Integrated Strategy For Information System Security Assessment Through The Implementation Of ISO 27001 Standards

Kartika Sari[1,*], Afsha Harnia[2], Siti Nur Hidayah[3], Neng Sri wardhani [4]

[1,2,3,4]Department of Accounting, Universitas Pembangunan Panca Budi, Medan, Indonesia
E-mail: [1,*]tk281005@gmail.com, [2]ashaharnia@gmail.com, [3]sitinurhidayahh2022@gmail.com, [4]nengsri_wardhani@dosen.pancabudi.ac.id
*E-mail Corresponding Author: tk281005@gmail.com

Abstract

Information security has become a critical organizational requirement in the era of digital transformation, as the increasing use of information systems exposes organizations to complex and evolving cyber threats. Information security can no longer be treated solely as a technical issue but must be managed through a structured management framework. This study aims to analyze and synthesize previous research related to the implementation of ISO/IEC 27001 as an international standard for Information Security Management Systems (ISMS). This research adopts a qualitative literature review approach by examining scientific articles, standards documents, and relevant publications related to ISO/IEC 27001, risk management, and information security governance. The analysis focuses on key themes, including risk-based security management, governance structures, continuous improvement using the Plan–Do–Check–Act (PDCA) cycle, and organizational readiness. The results indicate that ISO/IEC 27001 provides a comprehensive framework for strengthening information security governance, improving risk management practices, and enhancing organizational resilience against cyber threats. Furthermore, successful implementation is strongly influenced by leadership commitment, employee awareness, and continuous monitoring mechanisms. This study contributes by providing an integrated understanding of ISO/IEC 27001 implementation from prior studies and offers practical insights for organizations seeking to enhance their information security management practices.

Keywords: *information security, ISO/IEC 27001, information security management system, risk management, literature review*

I. INTRODUCTION

The development of digital transformation encourages organizations to ensure that information system security management is carried out in a structured, measurable manner that is aligned with the organization's strategic objectives. The increase in data breaches, cyber attacks, and operational disruptions shows that information technology security cannot rely solely on technical controls, but must be managed through a comprehensive, risk-oriented security management framework (Rahman & Putri, 2022). In this context, ISO/IEC 27001 serves as an international standard that provides systematic guidance in establishing an Information Security Management System (ISMS) focused on protecting the confidentiality, integrity, and availability of organizational information (Ardian & Siahaan, 2023).

A number of studies show that the implementation of ISO 27001 can strengthen information security governance while improving the maturity of risk control processes in various organizational sectors (Pratama et al., 2024). The implementation of this standard encourages organizations to identify information assets, map threats, and evaluate the effectiveness of security controls on an ongoing basis through the Plan–Do–Check–Act cycle (Nugroho & Hartati, 2022). Furthermore, ISO 27001-based security assessments enable organizations to obtain an objective picture of the readiness and capabilities of information system security in facing the dynamics of cyber threats (Hidayat & Ramadhani, 2025).

An integrated strategic approach to information system security assessment is important because it combines aspects of risk management, organizational control, and continuous security performance evaluation mechanisms. This integration not only serves as a tool for measuring compliance with standards, but also as an instrument for decision-making in improving information security governance (Sari & Utami, 2023). Therefore, this study focuses on formulating an information system security assessment strategy that refers to ISO 27001, with the aim of obtaining a comprehensive picture of the level of information security readiness while compiling recommendations for strengthening controls that are relevant to best practices and organizational needs (Hakim & Widodo, 2024).

II. RESEARCH METHODOLOGY

This study uses a qualitative descriptive method with a conceptual approach. This method was chosen because the research aims to review and explain an integrated strategy for assessing information system security through the implementation of the ISO/IEC 27001 standard, without involving hypothesis testing or empirical field data collection in specific organizations. The qualitative descriptive approach is applied to provide a systematic explanation of the role, objectives, and mechanisms of ISO 27001 as a framework for information security management and organizational security assessment. Research data were obtained through documentation studies, sourced from official ISO/IEC 27001 framework documents, supporting standards related to information security management, and scientific literature in the form of textbooks, conference papers, and journal articles published in the last five years. These sources were used to strengthen the conceptual foundation of the study and ensure that the discussion is aligned with recognized security governance practices and internationally accepted information security standards.

Data analysis was conducted descriptively and conceptually by examining the clauses, control domains, and risk management principles contained in ISO/IEC 27001 that are relevant to information system security assessment. The analysis process included identifying security control structures, mapping risk-based evaluation mechanisms, and interpreting how ISO 27001 supports the development of an integrated security assessment strategy. The results of the analysis are presented in the form of a narrative description, which illustrates how ISO 27001 can be applied as a structured instrument for evaluating information security readiness, managing risks, and strengthening organizational security governance. Through this approach, the study is expected to provide a comprehensive conceptual understanding of the strategic role of ISO 27001 in supporting systematic, measurable, and sustainable information system security assessment.

III. RESULTS AND DISCUSSION

A. Results

The results of the study indicate that the ISO/IEC 27001 standard functions as a comprehensive framework for structuring and assessing information security management within an organization. ISO 27001 provides an integrated control and risk-management structure that connects organizational objectives with security policies, technological infrastructure, and operational processes. The framework enables organizations to evaluate the level of security readiness through systematic identification of assets, threats, vulnerabilities, and risk-based security controls. The analysis shows that the implementation of ISO 27001 supports a structured and measurable approach to information security assessment. Each clause and control domain in the standard is designed to ensure that security practices are aligned with organizational strategic objectives and the principles of confidentiality, integrity, and availability. ISO 27001-based assessments make it possible to review the effectiveness of security controls, the consistency of policy implementation, and the maturity level of information security governance across critical business processes.

The findings also demonstrate that ISO 27001 positions information security as an integral part of organizational decision-making and risk governance. The framework emphasizes role clarity, responsibilities, and accountability among management, control owners, and stakeholders. Security assessment using ISO 27001 does not only focus on technical configurations, but also evaluates cultural, procedural, and managerial aspects of security implementation. Furthermore, the study shows that ISO 27001 facilitates a systematic and continuous improvement process in information security management. Clearly defined control objectives and evaluation criteria help organizations identify security gaps and prioritize areas requiring improvement. ISO 27001-based assessments provide an objective reference for determining the level of control adequacy and the maturity of information security governance. This condition strengthens transparency, documentation discipline, and consistency in managing security risks, while supporting the establishment of a more accountable and sustainable security management environment.

B. Discussion

The discussion of the findings indicates that ISO 27001-based security assessment plays a strategic role in strengthening information system governance and organizational resilience. The standard connects organizational goals with security controls through a structured risk-based framework, enabling assessments that are not limited to technical safeguards but extend to process alignment, organizational culture, and strategic priorities. This approach makes security assessment more value-oriented, as it focuses on how security contributes to operational reliability and strategic performance. ISO 27001 provides a comprehensive evaluation structure in which each control domain has clear objectives and measurable criteria that can be used during the assessment process. This enables evaluators to obtain systematic guidance when reviewing the adequacy of security policies, implementation consistency, and risk-handling mechanisms. Through this process, information security risks can be identified more clearly, while control weaknesses can be addressed in a structured and traceable manner.

The discussion also highlights that ISO 27001 encourages organizations to adopt a best-practice-oriented security culture. Security is not viewed merely as a technical obligation, but as a governance mechanism that supports business continuity, stakeholder trust, and organizational credibility. The framework promotes integration between policy, technology, and human behavior, which is essential for building sustainable security management capabilities. In addition, the use of ISO 27001 contributes to assessment consistency and transparency. Standardized clauses, controls, and evaluation principles reduce subjectivity during assessment activities and increase the reliability of reported findings. This strengthens stakeholder confidence and improves the organization's ability to communicate security posture in a clear and accountable manner. Overall, the discussion confirms that ISO 27001-based information security assessment is a relevant and effective approach for supporting the development of mature and measurable information security governance. The framework not only provides structured guidance for evaluating security performance, but also acts as a catalyst for continuous improvement and the enhancement of organizational security readiness.

IV. CONCLUSION

` The results of this study show that the implementation of ISO/IEC 27001 provides a structured and integrated foundation for assessing information system security within organizations. ISO 27001 functions not only as a compliance framework, but also as a strategic instrument that links security policies, organizational processes, and risk-management mechanisms in a systematic and measurable manner. Through risk-based control mapping, documentation discipline, and clearly defined responsibilities, the framework enables organizations to obtain an objective overview of their security readiness and governance maturity. The conceptual analysis confirms that ISO 27001-based security assessment strengthens transparency, accountability, and consistency in managing information security risks. Security is positioned as part of organizational decision-making rather than merely a technical function. This condition supports the development of a security culture that integrates policy, technology, and human behavior, while encouraging continuous improvement through the PDCA cycle embedded in the standard.

Overall, this study concludes that an integrated security assessment strategy based on ISO 27001 is highly relevant for supporting resilient and sustainable information security governance. The framework provides clear guidance for evaluating the adequacy of security controls, identifying priority improvement areas, and ensuring that information security contributes to organizational strategic objectives. Future studies can extend this conceptual analysis into empirical application across different organizational contexts to measure implementation effectiveness and comparative levels of security maturity.

V. RECOMMENDATIONS

Based on the findings and conceptual analysis of ISO/IEC 27001 as an integrated framework for information security assessment, several recommendations can be proposed to strengthen the implementation and governance of information security within organizations. Strengthen Risk-Based Security Management Organizations are advised to prioritize the development of a risk-based security framework by conducting periodic asset identification, threat analysis, and vulnerability assessment. The risk register should be updated regularly and integrated into decision-making processes to ensure that security controls are implemented proportionally to risk exposure.

Enhance Documentation and Policy Standardization To support accountability and audit readiness, organizations should improve policy standardization and documentation across all ISO 27001 control domains. Security procedures, incident handling records, and access management logs need to be maintained consistently to ensure traceability and compliance with ISMS requirements. Promote Security Awareness and Organizational Culture

Information security should not only rely on technical controls but must be embedded into organizational culture. Regular training, awareness programs, and role-based security responsibilities are recommended to ensure that employees understand their roles in protecting information assets.

Implement Continuous Monitoring and Improvement Mechanisms Organizations should strengthen continuous improvement through periodic internal audits, management reviews, and control performance evaluations aligned with the PDCA cycle. Findings from assessments should be used as inputs for corrective and preventive actions to enhance ISMS maturity. Integrate ISO 27001 with Broader Governance and IT Management Frameworks To maximize strategic value, ISO 27001 implementation should be aligned with other governance frameworks such as IT service management, enterprise risk management, and business continuity planning. This integration supports stronger coordination between technology, organizational strategy, and operational processes. Encourage Further Empirical Research and Implementation Studies Future research is recommended to expand this conceptual study into empirical investigations across different sectors and organizational scales. Comparative studies on implementation effectiveness, maturity assessment, and security performance outcomes will provide deeper insights into ISO 27001 application in real-world environments.

VI. REFERENCES

Ardian, R., & Siahaan, T. (2023). Implementation of ISO/IEC 27001 in strengthening information security management systems in digital-based organizations. Journal of

Information Technology and Security Systems, 8(2), 145–156.

Hakim, A., & Widodo, R. (2024). Strategies for improving ISO 27001-based information security governance: Risk analysis and organizational control. Journal of Information Systems Management, 12(1), 33–47.

Hidayat, F., & Ramadhani, S. (2025). Evaluation of organizational information security readiness through the implementation of the ISO/IEC 27001 framework. Journal of Information Systems Governance, 6(1), 21–34.

Nugroho, D., & Hartati, S. (2022). Application of the PDCA cycle in ISO 27001-based information security management systems. Journal of Information Systems and Technology, 10(3), 289–299.

Pratama, Y., Kurniawan, A., & Lestari, M. (2024). The impact of ISO 27001 implementation on the maturity level of organizational information security. International Journal of Information Security Management, 5(2), 101–113.

Rahman, A., & Putri, D. (2022). Challenges in information security governance in the era of digital transformation. Journal of Informatics and IT Management, 7(1), 55–67.

Sari, N., & Utami, R. (2023). Integration of information security evaluation in ISO 27001-based management decision making. Journal of Administration and Information Technology, 9(4), 212–224.