

Recommendations for Information Security Governance Referencing ISO/IEC 27001:2022 for Government Agencies

Azizah Bahirotun Ni'am¹, Rahadian Bisma²

^{1,2}*Universitas Negeri Surabaya, Surabaya, Indonesia*

azizahbahirotun.22020@mhs.unesa.ac.id, rahadianbisma@unesa.ac.id

ABSTRACT

Information security is crucial for local government agencies, especially those managing the Electronic-Based Government System (SPBE) infrastructure. Many agencies still lack clear and documented information security governance. This issue is evident at the Communication, Informatics, and Statistics Office (Diskominfo) X, where security operations remain reactive, and the KAMI Index rating is "Insufficient." The study aims to perform a gap analysis and design recommendations for information security governance at Diskominfo X, based on ISO/IEC 27001:2022 standards. It is a qualitative study using interviews, observations, and internal document reviews. Findings indicate that although Diskominfo has a regional legal basis and operational security practices, compliance with the standard is mostly "Not Yet Implemented." Information security management is still informal and not integrated into an Information Security Management System (ISMS) framework. The study outputs include draft SOP documents, operational forms, work regulations, and responsibility distribution drafts. Recommendations urge the institution to formalize these documents, standardize technical activities, and conduct regular internal audits and security awareness training for all employees.

Keyword: ISO/IEC 27001:2022, Tata Kelola Keamanan Informasi, Analisis Kesenjangan, Sistem Manajemen Keamanan Informasi (SMKI), Diskominfo.

Article Info:

Article history:

Received July 07, 2026

Revised August 07, 2026

Accepted September 14, 2026

Corresponding Author

Azizah Bahirotun Ni'am

Universitas Negeri Surabaya, Surabaya, Indonesia

azizahbahirotun.22020@mhs.unesa.ac.id

1. INTRODUCTION

Information is a highly valuable asset for every organization as it forms the foundation of all operational processes [1]. It is the only asset that must not be lost because the organization's continuity heavily depends on it [2]. Digital transformation has made data valuable but also vulnerable to leakage, manipulation, and loss [3]. According to the National Cyber and Crypto Agency (BSSN) report, Indonesia experienced approximately 609 to 610 million cyberattacks throughout 2024. This underscores the critical importance of information security protection for institutions relying on information technology in their business processes [4], [5]. Protection of information assets must guarantee the core principles of information security known as the CIA Triad (Confidentiality, Integrity, and Availability) [6].

To minimize risks, organizations require a structured Information Security Governance (ISG) framework to direct, manage, and evaluate the implementation of information security [7], [8]. Suboptimal information security governance can lead to vulnerabilities, triggering serious threats such as data loss, theft, damage, or unauthorized interception of important organizational information [9]. Additionally, good governance boosts public trust through effective data protection [10]. In Indonesia, this urgency is supported by formal regulations like the Minister of Communication and Information Regulation No. 4 of 2016 and BSSN Regulation No. 8 of 2020, mandating government agencies to implement an Information Security Management System (ISMS) based on the international ISO/IEC 27001 standard. As a preliminary evaluation tool, the government via BSSN developed the Information Security Index (Indeks KAMI) aligned with ISO clauses.

Despite strong legal foundations, ISG implementation in the public sector faces challenges such as low adoption of security frameworks like ISO/IEC 27001, limited training, weak leadership involvement, and bureaucratic complexity [11]. Diskominfo X exemplifies this by lacking formal, standardized information security governance guidelines. This can lead to a high risk to information security and increase the likelihood of security breaches [12]. As a result, in the evaluations over the past two years, the agency's KAMI Index score has been in the "Poor" category, indicating a significant governance gap. Additionally, the high frequency of cyber incidents on their public service websites further underscores the system's vulnerability due to the nature of services being directly accessed by the general public.

Previous studies show ISO/IEC 27001 effectively guides risk assessment and mitigation in local government settings, as seen in Diskominfo Kabupaten Bandung Barat [13]. The novelty of this research lies in tailoring governance recommendations based on identified gaps in local public service agencies.

This study proposes a gap analysis between Diskominfo X's current governance and ISO/IEC 27001:2022 requirements. The analysis results form the basis for drafting policy-level and non-technical governance recommendations. These drafts aim to serve as initial guidelines for creating a structured ISMS to strengthen protection of local government information assets.

2. METHODS

This research employs a qualitative approach with a case study design to depict the actual implementation conditions of the information security management system at the Communication, Informatics, and Statistics Office (Diskominfo) X. The qualitative approach was selected for its focus on gaining deep understanding of policy, processes, and information security practices at the organizational level. Following scientific data collection methodology classifications, this study combines both primary and secondary data. Primary data were collected directly from research subjects through interviews with staff in the cryptography and information application divisions, alongside direct observation of operational activities related to information asset security. Secondary data were gathered through documentation studies of internal regulations, organizational structure, available Standard Operating Procedures (SOPs), and formal documents of the international standard ISO/IEC 27001:2022.

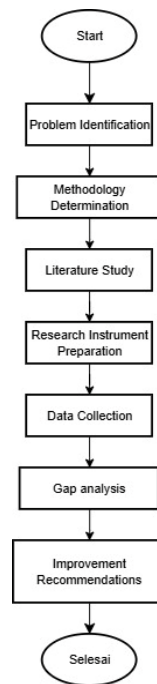


Figure 1 Research Flow

The research process is carried out through systematic stages as shown in Figure 1, including problem identification, methodology determination, literature study, research instrument preparation, field data collection, and finally the analysis and recommendation formulation stage. The data analysis method applied is gap analysis with assessment instruments derived from Clauses 4 to 10 and Annex A controls of the ISO/IEC 27001:2022 standard. The analysis process is carried out by comparing the actual condition of the organization against the ideal standard condition to classify the level of compliance into the categories of "Implemented," "Partially Implemented," or "Not Implemented." The final result of this gap analysis is used as a basis to formulate a draft of implementable information security governance recommendations for local government agencies..

3. RESULTS AND DISCUSSION

An overview of the existing conditions of information security governance at Diskominfo X was collected during the period of March–April 2026 through three main techniques: interviews with six key informants (Head of the Informatics Applications Division, Head of the Cryptography Division, and four technical staff of Computer Systems), field observations, and document studies. The findings indicate that the implementation of information security governance in the work units of the Informatics Applications Division (Aptika) and the Cryptography Division has generally been underway, but it is not yet fully formal and structured.

Top management commitment has been realized through the enactment of regulations in the form of the Regent's Regulation on the Guidelines for the Implementation of SPBE Information Security Management. At the technical level, the organization has implemented several basic Standard Operating Procedures (SOPs), such as website backup SOP, restore SOP, cyber incident handling SOP, and server room access SOP. However, daily protection of information assets remains reactive because security measures become optimal only when system disruptions occur. This limitation arises due to the absence of specific technical

guidelines or daily work instructions derived from the regulations. Moreover, the specific role distribution of the information security officer has not yet been formally established through a Decree (SK). Although there is cross-unit collaboration within the Computer Security Incident Response Team (CSIRT), the boundaries of members' tasks and responsibilities are not specifically defined. From a risk management perspective, a risk assessment document has been prepared but has yet to undergo periodic evaluation and updates.

3.1 ISO/IEC 27001:2022 Gap Analysis

The measurement of alignment between actual practices in the field and the ideal requirements of the Information Security Management System (ISMS) is conducted through a gap analysis phase. The assessment is classified into three status categories: "Implemented" (fulfilled and formally documented), "Partially Implemented" (operating verbally/informally or inconsistent evidence), and "Not Implemented" (no relevant procedures or documents). The ISO/IEC 27001:2022 standard integrates the requirements into 7 main clauses (Clauses 4 to 10) and security controls in Annex A into 4 main themes: organizational, people, physical, and technological controls. The details of the mapping results of the clauses and controls of ISO 27001:2022 at the X District Communication and Information Office (Diskominfo) are summarized in Table 1.

Table 1 Summary of Gap Analysis Results Clauses and Controls of ISO 27001:2022 at Diskominfo X

Clauses/Control ISO/IEC 27001:2022	Not Implemented	Partially Implemented	Implemented
Clauses 4 Context of the Organization	75%	25%	0%
Clauses 5 Leadership	33,3%	66,7%	0%
Clauses 6 Planning	66,7%	33,3%	0%
Clauses 7 Support	40%	60%	0%
Clauses 8 Operation	0%	100%	0%
Clauses 9 Performance Evaluation	100%	0%	0%.
Clauses 10 Improvement	100%	0%	0%
A.5 Organizational Controls	62,2%	37,8%	0%
A.6 People Controls	75%	25%	0%
A.7 Physical Controls	28,6%	71,4%	0%
A.8 Technological Controls	32,4%	67,6%	0%
Total	49,1%	50,9%	0%

Referring to the data in Table 1, it can be concluded:

a. Status "Implemented"

There are no Clauses or controls that are in the "Implemented" status (0%). Based on the ISO/IEC 27001:2022 certification methodology, a Clause or control can only be

declared "Implemented" if it meets all the mandatory requirements of the standard. These mandatory requirements include the existence of valid formal documents (internal policies/SOPs/work instructions) supported by implementation evidence (records/logs) that are consistently maintained and periodically reviewed. At Diskominfo X, although several security activities have been implemented, they are not all supported by formal agency-level documents documented to international standards, so their audit compliance cannot be fully categorized.

b. Status "Partially Implemented."

The status "Partially Implemented" holds a dominant percentage of 50.9%. This dominance is driven by the strong daily operations of technical staff in the field (especially in physical control A.7 and technological control A.8) and the legal basis provided by the Regent's Regulation. Staff have taken concrete security actions such as website backup-restore, server room access restrictions, and daily cyber incident handling. However, this practice is categorized as "Partial" because it operates based on informal habits and individual staff experience, rather than being driven by a structured system of standard instructions.

c. Status "Not Implemented"

The status "Not Implemented" has a significant percentage of 49.1%. This condition is caused by an organizational governance pattern that is still reactive in nature. The reactive work pattern focuses on handling issues when they occur rather than on planned preventive measures. As a result, elements requiring long-term strategic planning—such as the scope statement document of the Information Security Management System (ISMS), formal role distribution based on a Decree (SK) for roles and responsibilities, change management, risk effectiveness assessment, and the implementation of periodic internal audits—have not yet been initiated by the organization.

To provide a deep understanding of security gaps in the organization's management and operational systems, a detailed analysis is conducted based on the Clauses and Annex A controls.

Based on the mapping results of Clauses 4 to 10 of ISO/IEC 27001:2022, the biggest obstacle for Diskominfo X lies in the immaturity of strategic governance and organizational performance evaluation. In Clauses 9 (Performance Evaluation) and 10 (Improvement), which recorded a 100% "Not Implemented" status, the facts on the ground show that the organization has been conducting annual evaluations related to cryptographic (persandian) activity achievements to report to leadership. However, these activities do not meet standards because the organization lacks clear information security performance indicators and structured monitoring and evaluation procedure documents. Furthermore, Diskominfo X has never conducted internal or external audits, does not have an audit program, and has not formulated a plan for continuous improvement of information security quality.

This condition is closely related to the low fulfillment of Clauses 4 (Organizational Context) at 75% "Not Implemented" and Clause 6 (Planning) at 66.7% "Not Implemented." Currently, Diskominfo X has identified various internal and external organizational issues through the Risk Management document, the 2025-2029 Strategic Plan, and the 2025 Work Plan. However, the organization does not yet have a written document that aligns these strategic issues with the objectives of ISMS implementation. As a result, information security implementation proceeds without measurable achievement targets and comprehensive risk mitigation at the institutional level.

Meanwhile, Clauses 5 (Leadership) and 7 (Support) show a more positive condition due to the existence of the Regent's Regulation and the support of existing human resources. However, the lack of alignment in planning has caused Clause 8 (Operations) to be fully (100%) stalled at the "Partially Implemented" status. This indicates that all operational activities for protecting information assets within Diskominfo X are currently functioning only at the daily technical level, but have not yet been controlled by a standardized management system at the managerial level.

Based on the mapping results of the operational controls in Annex A, a significant gap was found between the technical practices in the field and compliance with the formal standards of ISO/IEC 27001:2022. The facts on the ground show that Diskominfo X has been implementing various basic security measures in daily operations. In the physical and technological aspects (A.7 and A.8), technical staff have implemented protections such as restricting access to the server room using physical keys, separating data and power cables, configuring firewalls, backing up website data, and using monitoring tools like Wazuh and Immunify. Managerial commitment is also evident with the issuance of the Regent's Regulation on SPBE Information Security Management, the formation of the CSIRT team, and the obligation for employees to sign an integrity pact.

However, the high percentage of "Partially Implemented" and "Not Implemented" statuses in all Annex A controls is due to three main organizational weaknesses. First, there is no formalization of rules and written SOPs. Although many technical actions have been routinely carried out, almost all of them still lack official SOP documents approved by the leadership, including the absence of a formal Decree for the division of roles and responsibilities in information security functions. As a result, daily security management still fully relies on the habits, initiatives, and personal experiences of each technical staff member. This condition triggers the risk of work inconsistency and overlapping functions between departments. Second, the weak preventive security controls and change management. The organization still neglects long-term strategic aspects, such as the unavailability of disaster recovery plans (Business Continuity Plan and Disaster Recovery Plan), lax security on employee work computers (no encryption, automatic screen locking, and clean desk policy), and the absence of restrictions on the use of personal USBs. Additionally, whenever there is an update to the application system or network configuration, the staff directly execute it in the production environment without going through a documented change management procedure. Third, there is no auditable record and no internal evaluation. The most critical gap is found in the absence of activity recording (logbook), both for employee entry and exit data in the server room and for centralized digital activity logs. The use of original data for application testing purposes is still often done without data masking. Lastly, the entire series of existing security procedures has never been tested for effectiveness because the organization has never conducted internal audits or compliance reviews on a regular basis. The operational conditions running without standard documents make the information security management at Diskominfo X not yet accountable according to international standards.

Based on the identification of the gaps mentioned above, the main priorities that need immediate attention are the establishment of formal governance, standardization of technical SOPs, recommendations for operational documentation, and internal evaluation. This priority is necessary to shift the work pattern from reactive to preventive through documentation and evaluation, and to ensure that information security does not depend on individuals but rather on standardized systems.

3.2 Strategies for Strengthening Information Security Governance

Based on the findings of security gaps in the previous analysis phase, a strategy for strengthening information security governance has been developed. This handling step is focused on transitioning the staff's work patterns from reactive and informal to a structured, standardized, and preventive security management system. The proposed strengthening of document governance for leaders and technical staff in the fields of Aptika and Cryptography is organized into three main aspects. Details of the focus distribution of the proposed governance document draft are presented in Table 2.

Table 2 Proposed Document Draft

Proposed Aspect Group	Control Focus	Main Function	Target Achievement
Governance	Establishment of organizational context, written rules, and legal validity.	Building a legal foundation, determining the scope of asset protection, and clarifying personnel responsibilities.	Overcoming the obstacles of unclear division of roles and employee work authority.
Operational Standards (Technical Control)	Data and system protection in the daily activity cycle.	Integrating standard security controls into every aspect of operational and written technical work procedures.	Mitigating the risk of sensitive data leaks and minimizing system vulnerabilities early on.
Evaluation (Monitoring)	Continuous improvement cycle	Providing internal audit mechanisms and scheduled monitoring to ensure compliance with document implementation.	Dynamically detect new security gaps as cyber threats evolve.

To realize the achievement targets in Table 2, the document recommendations are prepared in the form of draft policy plans, Circular Letters (SE), and Standard Operating Procedures (SOP) adjusted to the structural duties and functions of the organization. The main structural recommendation proposed to address the absence of cross-unit oversight functions is the establishment of a special SMKI Management team (SK) from the Head of the Department. This team acts as the "brain" of governance, holding full responsibility for the Organizational Context Document (Clause 4), the SMKI Governance Document (Clause 5), and the execution of the SMKI Internal Audit SOP (Clauses 9 and 10). The establishment of this function serves as a concrete recommendation to meet the requirements of Clause 5.3 ISO/IEC 27001:2022 regarding clarity of authority within the organization.

Meanwhile, the strengthening of daily operational aspects and technical protection is divided into the three existing work units, namely:

- a. The Aptika Division is appointed as the responsible party for the technical operational aspects of applications and digital infrastructure. The priority documents designed include SOP for Logical Access Management, SOP for System Development (Secure Coding), SOP for Configuration Management, SOP for Change Management, etc., to stop the habit of directly executing code in the production environment.
- b. The Cryptography Division is focused as a preventive defense and information risk mitigation fortress. The proposed critical documents include the Planning and Support

Document for SMKI (risk assessment methodology), SOP for Technical Vulnerability Management, SOP for Data Masking and Anonymization for trials, SOP for Preventing Personal Data Leaks, etc.

- c. The Secretariat is responsible for strengthening the aspects of administrative legality and physical asset management. The proposed documents include the Employee Non-Disclosure Agreement (NDA), Employee Offboarding SOP, SE Guidelines for Workplace Security (Clear Desk Clear Screen), etc.

Thru the implementation of a series of governance document recommendations on the three specific aspects mentioned above, the maturity level of information security at the Diskominfo of X is expected to gradually improve. This simultaneously strengthens the resilience of the region's digital infrastructure and boosts public trust in the reliability of government information services.

CONCLUSION

This research has successfully answered all the formulated research questions by evaluating the level of compliance and gaps in information security governance at the Diskominfo of X based on the ISO/IEC 27001:2022 standard. Thru mapping the 7 main clauses and Annex A controls of ISO/IEC 27001:2022, it was found that information security management in this organization is still dominated by informal and reactive governance. Although the commitment of top management has been realized thru the Regent's Regulation and the strong operational performance of technical staff in the field has pushed the status of "Partially Implemented" to a dominant 50.9%, the absence of formal institutional-level documents aligned with international standards has caused the status of "Not Implemented" to reach 49.1% and the status of "Implemented" to be at 0%.

Theoretically, this research makes an important contribution to the literature on information security management in the public sector, particularly in the local government environment. These findings enrich the conceptual framework regarding the dynamics of the transition in information security governance from a people-dependent work pattern (relying on the capacity and personal experience of individuals) to a system-dependent one (relying on structured systems and standardized instructions). This theoretical contribution emphasizes that the existence of regulations and daily physical-technical security activities in the field does not automatically guaranty compliance with international ISMS standards if not supported by role formalization (Decree), standardization of operating procedures (SOP), sustainable risk management, and evaluation mechanisms thru periodic internal audits.

The potential for further development of these research findings is the standardization and ratification of all formal governance design documents, technical SOPs, and recommended operational documentation forms so that the organization's work patterns can fully shift to a preventive approach. Meanwhile, the prospects for application in future studies can be directed toward expanding the scope of SMKI gap analysis to all other Regional Device Organizations (OPD) in order to build a strong cybersecurity ecosystem at the local government level. Additionally, future research can also focus on testing the effectiveness and measuring the maturity level post-implementation of the proposed recommendation documents to ensure the sustainability of reliable public services.

REFERENCES

- [1] Armah, S., & Firdaus, R. (2024). Konsep Dan Penerapan Sistem Informasi Manajemen. *Jurnal Inovasi Manajemen, Kewirausahaan, Bisnis Dan Digital*, 1(3), 50-56.

- [2] Brotby, W. K. (2009). Information security governance: A practical development and implementation approach [Tata Kelola Keamanan Informasi: Pendekatan Praktis dalam Pengembangan dan Implementasi]. John Wiley & Sons, Inc
- [3] Jelita, L. D. A., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001: 2022. *Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen*, 14(1), 84-94.
- [4] Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(5), 564-573.
- [5] Riswaya, A. R., Sasongko, A., & Maulana, A. (2020). Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia). *Jurnal Computech & Bisnis (e-Journal)*, 14(1), 10-18.
- [6] Osazuwa, C. M. (2024). Confidentiality, integrity, and availability in network systems: A review of related literature [kerahasiaan, Integritas, dan Ketersediaan dalam Sistem Jaringan: Tinjauan Literatur]. *International Journal of Innovative Science and Research Technology*.
- [7] Sweetly, M., Irawan, D., Refachriati, A., & Toar, M. J. (2023). Kapabilitas Tata Kelola Keamanan Informasi Menggunakan Cobit5 Pada Perguruan Tinggi Graha Kirana. *Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta*, 2(1), 71-75.
- [8] Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends [Tata Kelola Keamanan Informasi di Sektor Publik: Kajian, Pendekatan, Pengukuran dan Tren]. *International Journal of Information Security*, 24(4), 177.
- [9] Andayani, A. D., & Briliyant, O. C. (2021). Penilaian Kapabilitas Tata Kelola Keamanan Teknologi Informasi dan Rekomendasi Perbaikan Menggunakan COBIT 5. *Info Kripto*, 15(1), 1-10.
- [10] Fahmi, A. R. (2025). DIGITAL PUBLIC SERVICES AND CITIZEN TRUST IN GOVERNMENT.
- [11] Saraswati, K., Purwandari, B., & Trisnawaty, N. W. (2025). Investigating Challenges in Information Security Governance Implementation in Key Sectors: A Cross-Country Comparative Analysis [Investigasi Tantangan dalam Implementasi Tata Kelola Keamanan Informasi pada Sektor-Sektor Utama: Analisis Perbandingan Lintas Negara]. *The Indonesian Journal of Computer Science*, 14(2).
- [12] Alberto, J., & Karyati, C. M. (2023). Perancangan sistem manajemen keamanan informasi (SMKI) berdasarkan ISO 27001:2022 (Studi kasus data center Dinas Komunikasi dan Informatika Kota Tangerang Selatan). *Jurnal Ilmiah Komputasi*, 22(4).
- [13] Ananza, H. H. R. H., Darmawan, I., & Mulyana, R. (2019). Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001: 2013 (Studi Kasus: Diskominfotik Kabupaten Bandung Barat). *e-Proceeding Eng*, 6(2), 8368.