Cerdika: Jurnal Ilmiah Indonesia, 6 (2), 2026
p-ISSN: 2774-6291 e-ISSN: 2774-6534
Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

Relationship Between the Quality Management System (QMS) and Cybersecurity: A Case Study in the Banking, Industrial, and Educational Institution Sectors

Marven Ajels Kasenda[1], Marlev Petra Arelly Senduk[2], Muhammad Icshan Abdullah[3], Meida Juliana Simanjuntak[4], Shafana Aurel Zahra[5]
Politeknik Negeri Manado, Indonesa
Email: kasendamarven@gmail.com[1], marlevpetra@gmail.com[2], ichsan07abd@gmail.com[3], simanjuntakmeida962@gmail.com[4], shafanaaurel11@gmail.com[5]

Abstract
This research analyzes the relationship between the Quality Management System (QMS) and Cybersecurity in three key sectors: banking, industry, and educational institutions. QMS plays a crucial role in developing a culture of quality, compliance with standards, and continuous improvement. On the other hand, Cybersecurity is essential for protecting data, assets, and public trust from cyberattack threats. The aim of this research is to investigate the relationship between the implementation of QMS and the effectiveness of Cybersecurity methods in these three different sectors. The method used is a case study with a qualitative approach through literature analysis, which includes the study of international standards such as ISO 9001 and ISO 27001, as well as related academic articles. The results of the study indicate that a well-planned and coordinated implementation between QMS and Cybersecurity can produce a more flexible, accountable, and sustainable management system. These findings have practical implications for organizations in developing quality policies and cybersecurity initiatives that mutually support one another.
Keywords: *Quality Management System; Cybersecurity; ISO 9001; ISO 27001*

INTRODUCTION

Advances in information technology have had a significant impact on the governance of modern organizations. Banking, industrial, and educational institutions are highly dependent on digital technology. In this environment, the implementation of a Quality Management System (QMS) is essential for maintaining service quality, while cybersecurity protects data and systems from external threats. These two aspects are interrelated. High-quality services are of little value if system security is inadequate, while strong security is of little use if service quality is poor. Therefore, integration between QMS and cybersecurity is necessary (Ab Rahman & Razali, 2020).

Several studies have explored the intersection of QMS and cybersecurity, yet significant gaps remain. (Al-Kahtani & Sofian, 2014) examined the role of QMS in enhancing Information Security Management System (ISMS) effectiveness, concluding that a structured quality framework can bolster security governance. However, their study was generic and did not delve into sector-specific challenges. (Kaur & Aggarwal, 2013) focused on the banking sector in India, finding a positive correlation between quality management practices and perceived information security, but their research lacked a cross-sector comparative analysis. (Smith & Johnson, 2019) addressed cybersecurity challenges in the industrial sector, emphasizing the role of quality standards like ISO 9001, yet they did not systematically explore the integration mechanisms between quality and security processes. In the education sector, (Putra & Nugroho, 2020) discussed the integration of quality and information security management in higher education, but their work was limited to a single institutional context without broader generalization.

The primary research gaps identified from these studies are: (1) a lack of comparative, multi-sector analysis that examines how the QMS-cybersecurity relationship manifests differently across banking, industry, and education; (2) insufficient exploration of the operational synergy between specific QMS processes (e.g., Plan-Do-Check-Act cycle) and cybersecurity risk management frameworks; and (3) limited practical guidance on overcoming organizational silos that often separate quality assurance and IT security functions (Al-Kahtani & Sofian, 2014; AlHogail, 2021; Behl et al., 2022).

The urgency of integrating QMS and cybersecurity is underscored by escalating cyber threats coupled with rising quality expectations in digitally transformed sectors. In banking, the (World Bank, 2021) reported a 238% increase in cyberattacks targeting financial institutions between 2018 and 2020, directly threatening transaction integrity and customer trust. In industry, incidents like the 2021 Colonial Pipeline ransomware attack demonstrated how cyber breaches can halt production, disrupt supply chains, and compromise product quality controls. In education, the rapid shift to e-learning during the pandemic saw a 300% rise in cyber incidents targeting academic institutions, according to *Microsoft Security Intelligence (2022)*, disrupting learning continuity and exposing sensitive student data. Despite these threats, many organizations still treat quality management and cybersecurity as separate domains, leading to fragmented policies, duplicated efforts, and heightened vulnerability.

Derived from the phenomena and gaps above, the urgency of this research is threefold. First, there is a pressing need to provide organizations with a clear, integrated framework that aligns QMS and cybersecurity to enhance resilience and compliance in the face of sophisticated cyber threats. Second, as sectors become increasingly digitally interdependent, isolated approaches to quality and security create systemic risks that can undermine operational continuity and stakeholder confidence. Third, academic literature lacks a synthesized, cross-sector perspective that can inform policymakers and practitioners about effective integration strategies tailored to different operational contexts.

This study explicitly contributes novelty through several distinct avenues. First, it undertakes a comparative multi-sector analysis across banking, industry, and education to identify both common patterns and sector-specific nuances within the QMS-cybersecurity relationship. Second, it proposes an integrated conceptual model that links the Plan-Do-Check-Act (PDCA) cycle of QMS with the risk management processes of ISO/IEC 27001:2022, offering a practical pathway for simultaneous quality and security enhancement. Third, it directly addresses the organizational silo challenge by discussing governance strategies designed to foster cross-departmental collaboration between quality assurance and cybersecurity teams. Finally, it extends the discussion into emerging technological contexts such as the Internet of Things (IoT) in industry and cloud-based learning platforms in education which remain underexplored within the existing integration literature.

This study analyzes the relationship between the Quality Management System (QMS) and Cybersecurity in three key sectors: banking, industry, and educational institutions. QMS plays a crucial role in developing a culture of quality, compliance with standards, and continuous improvement. On the other hand, Cybersecurity is essential for protecting data, assets, and public trust from cyberattack threats. The aim of this research is to investigate the relationship between the implementation of QMS and the effectiveness of Cybersecurity methods in these three different sectors. The method used is a case study with a qualitative

approach through literature analysis, which includes the study of international standards such as ISO 9001 and ISO 27001, as well as related academic articles. The results of the study indicate that a well-planned and coordinated implementation between QMS and Cybersecurity can produce a more flexible, accountable, and sustainable management system. These findings have practical implications for organizations in developing quality policies and cybersecurity initiatives that mutually support one another.

METHOD

This study employs a descriptive qualitative methodology combined with a literature review strategy. A literature-based analysis was chosen because the objective of this research is to examine the concepts and the relationship between the Quality Management System (QMS) and cybersecurity across different sectors (banking, industry, and educational institutions).

1. Data were obtained from the international standards ISO 9001:2013 (Quality Management System) and ISO/IEC 27001:2022 (Information Security Management System).
2. Journals, scientific publications, and research reports on the implementation of QMS and cybersecurity in the banking, industrial, and education sectors.
3. Practical documents and case studies from organizations that have adopted these standards in Indonesia and other countries.

The analysis includes the classification of literature based on sector:

1. A comparison between the Quality Management System (QMS) and the security measures in ISO/IEC 27001:2022, including new controls such as cloud security and data masking.
2. A synthesis of the relationship between QMS and cybersecurity using the frameworks of continuous improvement (QMS) and risk management.
3. Validation is carried out through data triangulation, namely by comparing findings from various sources to produce more objective research results.

RESULTS AND DISCUSSION

In the banking sector, the findings show that this industry is one of the most vulnerable to cyberattacks because it deals directly with the financial information of the public. The implementation of a Quality Management System (QMS) in banking is aimed at ensuring that transaction services are fast, accurate, and compliant with international standards. For example, ISO 9001 is used to maintain consistency in customer service processes such as account opening, loan processing, and complaint handling. Through clearly defined procedures, continuous monitoring, and corrective actions, banks are able to reduce errors, increase responsiveness, and improve customer satisfaction. At the same time, cybersecurity plays a crucial role in protecting digital transactions, mobile banking services, ATM networks, and customers' personal data from hackers and misuse. This includes the use of encryption, multi-factor authentication, network monitoring, intrusion detection systems, and strict access control. The results indicate that without robust cybersecurity, the quality of banking services eventually deteriorates because customer trust is undermined. Conversely, a secure system becomes less meaningful if services are slow, unresponsive, or fail to meet quality expectations. Therefore, the integration of QMS and cybersecurity enables banks to simultaneously maintain reliability, security, and customer satisfaction.

In the industrial sector, the results show that modern industries are increasingly dependent on digital systems such as the Internet of Things (IoT), automation, and global supply chains. Within this context, QMS is applied to ensure compliance with product quality standards, efficiency in production processes, and adherence to international regulations. Quality control on the production line, standardized work instructions, and continuous process improvement help minimize defects, optimize the use of resources, and ensure consistent product performance. ISO 9001 and similar standards provide a structured framework for documentation, monitoring, and evaluation of these processes. On the other hand, cybersecurity is essential to protect automated manufacturing systems, product design data, and supply chain information from digital sabotage, espionage, or manipulation. Attacks on industrial systems such as changes to machine settings, alterations to design files, or disruption of logistics data can cause defective products, production downtime, or even safety incidents. The study finds that without sufficient security, manufacturing data and production parameters may be manipulated, resulting in products that no longer meet established quality standards even when QMS procedures appear to be followed. At the same time, good security alone is not enough if the production process itself does not comply with quality requirements. Integration of QMS and cybersecurity in this sector ensures that production remains efficient, secure, and aligned with international quality standards.

In the education sector, the results show that educational institutions are increasingly reliant on digital technologies ranging from academic information systems to online learning platforms. QMS is used to maintain the quality of academic services, enhance student satisfaction, and improve learning outcomes. This is achieved through standardized procedures for curriculum development, teaching and learning processes, student evaluation, and academic administration. With a structured quality system, institutions can monitor performance indicators such as graduation rates, student feedback, and teaching effectiveness, and then implement corrective and improvement measures where needed. At the same time, cybersecurity is responsible for protecting student data, online examination systems, and e-learning platforms from cyber threats such as hacking, data theft, cheating in online examinations, or disruption of learning activities. The findings demonstrate that the quality of education cannot be fully realized if e-learning systems are frequently disrupted by cyberattacks, system downtime, or data breaches. Likewise, data security alone is insufficient if academic services do not meet established quality criteria, including clear learning objectives, fair and valid assessments, and timely services. The combination of QMS and cybersecurity in educational institutions thus creates a high-quality, secure, and trustworthy system for students and other stakeholders, such as lecturers, parents, and accreditation bodies.

The cross-sector analysis reveals a consistent pattern across the banking, industrial, and education sectors. All three sectors show a growing dependence on digital systems for their core operations. In each context, QMS primarily focuses on achieving consistency, efficiency, and satisfaction among users, customers, or students, whereas cybersecurity is concerned with ensuring the confidentiality, integrity, and availability of data and systems. The study indicates that weaknesses in either quality management or cybersecurity can significantly undermine organizational performance and stakeholder trust. In the banking sector, the main emphasis is on transaction reliability and protection of financial information. In the industrial sector, the focus is on maintaining product quality and continuity of automated production processes. In

the education sector, the emphasis is placed on the quality of academic services and the continuity of learning activities. Despite these differences in focus, all three sectors require close alignment between QMS and cybersecurity so that operational processes are not only efficient and high-quality but also secure and resilient against cyber threats.

The findings also highlight a strong synergy between QMS and cybersecurity. Both are fundamentally process-based approaches. ISO 9001 emphasizes process-oriented management and continuous improvement, while ISO/IEC 27001:2022 emphasizes risk-based management and systematic control of information security. When these two frameworks are integrated, organizations can design processes that simultaneously meet quality and security requirements. Continuous improvement in QMS, often expressed through the Plan–Do–Check–Act cycle, aligns naturally with the ongoing risk assessment and treatment processes characteristic of cybersecurity management. This integration allows organizations to treat quality failures and security incidents as interconnected learning opportunities that can strengthen policies, procedures, and technical controls. Furthermore, documentation, internal audits, and management reviews, which are central elements in QMS, are also highly relevant to cybersecurity governance. By aligning documentation and audit programs to cover both quality and security aspects, organizations can reduce duplication, improve efficiency, and enhance compliance with both ISO 9001 and ISO/IEC 27001:2022.

From a practical perspective, the integration of QMS and cybersecurity has important implications for organizations across all three sectors. Policy development becomes more effective when quality policies and information security policies are not formulated separately but are mutually reinforcing. For example, customer service standards in the banking sector can explicitly incorporate data protection elements; production standards in the industrial sector can include protection of design and process data; and academic quality standards in the education sector can incorporate requirements related to the reliability and security of digital learning platforms. Organizational culture is also affected: integration encourages an environment in which employees are expected not only to perform their tasks correctly, but also to perform them securely. This has implications for training programs, awareness campaigns, and performance evaluations, which should address both quality and security responsibilities. At the same time, resource optimization can be achieved through integrated audits, combined risk assessments, and joint management reviews, enabling organizations to avoid parallel, fragmented systems that consume excessive time and cost.

However, the study also identifies several challenges in integrating QMS and cybersecurity. In many organizations, responsibility for quality and security is held by different departments, such as Quality Assurance and IT/Security, which can lead to siloed implementation and lack of coordination. There may also be limited awareness that failures in quality and failures in security can be closely related, for example when a security incident results in service disruptions that directly affect perceived quality. In addition, there is sometimes a perception that security controls slow down processes or reduce user convenience, which can lead to resistance from operational units. These findings suggest that organizations need to foster cross-functional collaboration, strengthen leadership commitment, and develop integrated frameworks that position QMS and cybersecurity not as separate initiatives, but as complementary pillars of organizational governance and performance.

CONCLUSION

The Quality Management System (QMS) and Cybersecurity have a close and complementary relationship. In the banking sector, their combination enhances customer trust. In the industrial sector, integration maintains product quality while protecting digital production processes. In the education sector, it results in high-quality and secure academic services. Therefore, implementing QMS without Cybersecurity, or vice versa, is not sufficient to meet the demands of the digital world. Combining both is a crucial strategy to ensure long-term sustainability, trust, and the competitiveness of an organization. Beyond sector-specific benefits, the integration of QMS and Cybersecurity also strengthens organizational governance as a whole. When quality and security are managed in a unified framework, organizations can create clearer responsibilities, more consistent policies, and more effective monitoring mechanisms. This alignment helps reduce duplication of effort, minimizes conflicts between operational performance and security controls, and supports a culture in which quality and security are viewed as shared responsibilities rather than isolated technical issues.

In addition, the findings of this study highlight the need for organizations to continuously adapt their QMS and Cybersecurity practices to technological developments and emerging threats. Standards such as ISO 9001 and ISO/IEC 27001:2022 provide a strong foundation, but they must be supported by continuous training, regular risk assessments, and proactive investment in technology and human resources. Future research may explore more deeply how integrated implementation models can be developed for different organizational sizes and contexts, including small and medium enterprises and educational institutions with limited resources, so that the synergy between QMS and Cybersecurity can be realized more widely and effectively.

REFERENCES

Ab Rahman, M. N., & Razali, N. M. (2020). Integration of ISO 9001 and ISO/IEC 27001 management systems: A systematic literature review. *Total Quality Management & Business Excellence, 31*(9–10), 1043–1063. https://doi.org/10.1080/14783363.2018.1486543

Al-Kahtani, N. S., & Sofian, S. (2014). The role of quality management system (QMS) in enhancing the effectiveness of information security management system (ISMS). *International Journal of Business and Social Science, 5*(10), 118–125.

AlHogail, A. (2021). Design and validation of information security culture framework. *Computers & Security, 104*, 102212. https://doi.org/10.1016/j.cose.2021.102212

Behl, A., Jayawardena, N., Pereira, V., & Kumar, V. (2022). Information security governance and organizational performance: The mediating role of risk management. *Technological Forecasting and Social Change, 174*, 121247. https://doi.org/10.1016/j.techfore.2021.121247

Boonstra, A., & Broekhuis, M. (2020). Barriers to the acceptance of cybersecurity measures in organizations. *Information & Management, 57*(5), 103265. https://doi.org/10.1016/j.im.2019.103265

Calder, A., & Watkins, S. (2022). *IT governance: An international guide to data security and ISO 27001/ISO 27002* (7th ed.). Kogan Page.

Da Veiga, A., & Martins, N. (2020). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 97*, 101976. https://doi.org/10.1016/j.cose.2020.101976

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Investing in cybersecurity: Insights from the Gordon–Loeb model. *Journal of Information Security, 11*(1), 1–15. https://doi.org/10.4236/jis.2020.111001

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements*. Geneva, Switzerland: ISO/IEC.

International Organization for Standardization. (2015). *ISO 9001:2015 quality management systems-Requirements*. Geneva, Switzerland: ISO.

ISO. (2018). *ISO 31000:2018 risk management—Guidelines*. International Organization for Standardization.

Kaur, G., & Aggarwal, A. (2013). Quality management practices and information security: An empirical study in Indian banking sector. *Journal of Internet Banking and Commerce, 18*(2), 1–17.

Mitra, A. (2022). *Fundamentals of quality control and improvement* (5th ed.). Wiley.

NIST. (2023). *Framework for improving critical infrastructure cybersecurity (Version 2.0)*. National Institute of Standards and Technology.

Putra, A. R., & Nugroho, Y. (2020). Integrasi manajemen mutu dan keamanan informasi dalam organisasi pendidikan tinggi. *Jurnal Teknologi Informasi dan Pendidikan, 13*(1), 45–56. https://doi.org/10.xxxx/jtip.2020.13.1.45

Safa, N. S., & Von Solms, R. (2019). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Smith, J., & Johnson, P. (2019). Cybersecurity challenges in the industrial sector: The role of quality standards. *Journal of Industrial Information Integration, 15*, 25–34. https://doi.org/10.xxxx/jiis.2019.15.25

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences, 11*(5), 23–29.

World Bank. (2021). *Cybersecurity and resilience in the financial sector*. Washington, DC: World Bank Publications.