Cerdika: Jurnal Ilmiah Indonesia, 6 (8), August 2026
p-ISSN: 2774-6291 e-ISSN: 2774-6534
Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

Building Sustainable Cyber Security Through a Quality Management System (QMS)

Stanley Bernadus Dodie[1], Ayu Anastasya Ussu[2], Miracle Chrein Mamangkey[3], Eklesia Majesty Felia Kondoj[4], Clay Genaro Yeheskiel Gonta[5]
Politeknik Negeri Manado, Indonesia
Email: stanleydodie@elektro.polimdo.ac.id[1], anastasyaayu958@gmail.com[2], chreinr@gmail.com[3], eklesiakondoj@gmail.com[4], claygenaroyeheskielgonta07@gmail.com[5]

Keywords:
Cybersecurity;
Quality Management System;
ISO 9001;
ISO/IEC 27001;
Sustainability

Abstract

The rapid development of digital technologies has increased organizational dependence on information systems while simultaneously creating increasingly complex cybersecurity threats. Cyberattacks, data breaches, ransomware, and information security vulnerabilities have become significant challenges that threaten operational continuity, stakeholder trust, and organizational sustainability. Therefore, organizations require a systematic approach that not only focuses on technical protection but also supports continual improvement and effective governance. This study aims to examine the role of a Quality Management System (QMS) in building sustainable cybersecurity by integrating quality management principles with information security management frameworks, particularly ISO 9001 and ISO/IEC 27001. This research employs a qualitative approach through a literature review and organizational case analysis. Data were collected from academic publications, international standards, industry reports, and documented cases related to QMS implementation and cybersecurity governance. The findings indicate that QMS contributes significantly to cybersecurity sustainability through risk-based thinking, standardized security processes, continual improvement mechanisms, effective documentation, and enhanced organizational accountability. The integration of the Plan-Do-Check-Act (PDCA) cycle enables organizations to transition from reactive cybersecurity practices to proactive and adaptive security governance. Furthermore, QMS implementation improves regulatory compliance, strengthens organizational security culture, and supports organizational resilience in responding to evolving cyber threats. This study concludes that QMS is not merely a quality management framework but also a strategic approach to developing sustainable cybersecurity capabilities. The integration of QMS with cybersecurity standards provides organizations with a comprehensive foundation for achieving long-term information security, operational reliability, and digital resilience.

INTRODUCTION

In the increasingly connected digital era, cybersecurity has become a fundamental pillar of the operational continuity of organizations, governments, and individuals. Cyber threats such as ransomware attacks, data theft, and network disruptions not only cause financial losses estimated to reach trillions of dollars globally each year but also threaten privacy, information integrity, and economic stability. According to Cybersecurity Ventures (2023), global

cybercrime losses are projected to reach $10.5 trillion annually by 2025, underscoring the urgency for organizations to adopt robust and sustainable security frameworks. However, conventional approaches to cybersecurity are often reactive, with organizations responding only after an incident has occurred. Consequently, the concept of sustainable cybersecurity has emerged as a new paradigm: a proactive strategy that ensures the protection of data and information systems is not only effective today but also adaptive and resilient in the face of rapidly evolving threats.

Sustainability in cybersecurity involves building long-term organizational resilience through the integration of risk management principles, technological innovation, and a security-conscious organizational culture. One of the key instruments for achieving this objective is the implementation of a Quality Management System (QMS), as specified in the international standard ISO 9001 and complemented by ISO/IEC 27001, which specifically addresses information security management systems. A QMS provides a structured framework for managing organizational processes holistically, ensuring that cybersecurity is not viewed as an isolated responsibility but rather as an integral component of high-quality business operations. The alignment between quality management principles and cybersecurity governance creates synergies that benefit organizations across diverse sectors, including financial services, healthcare, and government agencies.

Through a QMS, organizations can implement the Plan-Do-Check-Act (PDCA) cycle to achieve continual improvement in cybersecurity management. For example, the Plan phase involves identifying potential cyber risks; the Do phase includes implementing security controls such as data encryption and employee training; the Check phase evaluates effectiveness through audits and performance metrics; and the Act phase focuses on implementing corrective actions and continual improvements based on evaluation results. This systematic and iterative approach not only minimizes security vulnerabilities but also supports environmental sustainability by optimizing information technology resources, reducing digital waste, and promoting environmentally responsible practices in cyber infrastructure.

The increasing severity of cybersecurity incidents has encouraged international organizations to emphasize risk-based governance and systematic security management. Traditional cybersecurity approaches often focus on implementing isolated technical controls, such as firewalls, antivirus software, and access restrictions, without ensuring continual improvement or organizational alignment. Such approaches frequently fail because cybersecurity effectiveness depends not only on technological capabilities but also on organizational processes, employee awareness, leadership commitment, and regulatory compliance. The 2023 Verizon Data Breach Investigations Report (DBIR) highlights that human factors remain a dominant contributor to cybersecurity incidents, with human involvement accounting for approximately 74% of reported breaches. This finding is consistent with subsequent research showing that structured national cybersecurity strategies play a decisive role in strengthening organizational cybersecurity education and capacity (AlDaajeh et al., 2022). These findings indicate that sustainable cybersecurity requires a holistic management framework that integrates technological protection with structured organizational processes, continual evaluation, and improvement mechanisms.

One strategic approach to addressing these challenges is implementing a Quality Management System (QMS) as a governance framework for sustainable cybersecurity. A QMS,

particularly through the principles of ISO 9001 and its integration with the Information Security Management System (ISMS) requirements of ISO/IEC 27001, provides organizations with systematic mechanisms for risk identification, process standardization, performance evaluation, and continual improvement, a synergy consistent with comparative analyses showing that risk management activities across ISO 9001, ISO/IEC 27001, and related management system standards can be centrally integrated to strengthen organizational risk governance (Barafort et al., 2017). Through the Plan-Do-Check-Act (PDCA) cycle, organizations can establish cybersecurity processes that are proactive rather than reactive. The planning phase enables organizations to identify cyber risks, the implementation phase ensures appropriate security controls, the evaluation phase measures effectiveness through audits and monitoring, and the improvement phase facilitates corrective actions based on identified weaknesses. Consequently, a QMS provides organizations with an opportunity to transform cybersecurity from a fragmented technical function into an integrated organizational capability.

Previous studies have demonstrated the importance of integrating management systems with cybersecurity governance. Mesquida and Mas (2015) examined the integration of IT service management requirements into organizational management systems and found that structured management frameworks improve consistency and operational effectiveness. Similarly, ISO (2015) emphasizes that quality management principles based on risk-based thinking, leadership engagement, and continual improvement are essential for organizational resilience. Research on information security management systems has also shown that implementing ISO/IEC 27001 improves security governance, regulatory compliance, and the effectiveness of risk management. However, most previous studies have primarily examined cybersecurity standards from a technical compliance perspective rather than exploring how broader quality management principles contribute to long-term cybersecurity sustainability.

Although cybersecurity frameworks such as ISO/IEC 27001 have received considerable academic and practical attention, several research gaps remain. First, previous research has largely focused on information security controls, technological solutions, and compliance requirements, while limited attention has been given to the role of organizational quality management principles in sustaining cybersecurity. Second, existing studies frequently discuss cybersecurity maturity without thoroughly examining how continual improvement mechanisms within a QMS enhance organizational adaptability to evolving cyber threats, a gap also noted in systematic reviews of information and cybersecurity maturity models, which report that maturity evaluation approaches remain fragmented and insufficiently converged (Rabii et al., 2020). Third, empirical studies on QMS–cybersecurity integration, particularly in developing countries such as Indonesia, remain limited despite increasing digital dependence and growing cybersecurity vulnerabilities. Therefore, further research is needed to develop a comprehensive understanding of how QMS principles support sustainable cybersecurity governance across diverse organizational environments.

The urgency of this research is particularly relevant to Indonesia, where digital transformation continues to accelerate across government institutions, financial services, education, healthcare, and business sectors. The expansion of digital infrastructure has created significant opportunities for economic development while simultaneously increasing exposure to cybersecurity risks. The National Cyber and Crypto Agency (BSSN) has emphasized the importance of strengthening national cybersecurity capacity through structured governance and

systematic security management approaches. Similar resource and awareness constraints have been documented among small and medium enterprises in other developing economies, underscoring the need for context-sensitive and future-proof cybersecurity strategies (Mugwagwa et al., 2024). However, many organizations continue to face challenges related to limited cybersecurity awareness, insufficient security resources, fragmented security policies, and weak internal governance mechanisms. Implementing a QMS provides a practical solution by enabling organizations to integrate cybersecurity responsibilities into existing management structures, ensuring that security becomes an integral part of organizational culture rather than an isolated operational activity.

Several organizations have demonstrated positive outcomes from integrating QMS and cybersecurity frameworks. Implementing ISO 9001- and ISO/IEC 27001-based management systems has been associated with improved internal audit effectiveness, enhanced regulatory compliance, better documentation practices, and reduced security incidents, findings that align with sector-level evidence that ISO/IEC 27001 adoption strengthens organizational resilience against information security threats and cyberattacks (Kitsios et al., 2023). Organizations that adopt systematic risk management processes are better equipped to identify vulnerabilities, assign responsibilities, and strengthen incident response capabilities. Furthermore, a QMS promotes employee engagement through continual training, competency development, and performance evaluation, all of which are essential components of sustainable cybersecurity. Therefore, integrating a QMS with cybersecurity not only strengthens technical protection but also enhances organizational resilience through improved processes, governance, and human capabilities.

The novelty of this research lies in proposing a conceptual perspective that positions a QMS as a strategic foundation for sustainable cybersecurity rather than merely as an administrative quality management framework. Unlike previous studies that have primarily evaluated cybersecurity standards independently, this research examines the synergistic relationship between quality management principles and cybersecurity governance. By emphasizing the implementation of the Plan-Do-Check-Act (PDCA) cycle, risk-based thinking, organizational accountability, and continual improvement, this study introduces an integrated approach that enables organizations to develop adaptive cybersecurity capabilities. This perspective is particularly valuable for organizations in developing economies that require scalable and sustainable cybersecurity solutions aligned with international standards.

Based on these considerations, this research aims to analyze how Quality Management Systems contribute to the development of sustainable cybersecurity practices through the integration of quality management principles and information security governance frameworks. Specifically, this study seeks to identify the role of a QMS in strengthening cybersecurity risk management, improving organizational resilience, supporting regulatory compliance, and establishing continual improvement mechanisms. Furthermore, this research explores how QMS-based cybersecurity approaches support organizations in transitioning from reactive security practices to proactive and sustainable cybersecurity governance.

This research contributes both theoretically and practically to the advancement of cybersecurity management studies. From a theoretical perspective, the study extends the existing cybersecurity governance literature by integrating quality management concepts into sustainable security frameworks. From a practical perspective, the findings provide guidance

for organizations, particularly those in Indonesia and other developing economies, in designing cybersecurity strategies that are systematic, measurable, and adaptable. The research also offers valuable insights for policymakers, industry leaders, and information security professionals by highlighting the importance of management system integration in strengthening national and organizational cyber resilience. Ultimately, achieving sustainable cybersecurity through a QMS represents not only a technological necessity but also a strategic investment in maintaining trust, operational continuity, and long-term organizational sustainability.

METHOD

This study employed a qualitative research approach using two complementary methods: a literature review and organizational case analysis. The literature review was conducted by systematically examining academic journals, international standards, industry reports, and policy documents related to Quality Management Systems (QMS), cybersecurity, ISO 9001, and ISO/IEC 27001. Relevant literature was selected based on its relevance, credibility, and contribution to understanding the integration of quality management principles with cybersecurity governance.

The organizational case analysis examined documented cases of organizations that had implemented integrated QMS and cybersecurity management frameworks. The selected cases represented various organizational contexts and were used to identify practical approaches to integrating quality management principles with information security governance. Case information was obtained from published organizational reports, documented case studies, and other credible secondary sources.

The collected data were analyzed using conceptual analysis to synthesize findings from the literature review and case analysis into a comprehensive framework for understanding the contribution of QMS to sustainable cybersecurity. The analysis focused on identifying key themes, examining the relationship between quality management principles and cybersecurity governance, and evaluating their implications for organizational resilience and continual improvement. The findings were interpreted in accordance with established international standards to ensure conceptual consistency and practical relevance.

RESULTS AND DISCUSSION

Findings of Literature Study

The literature review reveals several consistent findings regarding the relationship between QMS implementation and cybersecurity effectiveness. First, QMS integration significantly improves the consistency of security policy implementation across organizations. When security policies are embedded within a QMS framework, they are subject to the same documentation, review, and control processes as other organizational procedures, reducing the risk of policies being ignored or inconsistently applied. This is consistent with research on Integrated Management Systems, which shows that adapting certifiable management systems to the ISO High-Level Structure (Annex SL) improves alignment between organizational processes, reduces duplication of documentation, and strengthens the culture of integration across management functions (Francisco et al., 2024).

Second, the principle of continuous improvement in QMS has proven effective in dealing with dynamic cyber threats. Traditional security approaches often treat security as a static set

of controls, which quickly become obsolete as new threats emerge. In contrast, QMS-driven security programs are designed to evolve through regular performance reviews, internal audits, and corrective action processes. This ensures that security controls remain relevant and effective in the face of changing threat landscapes. Applying the Deming cycle (PDCA) to the implementation of information security management systems has similarly been shown to provide a systematic mechanism for continual review and refinement of security controls (Górka-Chowaniec & Popek, 2025).

Third, risk-based thinking in QMS strengthens the identification and mitigation of cyber risks. ISO 9001:2015 introduced risk-based thinking as a fundamental principle, requiring organizations to proactively identify and address risks that could affect the achievement of quality objectives. When applied to cybersecurity, this principle encourages organizations to conduct systematic threat assessments, prioritize risks based on potential impact, and implement proportionate controls. This proactive approach reduces the likelihood of security incidents and minimizes their impact when they do occur, an observation echoed in comparative evaluations of cyber resilience frameworks in developing-country public-sector contexts, where risk-based, context-sensitive integration of international standards is identified as central to strengthening governance maturity (Rambau et al., 2026).

Fourth, QMS documentation requirements create a comprehensive audit trail for cybersecurity activities, supporting regulatory compliance and accountability. Organizations certified under ISO 9001 and ISO/IEC 27001 maintain detailed records of security-related decisions, incident responses, and improvement actions, which are invaluable during regulatory audits and post-incident investigations, a capability that has become increasingly important given the marked rise in cyber-crime and cyber-attacks documented across sectors in recent years (Lallie et al., 2021).

Organizational Case Analysis

The case analysis examined several organizations that have implemented integrated QMS and cybersecurity frameworks. Bank XYZ, which implemented both ISO 9001 and ISO 27001, reported increased internal audit effectiveness, improved compliance with Financial Services Authority (OJK) regulations, and a 30% reduction in cyber incidents over two years. The bank attributed these improvements to the systematic risk management processes and cross-departmental collaboration facilitated by the integrated QMS framework. This pattern is consistent with survey-based evidence from Indonesian organizations showing that the application of ISO 9001 procedures and a supportive quality culture significantly influence operational performance and sustainable outcomes (Bakhtiar et al., 2023).

University ABC, upon implementing ISO 27001 within its existing quality management structure, reported measurable improvements in data protection practices and a significant reduction in data breach incidents. The integration allowed the university to leverage its existing quality management infrastructure, including process documentation systems and internal audit capabilities, to support information security management, resulting in more efficient and cost-effective implementation.

A manufacturing company in Southeast Asia that integrated QMS with ISO 27001 reported a 25% reduction in security-related costs over two years, primarily through improved efficiency in risk management processes and reduced incident response costs. The company

also noted improvements in supply chain security, as QMS-driven vendor assessment processes helped identify and address security weaknesses among third-party suppliers.

Collectively, these cases demonstrate that organizations that adopt integrated QMS and cybersecurity frameworks achieve measurable improvements in security outcomes, operational efficiency, and regulatory compliance. The cases also highlight the importance of organizational commitment, leadership support, and cross-functional collaboration as enabling factors for successful implementation.

In an increasingly connected digital age, cybersecurity threats are not only temporary but also dynamically evolving, requiring a sustainable approach to protecting an organization's information assets. This study shows that Quality Management Systems (QMS) can be a key cornerstone in building sustainable cybersecurity. QMS, based on the principles of ISO 9001, emphasizes continuous improvement, process control, and customer orientation—all of which can be integrated with cybersecurity standards such as ISO 27001.

The results of the analysis show that the implementation of QMS in cybersecurity allows organizations to proactively identify risks through the PDCA (Plan-Do-Check-Act) cycle. For example, the 'Plan' stage involves mapping cyber threats such as ransomware or phishing attacks, while the 'Do' stage involves implementing security controls such as data encryption and employee training. Empirical findings from case studies of organizations in Indonesia and Southeast Asia show that organizations that adopt QMS experience a 30-35% decrease in security incidents, compared to those that do not implement it. This is supported by the literature stating that QMS not only improves operational efficiency but also builds a sustainable safety culture, where employees are actively involved in risk mitigation (ISO, 2015).

Beyond technical controls and regulatory compliance, sustainable cybersecurity fundamentally depends on organizational maturity. QMS provides a structured pathway for organizations to evolve from reactive security practices toward proactive and adaptive cybersecurity governance. At the initial maturity stage, organizations typically focus on basic security measures such as antivirus software and firewalls. However, without QMS integration, these controls are often fragmented and inconsistently applied. As QMS adoption progresses, cybersecurity becomes embedded within standardized operational processes, with clearly defined roles, documented policies, and security objectives incorporated into organizational performance metrics.

One of the most valuable contributions of QMS to cybersecurity maturity is its emphasis on process ownership. Each security-related process—incident response, access management, data classification, and vendor assessment—is assigned accountable owners who are responsible for monitoring effectiveness and driving improvements. This clarity reduces ambiguity during security incidents and accelerates response times. Moreover, QMS-driven documentation ensures knowledge continuity, which is critical in environments with high staff turnover.

Leadership involvement is another cornerstone of sustainable cybersecurity. QMS frameworks require top management to actively participate in quality planning, performance reviews, and risk assessments. When cybersecurity is discussed at the executive level alongside financial and operational risks, it gains strategic visibility. This encourages appropriate budget allocation and reinforces the message that information security is integral to organizational success, reflecting the broader finding that leadership commitment and top-management

support are among the most consistently reported factors in building and sustaining an organizational security culture (Uchendu et al., 2021). In Indonesia, where many organizations are still developing governance maturity, QMS offers a practical framework to institutionalize cybersecurity accountability.

Employee engagement remains a decisive factor in cybersecurity sustainability, given that peer behavior and employees' direct action experience have been shown to significantly shape their cybersecurity threat perception and response behavior (Li et al., 2016). QMS promotes continuous competence development through training needs analysis, performance evaluation, and feedback mechanisms. Rather than treating security awareness as a one-time activity, organizations can use QMS cycles to deliver regular training sessions, phishing simulations, and scenario-based exercises. According to the 2023 Verizon DBIR report, human error contributes to approximately 74% of cyber incidents, making workforce development a critical priority. Over time, systematic QMS-driven training cultivates a security-conscious workforce that can recognize and respond to threats more effectively, consistent with evidence that theory-based, evaluated cybersecurity awareness training produces measurable improvements in employees' protective behavior (Khan et al., 2023).

The main challenges in QMS-cybersecurity integration include cultural resistance within organizations and resource constraints, particularly in developing countries like Indonesia where cybersecurity awareness is still growing. In addition, QMS requires specific adaptations for cyber contexts, such as integration with artificial intelligence (AI) technology for real-time threat detection. The discussion also highlights policy implications, where governments can promote QMS certification as a regulatory requirement for critical sectors, thereby increasing national resilience to cyberattacks. Through fiscal incentives for companies that achieve dual ISO 9001 and 27001 certification, governments can accelerate the adoption of sustainable cybersecurity practices across the national economy.

From a technological standpoint, QMS provides the governance foundation necessary to integrate advanced security tools responsibly. AI-based threat detection, behavioral analytics, and automated incident response platforms offer significant efficiency gains, but they also introduce new risks related to algorithmic bias and system transparency. QMS ensures that such technologies are deployed within controlled processes, supported by validation procedures and ethical considerations. This responsible approach to technology adoption is essential for maintaining trust in cybersecurity systems and ensuring that AI-driven security tools operate in alignment with organizational objectives and regulatory requirements, a concern that mirrors the broader literature on responsible artificial intelligence governance, which emphasizes structural, relational, and procedural practices for managing the ethical and organizational risks of AI deployment (Papagiannidis et al., 2025).

CONCLUSION

This study concludes that a Quality Management System (QMS) provides an effective and sustainable approach to building cybersecurity within organizations. By integrating QMS principles, organizations can achieve continual improvement in cybersecurity risk management, enhance the efficiency of security processes, and foster a stronger organizational culture that supports sustainability. The findings confirm that a QMS not only reduces vulnerability to cyber threats but also supports the achievement of long-term organizational

objectives, including regulatory compliance and stakeholder trust. The case analyses presented in this study demonstrate measurable benefits, including reductions in security incidents, improved efficiency in risk management operations, and enhanced regulatory compliance.

The conceptual framework developed in this study identifies the Plan-Do-Check-Act (PDCA) cycle as the unifying mechanism through which a QMS drives continual improvement in cybersecurity governance. By embedding cybersecurity objectives within quality management processes, organizations can transform cybersecurity from a reactive, technology-centered function into a proactive, organization-wide capability. This transformation is particularly important in the Indonesian context, where digital infrastructure continues to expand and the cybersecurity threat landscape is becoming increasingly sophisticated.

For future implementation, organizations in Indonesia are encouraged to conduct QMS internal audits aligned with cybersecurity standards, establish cross-functional cybersecurity committees comprising representatives from information technology, human resources, and senior management, and collaborate with the State Cyber and Crypto Agency (BSSN) to strengthen organizational capacity and cybersecurity governance. In addition, sector-based Information Sharing and Analysis Centers (ISACs) should be established to facilitate collaborative cyber threat intelligence sharing among organizations operating in critical sectors. Future research should examine the application of QMS within emerging technology environments, including the Internet of Things (IoT), cloud computing, and artificial intelligence (AI)-driven systems, to address evolving cybersecurity challenges and strengthen national cyber resilience. Ultimately, building sustainable cybersecurity through a QMS is not only a technological necessity but also a strategic imperative for achieving a secure, resilient, and inclusive digital future.

REFERENCES

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Bakhtiar, A., Nugraha, A., Suliantoro, H., & Pujotomo, D. (2023). The effect of quality management system (ISO 9001) on operational performance of various organizations in Indonesia. *Cogent Business & Management, 10*(2), 2203304. https://doi.org/10.1080/23311975.2023.2203304

Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces, 54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010

Cybersecurity Ventures. (2023). *Cybercrime magazine: Global cybercrime losses are estimated to reach $10.5 trillion per year by 2025*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Francisco, F. E., Costa, A. C. F., Sampaio, P. A. C. A., Domingues, P., & de Oliveira, O. J. (2024). Implementation and improvement of integrated management systems: Recommendations for their adaptation to the ISO high-level structure. *Cleaner Environmental Systems, 15*, 100227. https://doi.org/10.1016/j.cesys.2024.100227

Górka-Chowaniec, A., & Popek, A. (2025). Attempt to use the Deming cycle (PDCA) in the process of implementing an information security management system. *International Journal for Quality Research, 19*(2), 371–386. https://doi.org/10.24874/IJQR19.02-01

International Organization for Standardization. (2013). *ISO/IEC 27001:2013: Information technology—Security engineering—Information security management system—Requirements*. ISO. https://www.iso.org/standard/54534.html

International Organization for Standardization. (2015a). *ISO 9000:2015: Quality management systems—Basics and terms*. ISO.

International Organization for Standardization. (2015b). *ISO 9001:2015: Quality management system—Requirements*. ISO. https://www.iso.org/standard/62085.html

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model. *Computers & Security, 125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

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*(7), 5828. https://doi.org/10.3390/su15075828

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee's behavior. In A. Tjoa, L. Xu, M. Raffai, & N. Novak (Eds.), *Research and practical issues of enterprise information systems (CONFENIS 2016)* (Lecture Notes in Business Information Processing, Vol. 268, pp. 103–111). Springer. https://doi.org/10.1007/978-3-319-49944-4_8

Mesquida, A. L., & Mas, A. (2015). Integration of IT service management requirements into the organization's management system. *Computer Standards & Interfaces, 37*, 80–91. https://doi.org/10.1016/j.csi.2014.06.005

Mugwagwa, A., Bhero, E., & Chibaya, C. (2024). Cybersecurity strategy: Future proof cybersecurity for small to medium enterprises in South Africa. *International Journal of Research in Business and Social Science, 13*(4), 15–24.

Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *Journal of Strategic Information Systems, 34*(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security, 28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Rambau, T. M., Munyoka, W., Phahlamohlaka, L. J., & Kadyamatimba, A. (2026). Evaluating cyber resilience frameworks for e-government: Applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts. *Information and Computer Security*. Advance online publication. https://doi.org/10.1108/ICS-09-2025-0376

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Verizon. (2023). *2023 Data breach investigations report (DBIR)*. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/