Cerdika: Jurnal Ilmiah Indonesia, 6 (7), July 2026
p-ISSN: 2774-6291 e-ISSN: 2774-6534
Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

Implementation of Quality Management System (QMS) in Enhancing Cybersecurity Governance in Organizations

Deitje Sofie Pongoh*, Ahmad Syarif Abdul Kader, Renaldi Gilang Pratama, Theola Trixie Silfia Rapithan, Zahara Mifta Luve
Politeknik Negeri Manado, Indonesia
Email: pongohdeitje@gmail.com*, theolaraphitan@gmail.com, naldygilangpratama@gmail.com, zaharalufve7@gmail.com, syehahmadkader@gmail.com

Keywords:
Quality Management System (QMS); Cybersecurity Governance, ISO 9001:2015, ISO/IEC 27001

Abstract
The rapid advancement of digital transformation has led organizations to become increasingly dependent on information governance and digital infrastructure. This dependency introduces potential risks in the form of cybersecurity threats that can disrupt business continuity, damage organizational reputation, and cause financial losses. To address these challenges, the implementation of a Quality Management System (QMS) can provide a structured framework for enhancing cybersecurity governance. This research aims to analyze the role of QMS in strengthening cybersecurity governance in organizations. The approach used was descriptive qualitative through case studies, document analysis, and expert interviews. The results show that integrating QMS principles such as continuous improvement, risk-based thinking, and stakeholder engagement into cybersecurity management significantly enhances organizational resilience against cyber threats. Additionally, the study identifies that alignment between ISO 9001:2015 (QMS standard) and ISO/IEC 27001 (Information Security Management System/ISMS) produces an effective governance framework. This alignment enables organizations to establish standardized processes, improve regulatory compliance, and foster a culture of security awareness among employees. The study concludes that QMS implementation is not only beneficial for quality assurance but also serves as a primary driver for effective cybersecurity governance. It is recommended that organizations adopt an integrated management approach that combines QMS and ISMS to achieve sustainable security governance.

INTRODUCTION

A Quality Management System (QMS) is a structured framework consisting of documented policies, processes, and procedures that enables an organization to consistently meet customer expectations, regulatory requirements, and the needs of other stakeholders (Agmon & Kordova, 2024; Ali, 2023; Bouchetara et al., 2022; Ferreira et al., 2025; Mohammad et al., 2024; Reinhardt et al., 2026). The most widely adopted international standard for QMS is ISO 9001, which has undergone continuous development since its initial publication in 1987, with ISO 9001:2015 representing its latest major revision. This standard is built upon seven quality management principles, namely customer focus, leadership, engagement of people, process approach, continuous improvement, evidence-based decision making, and relationship management (Buckė et al., 2022; Iqbal et al., 2025; Kayani et al., 2025; Myeda et al., 2023; Qureshi, 2024; Ranjith Kumar et al., 2022). Customer focus emphasizes understanding and fulfilling customer needs to achieve long-term satisfaction. Leadership ensures that

organizational leaders establish a clear vision, strategic direction, and supportive environment. Engagement of people encourages active participation and competence across all organizational levels, while the process approach promotes the management of activities as interconnected processes to improve efficiency and effectiveness. Continuous improvement fosters innovation and sustainable organizational development, evidence-based decision making ensures that managerial decisions rely on accurate and reliable information, and relationship management strengthens mutually beneficial partnerships with customers, suppliers, regulators, and other stakeholders. Although QMS was initially developed for manufacturing industries to ensure consistent product quality, its principles have since been widely implemented across various sectors, including services, healthcare, education, and information security, demonstrating its flexibility and broad applicability in improving organizational performance.

Cybersecurity governance represents a critical component of information technology governance that focuses on the strategic management of cybersecurity risks across an organization (Agarwal & Shah, 2024; Kehinde, n.d.; Mızrak, 2023; Oh et al., 2025; Savaş & Karataş, 2022; Shaikh & Siponen, 2023). According to the National Institute of Standards and Technology (NIST), cybersecurity governance encompasses a comprehensive framework of policies, risk management practices, organizational structures, and control mechanisms designed to safeguard information assets and ensure business continuity. Effective cybersecurity governance consists of several essential elements, including policy and regulatory frameworks, cyber risk management, clearly defined roles and responsibilities, organizational awareness and security culture, and continuous monitoring and evaluation. Policy and regulatory frameworks establish internal security standards while ensuring compliance with external legal and regulatory requirements. Cyber risk management involves identifying, assessing, mitigating, and continuously monitoring cybersecurity risks that may threaten organizational operations. Clearly defined roles and responsibilities ensure accountability and effective coordination among management, IT personnel, and other stakeholders. Organizational awareness and security culture encourage employees at every level to adopt secure behaviors and recognize cybersecurity as a shared responsibility. Continuous monitoring and evaluation, through mechanisms such as security audits, penetration testing, performance measurement, and incident reporting, enable organizations to assess the effectiveness of implemented security controls. Consequently, robust cybersecurity governance not only reduces the likelihood of cyber incidents but also strengthens an organization's ability to respond rapidly and recover effectively following cybersecurity breaches.

The integration of Quality Management Systems with cybersecurity governance provides organizations with a structured and systematic approach to managing information security while continuously improving organizational performance. One of the primary contributions of QMS is its emphasis on risk-based thinking, a principle embedded in ISO 9001:2015 that encourages organizations to identify potential risks and opportunities before they affect operational objectives. This principle closely aligns with cybersecurity risk management, which focuses on anticipating and mitigating cyber threats. Furthermore, QMS requires comprehensive documentation of organizational processes, procedures, and responsibilities, providing a strong foundation for developing, implementing, and maintaining information

security policies. The internal and external audit mechanisms established within QMS also serve as effective tools for evaluating the performance of cybersecurity controls, identifying weaknesses, and ensuring compliance with established standards. Additionally, the culture of continuous improvement promoted by QMS is particularly relevant to cybersecurity because cyber threats evolve rapidly, requiring organizations to continually update security controls, policies, and technologies. By integrating QMS principles into cybersecurity governance, organizations can establish a governance system that is more adaptive, measurable, efficient, and aligned with internationally recognized management standards.

The integration of ISO 9001:2015 and ISO/IEC 27001:2013 offers a practical framework for simultaneously managing organizational quality and information security. While ISO 9001 focuses on quality management systems and customer satisfaction, ISO/IEC 27001 establishes the requirements for Information Security Management Systems (ISMS) aimed at protecting the confidentiality, integrity, and availability of information assets. Both standards are based on the High-Level Structure (HLS) developed by ISO, enabling organizations to integrate their management systems efficiently through common structural elements. These shared elements include organizational context, leadership, planning, support, operational processes, performance evaluation, and continual improvement. The common architecture reduces duplication in documentation, auditing activities, and management processes, allowing organizations to streamline implementation while maintaining consistency between quality objectives and information security policies. As a result, integrating ISO 9001 and ISO/IEC 27001 enhances organizational efficiency, improves governance coordination, minimizes administrative redundancy, and promotes collaboration among all stakeholders involved in quality and cybersecurity management.

Previous studies have provided important theoretical foundations for understanding the relationship between quality management and organizational governance, although relatively few have explicitly examined their integration with cybersecurity. The work of Anderson and Krathwohl (2001), although primarily focused on educational frameworks, demonstrates the value of systematic and structured management approaches that parallel the principles of quality management systems. Bell (2010) highlights project-based implementation as an effective strategy for encouraging innovation, collaboration, and continuous improvement, concepts that are consistent with the philosophy of QMS. Research conducted by ISO (2018) further demonstrates that organizations integrating ISO 9001 and ISO/IEC 27001 achieve greater efficiency in managing both quality performance and information security risks by reducing duplication and improving coordination across organizational functions. In addition, the NIST Cybersecurity Framework (2020) identifies governance as the strategic foundation for effective cybersecurity management, emphasizing leadership commitment, risk management, organizational accountability, and continuous improvement as essential components of resilient cybersecurity programs.

Despite the growing body of literature on Quality Management Systems and Information Security Management Systems, existing studies generally examine these two management systems independently rather than as complementary organizational governance mechanisms. Most organizations continue to perceive cybersecurity primarily as a technical or information technology function, with limited recognition of its strategic relationship with organizational quality management. Consequently, there remains insufficient empirical and conceptual

research investigating how QMS principles can strengthen cybersecurity governance through integrated management practices. This study addresses that gap by examining the integration of QMS into cybersecurity governance, proposing a comprehensive framework that combines quality management principles with cybersecurity governance practices to enhance organizational resilience, operational effectiveness, regulatory compliance, and continuous improvement.

This study offers several novel contributions by providing an integrated conceptual framework that explicitly demonstrates the synergy between ISO 9001:2015 quality management principles and cybersecurity governance across multiple sectors, supported by cross-sectoral empirical evidence from banking, government, and manufacturing that reveals how organizational context influences integration success—a perspective largely absent in prior literature. Additionally, it develops a practical five-level framework (Policy, Process, Human Resources, Technology, and Continuous Improvement) that translates theoretical QMS principles into actionable cybersecurity strategies, while identifying specific implementation barriers such as organizational culture, resource limitations, documentation complexity, and resistance to change. This research aims to analyze the role of QMS in strengthening cybersecurity governance by examining the application of QMS principles, evaluating integration patterns across sectors, identifying success factors and barriers, and developing a practical integration framework. The findings are expected to benefit organizational practitioners through actionable implementation strategies, policymakers through insights for regulatory incentives, academic researchers through theoretical contributions to integrated management systems literature, and the broader business community by demonstrating that cybersecurity should be viewed as an integral component of organizational governance that enhances resilience, stakeholder trust, and sustainable competitive advantage.

METHOD

This research employed a descriptive qualitative research approach with a case study design to explore the implementation of Quality Management Systems (QMS) in enhancing cybersecurity governance across organizations. The descriptive qualitative approach was selected because it enables an in-depth understanding of complex social and organizational phenomena by capturing detailed narratives, perspectives, and contextual factors that influence the integration of QMS principles into cybersecurity governance practices. The case study design allows for comprehensive investigation of multiple organizational contexts, facilitating comparative analysis across different sectors to identify patterns, variations, and best practices in QMS-cybersecurity integration.

Data Collection Techniques

Literature study:

- Referring to international standards such as ISO 9001 and ISO/IEC 27001, the NIST framework, and previous studies.
- Providing a theoretical foundation that complements field findings.

Research Instruments

The instruments used in this study include interview guidelines, checklists for document analysis, and observation sheets. Sample indicators included in these instruments are:

- Availability of well-documented information security policies.

- Application of QMS principles, such as risk-based thinking and continuous improvement, within the cyber governance framework.
- Internal audit mechanisms and follow-up actions.
- Level of top management participation in information security management.

Data Analysis Techniques

The data analysis process was conducted using a thematic analysis approach consisting of the following stages:

- Data collection: integrating results from interviews, document analysis, and observations.
- Data reduction: selecting and filtering the most relevant information in relation to the research objectives.
- Classification: grouping data into main themes such as risk management, documentation, audit processes, and continuous improvement.
- Relationship analysis: evaluating the relationship between QMS and the effectiveness of cybersecurity governance.
- Presentation of results: presenting findings through descriptive narratives, comparative tables, and conceptual frameworks.

Data Validity and Reliability

To ensure data validity and reliability, the following measures were taken:

- Source triangulation: comparing information from interviews, documents, and observations for cross-verification.
- Member checking: confirming interview findings with respondents to ensure accuracy of interpretation.
- Peer review: obtaining feedback from experts in quality management and cybersecurity.
- Audit trail: thoroughly documenting the entire research process so it can be traced and verified.

Research Ethics

This study adheres to ethical principles through measures such as:

- Obtaining written consent from organizations and respondents before collecting data.
- Maintaining the confidentiality of the identities of organizations and individuals involved.
- Using data exclusively for academic and research purposes, with no other use.

RESULTS AND DISCUSSION

This study involved three main groups of organizations:

Financial and Banking Sector Has adopted ISO 9001 for more than a decade. Integrates QMS with overall risk management and has obtained ISO/IEC 27001 certification. Primary emphasis is on protecting customer data and digital transactions.

Government and Public Service Sector Recently began adopting QMS as part of bureaucratic reform efforts. Cybersecurity is still viewed as a technical issue and has not been fully integrated into management governance. Policy documents are available, but implementation is not yet uniform.

Manufacturing and Technology Sector Has implemented QMS for a long time, primarily for product quality control. Attention to cybersecurity has only increased in the past five years,

coinciding with the implementation of Industrial Internet of Things (IIoT). Efforts to integrate QMS and ISMS are ongoing, though there is resistance from employees outside the IT field.

Integration of ISO 9001 and ISO/IEC 27001

The analysis revealed three main integration patterns between QMS and ISMS:

Full Integration: Common in the banking sector. ISO 9001 and ISO/IEC 27001 are managed within a single integrated documentation system. Internal audits are conducted simultaneously to improve efficiency.

Partial Integration: Occurs in the manufacturing sector. Some quality processes (such as audits and corrective actions) have been applied to cybersecurity, but system documentation remains separate.

Minimal Integration: Dominant in the government sector. Quality policies and information security policies operate independently without adequate alignment.

Implementation Barriers

The study identified several key barriers in implementing QMS for cybersecurity governance:

Organizational culture: Many employees view cybersecurity as the exclusive responsibility of the IT department.

Resource limitations: Not all organizations have sufficient budget or expertise for integrated audits.

Documentation complexity: Integrating QMS and ISMS is often seen as burdensome due to extensive document adjustments.

Resistance to change: Employees tend to maintain old habits, such as using simple passwords.

Lack of leadership support: In organizations without management commitment, policy implementation is merely formal.

Cross-Sector Comparative Analysis

The banking sector stands out as the most advanced in integrating QMS and cybersecurity governance, driven by regulatory pressure and customer expectations. The government sector faces the greatest barriers due to limited funds, complex bureaucratic procedures, and low employee awareness. The manufacturing and technology sector is at a moderate level, driven by the need to protect digital supply chains, although it still faces internal resistance.

Conceptual Framework for QMS and Cybersecurity Governance Integration

Based on the analysis of results, this study formulates the following conceptual framework for integrating QMS with cybersecurity governance:

1. Policy Level: Combining quality policies and cybersecurity policies in a single strategic document.
2. Process Level: Applying QMS processes (such as audits, corrective actions, and risk management) to information security.
3. Human Resources Level: Engaging employees through training, awareness raising, and participation in audits.

4. Technology Level: Leveraging technology to support documentation, monitoring, and data-based decision making.
5. Continuous Improvement Level: Conducting periodic audits and evaluations to maintain the system's relevance to current threats.
6.

Relevance of Findings to QMS Theory

The research findings confirm that QMS principles can be effectively applied in cybersecurity governance. This is consistent with the foundation of ISO 9001:2015, which emphasizes risk-based thinking and continuous improvement.

- Risk-based thinking in QMS aligns with cyber risk management frameworks (such as NIST and ISO/IEC 27005), making organizations that adopt it better prepared to identify and address cyber threats.
- Continuous improvement plays a crucial role given the constantly evolving dynamics of cyber threats; QMS internal audit processes can be extended to encompass information security evaluations.
- Leadership and customer orientation in QMS have a significant impact on cybersecurity culture. The banking sector, which actively involves top management, demonstrates a more mature system compared to the government sector.

Overall, these findings reinforce the idea that QMS is not merely a quality management tool but a flexible governance framework applicable to new domains such as cybersecurity.

QMS and ISMS Integration: Synergy or Burden?

The integration of QMS (ISO 9001) and ISMS (ISO/IEC 27001) presents two main aspects in practice:

Synergies:

- Reduces repetition in documentation and audits.
- Ensures consistency in risk management.
- Facilitates achievement of regulatory compliance.

Burdens:

- Requires substantial initial investment in training, documentation, and consultation.
- Creates resistance from non-IT employees who perceive it as additional workload.

The analysis shows that the success of integration depends on top management commitment and an appropriate organizational change management strategy.

Managerial Implications

These findings have important implications for organizations:

1. Leadership plays a central role; without top management support, QMS application to cybersecurity tends to be limited to administrative aspects.
2. Training and awareness-raising are strategic investments; organizations that consistently train their employees demonstrate higher cyber readiness.
3. Audits as strategic instruments; QMS internal audits can serve as early detection tools for cyber vulnerabilities, not merely formal obligations.

4. Staged integration is more feasible; organizations are advised to start with partial integration before moving toward full integration as resource readiness improves.

Academic Implications

From an academic perspective, this study opens space for the development of new literature on the integration of quality management and information security. Key points include:

- QMS can function as a governance driver in non-quality domains, such as cybersecurity, environmental management, or sustainability.
- Cross-sector case studies show that organizational context influences implementation success, enriching contingency theory in management.
- Further research using quantitative methods is needed to statistically measure the impact of QMS on cybersecurity performance.

Future Challenges and Opportunities

This study also highlights challenges still faced by organizations:

Challenges: Resource limitations, cultural resistance, and the complexity of standards.

Opportunities: Increasingly strong regulatory momentum for adopting international standards; technological advances such as artificial intelligence (AI) and machine learning to support audits and monitoring; and growing public awareness of data protection.

Going forward, the implementation of an Integrated Management System (IMS) combining QMS, ISMS, and other standards such as ISO 22301 (Business Continuity) could become a primary strategy for sustainable security governance.

CONCLUSION

Quality Management Systems (QMS) are increasingly seen as a powerful tool for strengthening cybersecurity governance, not just a framework for quality assurance. Core principles like risk-based thinking, leadership commitment, and continuous improvement help organizations manage cyber risks systematically instead of treating security as a purely technical issue. Combining QMS (ISO 9001) with information security standards (ISO/IEC 27001) reduces duplicate paperwork, simplifies audits and compliance, and helps organizations manage both quality and security more efficiently. Success depends on strong leadership commitment, a security-conscious culture, sufficient resources, and ongoing monitoring through audits and evaluations. Adoption varies by industry banking and finance lead due to strict regulations and high cyber risk, manufacturing and tech are catching up as they digitize supply chains, while public sector organizations lag behind due to limited budgets, staff shortages, and resistance to change. Overall, in today's world of growing cyber threats, integrating QMS with cybersecurity governance isn't optional it's a strategic necessity that helps organizations improve service quality, strengthen compliance, and build lasting resilience and trust.

REFERENCES

Agarwal, K., & Shah, M. (2024). The Role of Corporate Governance in Managing Cybersecurity Risks: A Comprehensive Analysis. *LawFoyer Int'l J. Doctrinal Legal Rsch.*, *2*, 352.

Agmon, N., & Kordova, S. (2024). Model for global quality management system in system of systems: Quality management in system of systems project. *Applied System Innovation*, *8*(1), 3.

Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman.

Ali, M. A. (2023). *Analysis Of Quality Management System (Qms) Applied On Manufacturing & Design Companies*. Politecnico di Torino.

Bell, S. (2010). Project-Based Learning for the 21st Century: Skills for the Future. The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 83(2), 39–43. https://doi.org/10.1080/00098650903505415

Bouchetara, M., Amrani, A. F. Z., & Bedaida, I. E. (2022). The implementation of a quality management system in accordance with ISO 9001: 2015 standard: A case study. *International Journal of Economics & Business Administration (IJEBA)*, *10*(1), 261–286.

Buckė, V., Ruželė, D., Ruževičius, J., & Buckus, R. (2022). *The link between the application of quality management principles and risk management in healthcare*.

Ferreira, M. H. L., Melo, R. M. de, Urtiga, M. M., & Garcez, T. V. (2025). Prioritizing supporting ISO standards in quality management systems (QMS): an integrative approach based on the QMS lifecycle stages and the FITradeoff method. *Benchmarking: An International Journal*, 1–34.

Iqbal, S., Taib, C. A. Bin, Allumi, N. A., & Abbas, M. (2025). Quality-driven education: Analyzing the effects of ISO 9001 quality management principles on university performance. *Journal of Cultural Analysis and Social Change*, 1146–1159.

Kayani, S. A., Abbas, A., & Ekowati, D. (2025). Building a strategic framework for quality improvement: a review of related research, management processes and lean methodologies. *Cogent Education*, *12*(1), 2527929.

Kehinde, S. (n.d.). *Information governance frameworks for strengthening cybersecurity resilience in organizations*.

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98–108.

Mohammad, M. F. N., Abdullah, R., Jabar, M. A., Nor, R. N. H., & Nur, N. M. (2024). A theoretical framework of knowledge management systems on quality management systems. *JOIV: International Journal on Informatics Visualization*, *8*(4), 2163–2172.

Myeda, N. E., Chua, S. J. L., & Aqillah, N. S. (2023). Adopting quality management (QM) principles in managing facilities management service delivery. *International Journal of Quality & Reliability Management*, *40*(10), 2393–2419.

Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025). Cybersecurity and Governance. In *Cybersecurity Governance: An Enterprise Risk Management Strategy for Cyber Risk Control* (pp. 19–63). Springer.

Qureshi, F. (2024). Quality Management in Business: Delivering Excellence. *Journal of*

Management Science Research Review, *2*(1), 44–53.

Ranjith Kumar, R., Ganesh, L. S., & Rajendran, C. (2022). Quality 4.0–a review of and framework for quality management in the digital era. *International Journal of Quality & Reliability Management*, *39*(6), 1385–1411.

Reinhardt, J. C. V., de Freitas Dewes, M., & Gonçalez, O. L. (2026). From customer satisfaction to strategic alignment: a new framework for strategic quality management systems. *International Journal of Quality & Reliability Management*, *43*(5), 1273–1306.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974.