PUBLISHED BY
JR EDUCATION

Available online at http://ijite.jredu.id

International Journal of Information Technology and Education (IJITE) 4 (2), (March 2025) 75-80

International Journal of Information Technology and Education (IJITE)

http://ijite.jredu.id

Implementation Policy of the Information Security Management System (ISMS) in Bitung Digital City

Ignatius Rudy Theno[1]*, Recky H E Sendouw[1], Goinpeace H. Tumbel[1]

[1]Master of Public Administration Program, Universitas Negeri Manado, Indonesia

*Corresponding author: rudytheno@gmail.com

ARTICLE INFO
Article history:
Received: January 21, 2025; Received in revised form: February 22, 2025; Accepted: March 06, 2025;
Available online: March 10, 2025;

ABSTRACT

This study aims to analyze the implementation of the Information Security Management System (ISMS) policy in Bitung City as part of its digital transformation initiative. The policy is crucial to ensure the security, integrity, and availability of public information amid increasing cybersecurity threats in the digital era. This research employs a descriptive qualitative approach using in-depth interviews, document analysis, and observations as data collection techniques. The findings reveal several obstacles in implementing the ISMS policy, including limited human resources, a lack of awareness about information security among civil servants, and the absence of a dedicated information security management team. Budget constraints and inadequate cross-sectoral coordination further hinder effective implementation. Although Bitung City has established regulatory frameworks such as mayoral regulations and regional laws related to e-government systems (SPBE), the enforcement remains suboptimal. The study recommends strengthening human resource capacities, enhancing stakeholder collaboration, and adopting standardized security protocols based on SNI ISO/IEC 27001 to ensure effective ISMS implementation, ultimately supporting Bitung's vision as a secure and reliable digital city.

Keywords: Digital City, government systems, Information Security, ISMS, ISO/IEC 27001

INTRODUCTION

The rapid advancement of information and communication technology has pushed government institutions worldwide, including in Indonesia, to adapt through the implementation of electronic-based governance systems. Bitung City, as one of the municipalities aspiring to become a digital city, has initiated several efforts to enhance digital services to the public. However, these digital initiatives expose government information systems to various risks, especially concerning information security.

The problem addressed in this study centers on the implementation of the Information Security Management System (ISMS) policy in Bitung City. Although the municipal government has issued regulatory frameworks such as mayoral decrees and has participated in Electronic-Based Government System (SPBE) programs, the actual enforcement and institutionalization of ISMS policies remain limited. Challenges include inadequate human resources skilled in information security, limited understanding among civil servants about the importance of ISMS, and the absence of integrated security protocols aligned with international standards like ISO/IEC 27001.

Moreover, the study observes that the lack of a dedicated team for information security and insufficient budget allocations hinder the effective implementation of the ISMS policy. Another issue lies in the low level of inter-agency coordination, which weakens the synergy necessary for securing government-managed data. These problems are particularly critical considering the increasing rate of cyber threats, phishing attempts, and data breaches faced by public institutions.

Thus, the research problem is rooted in the gap between regulatory intent and field implementation regarding ISMS in Bitung City. The study aims to identify and analyze the key constraints in policy implementation and to provide strategic recommendations for improving the ISMS framework. It also investigates the roles of various stakeholders and institutional arrangements that influence the success or failure of the policy.

This problem is not only administrative but also strategic, as it affects public trust in digital services and the integrity of government data. The research thus contributes to the discourse on public administration, e-government security, and digital governance by contextualizing the Bitung experience within the broader framework of policy implementation in developing digital cities.

LITERATURE REVIEW

The implementation of Information Security Management Systems (ISMS) in public institutions has increasingly gained attention due to the rise of digital governance and the associated risks of data breaches. ISMS refers to a systematic approach to managing sensitive information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process. The international standard ISO/IEC 27001 provides the requirements for establishing, implementing, maintaining, and continually improving an ISMS.

Several scholars have emphasized the importance of aligning ISMS with organizational policies and legal frameworks. For example, Calder and Watkins (2018) explain that successful ISMS adoption is contingent on leadership commitment, organizational culture, and adequate training. In the context of public sector governance, Dhillon and Backhouse (2001) highlight that policy-level support and cross-functional collaboration are crucial for sustainable ISMS implementation.

In Indonesia, the Electronic-Based Government System (SPBE) initiative mandates that local governments enhance their information system infrastructure, including the security dimension. The Ministry of Administrative and Bureaucratic Reform (KemenPAN-RB) introduced evaluation indicators that include data security as one of the benchmarks. However, studies (e.g., Rahardjo et al., 2020) suggest that many local governments still struggle with ISMS due to a lack of resources and technical expertise.

Furthermore, institutional theory (Scott, 2004) posits that policy implementation is influenced by the interaction of regulatory structures, normative pressures, and cultural-cognitive elements. Applying this theory to ISMS adoption, it is evident that formal regulations alone are insufficient without shared understanding and internalized norms regarding information security practices.

In addition, the policy implementation framework by Grindle (1980) offers a useful lens to analyze the ISMS policy in Bitung City. This framework emphasizes the role of content and context in shaping policy outcomes. Content includes clarity of objectives, allocation of resources, and institutional arrangements, while context considers the socio-political environment, bureaucratic capacity, and support from stakeholders.

Therefore, the literature underlines that ISMS policy implementation requires a multi-dimensional strategy that combines regulatory compliance, organizational readiness, human capacity development, and a supportive institutional environment. These insights provide the conceptual foundation for analyzing the case of Bitung City's ISMS policy as discussed in this study.

METHOD

This study employs a descriptive qualitative research approach to explore the implementation of the Information Security Management System (ISMS) policy in Bitung City. The qualitative method is deemed appropriate due to the study's focus on understanding social phenomena, stakeholder perceptions, and contextual factors that influence public policy implementation.

Data collection techniques included in-depth interviews with key informants such as officials from the Department of Communication and Informatics, district and sub-district administrators, and IT personnel responsible for managing government digital infrastructure. Document analysis and direct observation were also conducted to validate and triangulate the data obtained from interviews.

The research site is Bitung City, North Sulawesi, where digital transformation efforts are currently underway. The study focused on institutional frameworks, human resources, financial support, inter-organizational coordination, and technical infrastructure related to ISMS. Data were

analyzed using an interactive model involving data condensation, data display, and conclusion drawing as proposed by Miles and Huberman (1994).

To ensure the validity of the research, triangulation of sources and methods was employed. Credibility was further enhanced through member checking, while transferability and dependability were supported by thick descriptions and audit trails. This methodological rigor ensures that the study's findings offer a trustworthy account of the challenges and opportunities surrounding ISMS policy implementation in Bitung.

RESULTS AND DISCUSSION

The implementation of the Information Security Management System (ISMS) policy in Bitung City reveals a complex landscape influenced by various organizational, technical, and socio-political factors. The results of this study are organized into four key themes: institutional readiness, human resource capacity, financial support, and cross-sectoral integration.

Institutional Readiness

Despite the issuance of mayoral regulations and Bitung's inclusion in the Electronic-Based Government System (SPBE) framework, the institutional readiness for ISMS implementation remains limited. Interviews with officials revealed that regulatory compliance exists mainly on paper, and the absence of a dedicated unit or task force to oversee information security weakens execution. Policy documents are not yet translated into operational procedures aligned with ISO/IEC 27001.

Human Resource Capacity

One of the most pressing challenges identified is the limited capacity of human resources. Most civil servants and IT personnel lack formal training on information security protocols. While some training initiatives have been introduced, they are sporadic and not tailored to specific ISMS frameworks. This affects daily operations, such as secure data handling and response to digital threats.

Financial Support

Budget limitations significantly hinder ISMS implementation. According to key informants, funding for cybersecurity initiatives is minimal and often grouped under general IT expenditures without a clear allocation for ISMS. This results in underfunded activities related to monitoring, auditing, and improving system security.

Cross-Sectoral Coordination

Coordination between government departments, including the Department of Communication and Informatics and other agencies, remains fragmented. This lack of synergy prevents unified responses to security incidents and hampers the development of integrated systems. Some informants

expressed concern that the decentralization of digital operations across offices leads to inconsistent application of security standards.

These findings align with Grindle's (1980) framework, where both policy content and context influence implementation outcomes. Although Bitung City has shown commitment to digital transformation, the ISMS policy struggles due to vague objectives, a lack of resource allocation, and inadequate institutional coordination. The study also supports institutional theory (Scott, 2004), indicating that norms and internalized practices are equally important as regulations.

Efforts to improve policy implementation should focus on establishing a permanent ISMS unit, increasing capacity-building initiatives, defining budget priorities, and strengthening coordination mechanisms. These steps would not only enhance security but also promote trust in public digital services.

CONCLUSION

The study concludes that the implementation of the Information Security Management System (ISMS) policy in Bitung City is still in its formative stages, characterized by fragmented execution and limited institutional capacity. While the city government has demonstrated initial regulatory commitment through mayoral regulations and SPBE participation, the practical application of ISMS principles remains inconsistent and underdeveloped. Key barriers identified include inadequate human resources, low awareness among civil servants, insufficient budget allocation, and weak interdepartmental coordination. These factors collectively impede the establishment of a comprehensive and functional ISMS framework aligned with ISO/IEC 27001 standards. The study affirms that successful ISMS policy implementation requires not only regulatory frameworks but also the nurturing of institutional culture, capacity building, and structural investments. Applying Grindle's and Scott's theoretical models, the research highlights the necessity of considering both policy content and implementation context. To move forward, the Bitung City Government needs to institutionalize an ISMS task force, allocate dedicated cybersecurity funding, and improve training programs across all departments. Additionally, fostering a culture of information security through continuous education and stakeholder engagement will enhance the city's resilience against cyber threats. Ultimately, strengthening ISMS will not only safeguard public data but also reinforce public trust and confidence in digital government services, thereby supporting Bitung's vision as a secure and progressive digital city.

REFERENCES

Calder, A., & Watkins, S. (2018). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page Publishers.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11(2), 127–153.

Grindle, M. S. (1980). Politics and Policy Implementation in the Third World. Princeton University Press.

Miles, M. B., & Huberman, A. M. (1994). Qualitative Data Analysis: An Expanded Sourcebook. Sage Publications.

Rahardjo, B., Girsang, A. S., & Priyadi, Y. (2020). Cybersecurity readiness in local governments: An Indonesian perspective. Journal of Information Security, 11(3), 145–157.

Scott, W. R. (2004). Institutional theory. In Encyclopedia of Social Theory (Vol. 2, pp. 408–414). Sage Publications.

The Ministry of Administrative and Bureaucratic Reform. (2021). Guidelines for Electronic-Based Government Systems (SPBE). Government of Indonesia.