, pp.44756-44777.

[82] Sun, N., Li, C.T., Chan, H., Le, B.D., Islam, M.Z., Zhang, L.Y., Islam, M.R. and Armstrong, W., 2022. Defining security requirements with the common criteria: Applications, adoptions, and challenges. *IEEE Access*, *10*, pp.44756-44777.

[83] Susukailo, V., Opirsky, I. and Yaremko, O., 2021. Methodology of ISMS establishment against modern cybersecurity threats. In *Future Intent-Based Networking: On the QoS Robust and Energy Efficient Heterogeneous Software Defined Networks* (pp. 257-271). Cham: Springer International Publishing.

[84] Syafrizal, M., Selamat, S.R. and Zakaria, N.A., 2020. Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), pp.417-432.

[85] Taherdoost, H., 2022. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), p.2181.

[86] Tornjanski, V., Knežević, S., Ljubanić, D., Glišić, V., Žižić, D. and Travica, J., 2021, September. Towards secured digital business ecosystems: From threats to opportunities. In *E-business technologies conference proceedings* (Vol. 1, No. 1, pp. 1-14).

[87] Ukidve, A., Mantha, S.S. and Reddy, D.N., 2022. Analyzing Mapping of ISO 27001: 2013 Controls for Alignment with Enterprise Risks Management. *Asian Journal of Organic & Medicinal Chemistry*, *7*(2), pp.123-129.

[88] Viegas, V. and Kuyucu, O., 2022. International security standards. In *IT Security Controls: A Guide to Corporate Standards and Frameworks* (pp. 17-65). Berkeley, CA: Apress.

[89] Villela, M., Bulgacov, S. and Morgan, G., 2021. B Corp certification and its impact on organizations over time. *Journal of Business Ethics*, *170*, pp.343-357.

[90] Wang, W. and Yongchareon, S., 2020. Security-as-a-service: a literature review. *International Journal of Web Information Systems*, *16*(5), pp.493-517.

[91] Weil, T.R., 2020, October. Standards for Cloud Risk Assessments-What's Missing?. In *2020 IEEE Cloud Summit* (pp. 11-17). IEEE.

[92] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C. and Platts, J., 2022. Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), p.127.

[93] Yalcinkaya, E., Maffei, A., Akillioglu, H. and Onori, M., 2021. Empowering ISA95 compliant traditional and smart manufacturing systems with the blockchain technology. *Manufacturing review*, *8*, p.15.

[94] Yigit Ozkan, B., van Lingen, S. and Spruit, M., 2021. The cybersecurity focus area maturity (CYSFAM) model. *Journal of Cybersecurity and Privacy*, *1*(1), pp.119-139.

[95] Zamani, E., He, Y. and Phillips, M., 2020. On the security risks of the blockchain. *Journal of Computer Information Systems*, *60*(6), pp.495-506.

[96] Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., Parchure, A. and Luzcando, E., 2022. Practical adoption of cloud computing in power systems—Drivers, challenges, guidance, and real-world use cases. *IEEE Transactions on Smart Grid*, *13*(3), pp.2390-2411.

[97] Zhao, X., Castka, P. and Searcy, C., 2020. ISO standards: a platform for achieving sustainable development goal 2. *Sustainability*, *12*(22), p.9332.

[98] Zimmermann, V. and Renaud, K., 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, pp.169-187