Evaluation of the Information Security Level at the Department of Communication and Informatics of Tabanan Regency Using ISO/IEC 27001:2022

Gede Ade Rangga Arinata[a1], Anak Agung Ngurah Hary Susila[a2], Muhammad Alam Pasirulloh[b3]

[a]Dept. of. Information Technology, Faculty of Engineering, Udayana University, Jimbaran, Bali, Indonesia
e-mail: [1]ade.rangga142@student.unud.ac.id, [2]harysusila@unud.ac.id, [3]muhammad.alam@unud.ac.id

Abstrak

Keamanan informasi merupakan aspek yang sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data, khususnya pada lingkungan pemerintahan yang mengelola layanan publik yang tentunya berbasis digital. Dinas Komunikasi dan Informatika Kabupaten Tabanan memiliki peran strategis dalam pengelolaan sistem informasi dan penyediaan layanan informasi kepada masyarakat, sehingga membutuhkan penerapan sistem manajemen keamanan informasi yang terstandarisasi dan terukur. Penelitian ini bertujuan untuk mengevaluasi tingkat penerapan sistem manajemen keamanan informasi (SMKI) pada Diskominfo Kabupaten Tabanan berdasarkan standar ISO/IEC 27001:2022 serta menyusun rekomendasi perbaikan dengan mengacu pada pedoman kontrol ISO/IEC 27002:2022. Metode penelitian yang digunakan meliputi observasi, wawancara, dan analisis dokumen untuk mengidentifikasi kesesuaian antara kondisi keamanan informasi yang diterapkan dengan 93 kontrol keamanan yang tercantum dalam Annex A ISO/IEC 27001:2022. Proses evaluasi dilakukan menggunakan pendekatan gap analysis untuk mengetahui seberapa tingkat kepatuhan serta kesenjangan dalam penerapan kontrol keamanan informasi. Hasil dari penelitian ini menunjukkan bahwa adanya tingkat implementasi keamanan informasi secara keseluruhan berada pada kategori cukup, namun masih terdapat beberapa kontrol yang belum diterapkan secara optimal. Kontrol yang memerlukan perhatian lebih lanjut meliputi autentikasi informasi, pengelolaan hak akses, serta kesiapan teknologi informasi dan komunikasi dalam mendukung kontinuitas bisnis. Berdasarkan hasil evaluasi tersebut, penelitian ini menghasilkan rekomendasi teknis yang meliputi penerapan multi-factor authentication, penyusunan dan penguatan kebijakan keamanan informasi, peningkatan infrastruktur teknologi informasi dan komunikasi, serta pelaksanaan pelatihan kesadaran keamanan informasi secara berkala. Rekomendasi yang dihasilkan ini sangat diharapkan dapat menjadi acuan penting bagi Diskominfo di Kabupaten Tabanan dalam meningkatkan suatu efektivitas penerapan sistem manajemen keamanan informasi yang tentunya sesuai dengan standar internasional..

Kata kunci: *Diskominfo Tabanan, gap analysis, Keamanan informasi, ISO/IEC 27001:2022, ISO/IEC 27002:2022*

Abstract

Information security is a crucial aspect in maintaining the confidentiality, integrity, and availability of data, particularly within government environments that manage digital-based public services. The Tabanan Regency Communication and Informatics Office plays a strategic role in managing information systems and providing public information services, thus requiring the implementation of a standardized and measurable information security management system. This study aims to evaluate the level of implementation of the Information Security Management System (ISMS) at the Tabanan Regency Communication and Informatics Office based on the ISO/IEC 27001:2022 standard and to formulate improvement recommendations by referring to the control guidelines in ISO/IEC 27002:2022. The research methods employed include observation, interviews, and document analysis to identify the conformity between the existing information security conditions and the 93 security controls listed in Annex A of ISO/IEC

27001:2022. The evaluation process was conducted using a gap analysis approach to determine the level of compliance and identify gaps in the implementation of information security controls. The results indicate that the overall level of information security implementation falls within the sufficient category; however, several controls have not yet been optimally implemented. The controls requiring further attention include information authentication, access rights management, and the readiness of information and communication technology to support business continuity. Based on these findings, this study proposes technical recommendations, including the implementation of multi-factor authentication, the development and strengthening of information security policies, the enhancement of information and communication technology infrastructure, and the conduct of regular information security awareness training. These recommendations are expected to serve as a reference for the Tabanan Regency Communication and Informatics Office in improving the effectiveness of ISMS implementation in accordance with international standards.

Keywords : *Diskominfo Tabanan, gap analysis, Information security, ISO/IEC 27001:2022, ISO/IEC 27002:2022.*

1. Introduction

The rapid development of information technology (IT) has significantly impacted various sectors, including public information and communication services. Organizations across different fields must continuously adapt and implement technological advancements to remain relevant and efficient. Over time, significant changes in the utilization of IT within the information and communication sector have occurred, where service institutions increasingly rely on IT to improve the quality of public information and communication services.

The extensive use of IT has encouraged the expansion of digital-based public services aimed at increasing service efficiency. However, these changes introduce new consequences, particularly regarding information security. Malware and Denial of Service (DoS) attacks, for example, have become increasingly concerning threats, especially targeting government institutions such as the Department of Communication and Informatics (Eko Jhony Peranata, 2023). Such attacks not only disrupt operational services but also endanger user data and organizational information assets.

Based on interview results, during the development phase at the Department of Communication and Informatics of Tabanan Regency, significant issues were identified, particularly Malware and DoS attacks that posed substantial risks to stored information systems. In 2021, a Malware attack resulted in the encryption of a large amount of critical data, including essential reports and statistical documents necessary for operational activities. A subsequent attack occurred in 2022 in the form of a DoS attack, where massive internet traffic was directed at the institution's servers, overwhelming their capacity to process legitimate requests and causing system failure. Consequently, the official website of Diskominfo Tabanan became inaccessible to the public, disrupting access to essential information and online services.

One effort to enhance organizational information security quality is the implementation of ISO/IEC 27001:2022, promoted by the National Cyber and Crypto Agency (BSSN, 2023). ISO/IEC 27001:2022 serves as an evaluation framework to assess an organization's readiness in managing information security. However, the Department of Communication and Informatics of Tabanan Regency has never conducted a formal information security evaluation since the initial implementation of its information systems.

ISO/IEC 27001:2022 is an international standard that provides guidelines for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) (ISO, 2022). Through structured information security management, organizations can systematically manage, control, and enhance information protection to mitigate potential security risks. Effective ISMS implementation enables organizations to reduce vulnerabilities that could disrupt operations and cause institutional losses (Lucia Devlina Adventia Jelita, Moh Noor Al Azam, Aryo Nugroho, 2024).

Previous research by Dayyan Fatih and Rizal Fathoni Aji (2024), titled "Information Security Evaluation Using ISO/IEC 27001: A Case Study of PT XYZ," evaluated the implementation of the ISO 27001 framework in managing information security risks in the

private sector. The study found that 17 ISO/IEC 27001:2022 controls were not fully implemented, with several only partially applied. The evaluation included IT asset identification and risk assessment through gap analysis, resulting in prioritized control recommendations based on ISO/IEC 27002:2022. However, the study focused on the private sector and did not examine implementation within regional government institutions.

Similarly, research conducted by Aris Kusnandar (2024) analyzed information security risks using the ISO/IEC 27001:2022 framework in a regional population agency. The study applied Failure Mode and Effects Analysis (FMEA) integrated with fuzzy logic to evaluate risk levels. The findings identified 13 very high risks and 10 high risks, highlighting the urgency of implementing standardized security policies. Nonetheless, the research emphasized risk processing rather than conducting a comprehensive evaluation of all ISO/IEC 27001:2022 controls within a local government context.

Based on the review of previous studies, there remains a research gap in comprehensively evaluating the implementation of ISO/IEC 27001:2022 within regional government institutions. Government sectors possess unique characteristics in managing information security, including limited resources, public transparency requirements, and regulatory compliance obligations. Therefore, the present study conducted at the Department of Communication and Informatics of Tabanan Regency aims to provide a comprehensive evaluation of all ISO/IEC 27001:2022 controls. This research offers deeper insight into the challenges of implementing information security frameworks in local government environments and generates practical recommendations tailored to institutional needs. Ultimately, the study is expected to strengthen the effectiveness and international standard compliance of the organization's Information Security Management System (ISMS).

2. Research Method / Proposed Method

This study applies a structured evaluation framework based on ISO/IEC 27001:2022 to assess the level of Information Security Management System (ISMS) implementation at the Communication and Informatics Office of Tabanan Regency. The research procedure follows a sequential methodological flow consisting of six main stages, as illustrated in the research framework.

Figure 1. Research Method Flowchart

2.1 Scope and Limitation Determination

The research begins with defining the scope and boundaries of the evaluation. The scope is limited to the Information Security Management System (ISMS) implemented within the Communication and Informatics Office of Tabanan Regency. The evaluation focuses exclusively on controls listed in Annex A of ISO/IEC 27001:2022 and assets directly related to information technology governance. This stage ensures that the assessment remains aligned with organizational objectives and research constraints.

2.2 Information Security Gap Analysis

The second stage involves conducting a gap analysis to identify discrepancies between existing security practices and ISO/IEC 27001:2022 requirements. Data collection methods include:

- Structured questionnaires derived from the 93 controls in Annex A
- Interviews with selected stakeholders determined using the RACI matrix approach
- Direct observation of IT infrastructure
- Review of internal policies and documentation

Each control is evaluated based on its implementation status to determine compliance level and identify deficiencies.

2.3 Asset Identification

After identifying security gaps, the study proceeds with asset identification. Information assets are categorized according to ISO/IEC 27005:2018 into:

- Business processes
- Information/data
- Hardware
- Software
- Network infrastructure

- Personnel
- Organizational structure

This stage determines critical assets that require priority protection.

2.4 Risk Assessment

A qualitative risk assessment is then conducted on identified assets. Risk values are calculated using: Risk=Probability×Impact Probability and impact are measured using a scale from 1 (very low) to 5 (very high). A 5×5 risk matrix is applied to classify risks into Low, Medium, High, and Critical levels. This assessment enables prioritization of mitigation strategies based on risk severity.

2.5 Recommendation Formulation

Based on the results of the gap analysis and risk assessment, corrective and preventive recommendations are developed by referring to ISO/IEC 27002:2022 guidelines. Recommendations are prioritized according to risk level:

- Critical → High urgency
- High → Medium urgency
- Medium → Low urgency

Proposed improvements may include strengthening access control mechanisms, implementing multi-factor authentication, improving ICT infrastructure readiness, enhancing security awareness programs, and refining documented procedures.

2.6 Conclusion of Evaluation Process

The final stage synthesizes the findings to determine the overall level of ISMS implementation and provide structured guidance for continuous improvement aligned with the PDCA (Plan–Do–Check–Act) cycle.

3. Literature Study

Information security has become a critical component in modern organizations, particularly in government institutions that rely heavily on digital services. The increasing frequency of cyber threats such as malware attacks, data breaches, and denial-of-service (DoS) incidents necessitates a structured and standardized approach to managing information security risks. One of the most widely adopted international standards for this purpose is ISO/IEC 27001. ISO/IEC 27001:2022 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The standard adopts a risk-based approach and follows the Plan–Do–Check–Act (PDCA) cycle to ensure systematic governance of information security. The 2022 revision introduces updated controls aligned with emerging technologies such as cloud computing, remote working environments, and advanced cyber threats. Annex A of ISO/IEC 27001:2022 contains 93 controls grouped into four domains: Organizational, People, Physical, and Technological controls.

Several previous studies have applied ISO/IEC 27001 as an evaluation framework in both private and public sectors. Research conducted in the private sector commonly focuses on gap analysis and risk assessment to measure compliance levels and formulate corrective actions. These studies generally reveal that many organizations partially implement security controls, particularly in documentation, governance formalization, and technical monitoring mechanisms. In the public sector context, prior research highlights additional challenges, including limited human resources, budget constraints, regulatory complexity, and the need for transparency and accountability. Studies evaluating government institutions often identify weaknesses in security awareness, policy enforcement, incident response preparedness, and continuity planning. However, many of these studies focus either on specific control domains or on earlier versions of the ISO/IEC 27001 standard, rather than providing a comprehensive evaluation using the updated 2022 revision.

Risk assessment frameworks such as ISO/IEC 27005 are frequently integrated into ISO/IEC 27001 evaluations to identify, analyze, and prioritize risks associated with information assets. The qualitative risk matrix method—based on probability and impact scoring—is widely used due to its practicality and clarity in determining risk levels. This approach enables organizations to align control improvements with actual risk exposure rather than implementing controls without prioritization. Based on the reviewed literature, there remains a need for comprehensive evaluation studies that apply ISO/IEC 27001:2022 in regional government

institutions. Such research is important because government entities manage critical public data and essential services, making them highly sensitive to information security failures. Therefore, this study contributes to the literature by providing an integrated evaluation combining gap analysis, asset identification, and risk assessment to formulate structured and prioritized recommendations aligned with ISO/IEC 27001:2022.

4. Result and Discussion

4.1. Gap Analysis Results

Gap analysis is a crucial step in evaluating the level of conformity of information security implementation at the Communication and Informatics Office of Tabanan Regency against the ISO/IEC 27001:2022 standard. Through this process, the current condition of information security implementation was compared with the requirements specified in the 93 controls listed in Annex A. Each control was assessed using three categories: Complete, Partial, and None, providing an objective overview of the extent to which each control has been implemented by the institution. The assessment was conducted using structured questionnaires and document verification to ensure that the assigned ratings accurately reflected the actual operational conditions.

The purpose of the gap analysis was to identify non-conformities or weaknesses within the existing information security system. By determining the status of each control, the organization can clearly recognize which aspects already meet international standards and which require significant improvement. Furthermore, the analysis helped identify contributing factors to non-conformity, such as limited documentation, insufficient staff training, absence of formal policies, or technological limitations in supporting information security. The results of the gap analysis not only indicate the implementation level of each control but also provide insight into the institution's capability to manage risks, respond to incidents, and maintain the confidentiality, integrity, and availability of information. By calculating implementation scores across the four control groups Organizational Controls, People Controls, Physical Controls, and Technological Controls this study delivers a comprehensive assessment of the institution's compliance level with ISO/IEC 27001:2022. These findings serve as a fundamental basis for formulating improvement recommendations, ensuring that information security enhancement efforts are risk-prioritized and systematically directed.

Based on the evaluation results of ISO/IEC 27001:2022 control implementation at Diskominfo Tabanan Regency, it was found that out of all assessed controls, 1 control was categorized as Complete, 83 controls were categorized as Partial, and 9 controls were categorized as None. This indicates that most controls have only been partially implemented, while several have not been implemented at all. To obtain a measurable implementation level, a weighted scoring method was applied:

Complete = 1
Partial = 0.5
None = 0

The percentage calculation followed the formula referenced from Dayyan Fatih & Rizal Fathoni Aji (2024). The calculation results for the four control groups are as follows:

- Organizational Controls:
  1 Complete, 34 Partial, and 2 None out of 37 controls.
  Total score: 18
  Achievement percentage: 48.64%

- People Controls:
  0 Complete, 5 Partial, and 3 None out of 8 controls.
  Total score: 2.5
  Achievement percentage: 31.25%

- Physical Controls:
  14 Partial out of 14 controls.
  Total score: 7
  Achievement percentage: 50%

- Technological Controls:
  30 Partial and 4 None out of 34 controls.
  Total score: 15
  Achievement percentage: 44.11%

Overall, People Controls represent the lowest-performing area (31.25%), indicating that human resource aspects in information security management require significant improvement, particularly in security awareness, post-termination procedures, teleworking arrangements, and confidentiality agreements. The Technological Controls group (44.11%) also demonstrates relatively low implementation, highlighting the need to strengthen secure authentication mechanisms, data loss prevention (DLP), backup procedures, and data protection during system testing. Meanwhile, Organizational Controls (48.64%) and Physical Controls (50%) show comparatively higher implementation levels, although they still fall short of optimal compliance with ISO/IEC 27001:2022 requirements. In conclusion, the gap analysis results provide a clear depiction of the current state of information security implementation at Diskominfo Tabanan Regency and identify priority areas for improvement. These findings subsequently serve as the foundation for developing structured recommendations and an information security enhancement plan aligned with ISO/IEC 27001:2022 standards.

Table 1. Assessment Results by Control Group

Assessment Aspect Based on ISO/IEC 27001:2022 Control Groups	Maximum Score	Obtained Score	Percentage
Organizational Controls	37	18	48.64%
People Controls	8	2.5	31.25%
Physical Controls	14	7	50%
Technological Controls	34	15	44.11%

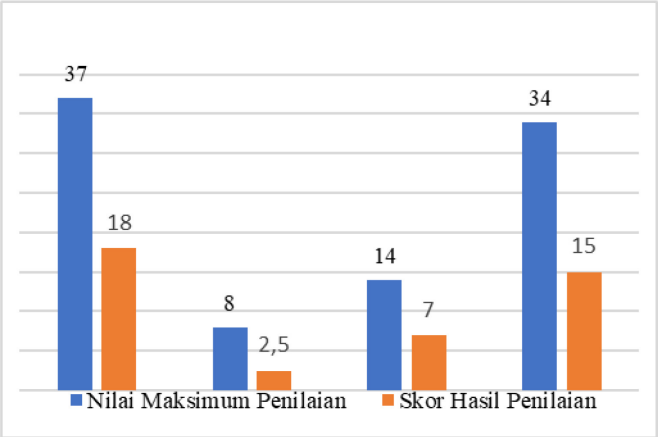

Figure 1. Gap Score of Assessment Results by Control Group

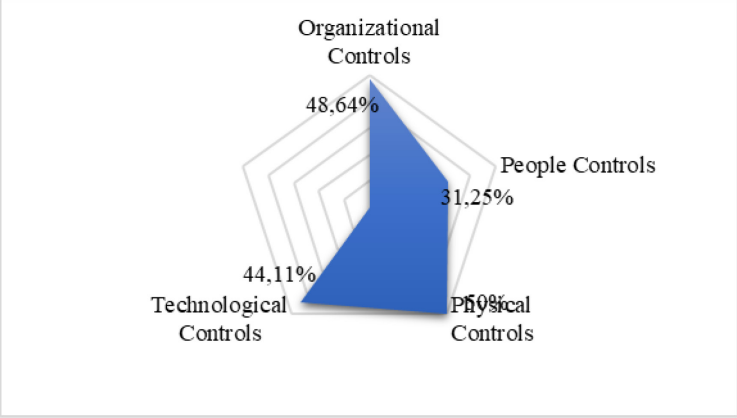

Figure 2. Comparison of Assessment Results by Control Group

4.2 Asset Identification

Based on the mapping results between ISO/IEC 27001:2022 clauses categorized as Partial and None and the assets owned by the Communication and Informatics Office of Tabanan Regency (Diskominfo), several control weaknesses were identified as potentially posing significant risks to the sustainability of information systems.

Within the Organizational Controls aspect, risks arise due to incomplete compliance with information security policies, unclear roles and responsibilities, lack of segregation of duties, and weak incident management and service continuity mechanisms. These conditions potentially affect critical assets such as servers, routers, internet networks, policy documents, the SIMKITA application, and OPD websites. Possible consequences include procedural violations, data breaches, unauthorized access, and delayed incident response.

In the People Controls aspect, risks are primarily triggered by inadequate employee screening, unclear security clauses in employment contracts, insufficient security awareness training, and weak termination procedures. These weaknesses impact assets such as user accounts, login systems, HR documents, work devices, and employee data. The associated risks include insider threats, human error, and misuse of access rights by former employees.

Regarding Physical Controls, several weaknesses were identified in perimeter security, physical access control, device protection, and facility maintenance. These deficiencies create risks to assets such as server rooms, network devices, storage media, CCTV systems, and electrical infrastructure (UPS and generators). Potential impacts include equipment theft, physical damage, operational disruptions, and data loss due to insufficient physical safeguards and improper media disposal.

Meanwhile, in the Technological Controls aspect, risks stem from the absence of secure authentication mechanisms (such as multi-factor authentication), weak vulnerability management, limited network segmentation, lack of data loss prevention (DLP) systems, and suboptimal logging and monitoring activities. Key affected assets include application servers, SIMKITA databases, OPD websites, endpoint devices, storage media, LAN and fiber optic networks, and the NOC monitoring system. These weaknesses may lead to malware attacks, exploitation of security vulnerabilities, sensitive data leakage, and public service disruptions.

Overall, the mapping indicates that most risks are associated with insufficient formal documentation, procedures that have not been fully implemented, and technical as well as human resource constraints. This asset mapping serves as a critical foundation for prioritizing information security control enhancements in accordance with ISO/IEC 27001:2022.

4.3 Risk Assessment

Risk assessment was conducted by measuring the probability (likelihood of occurrence) and impact (severity of service disruption) of ISO/IEC 27001:2022 controls previously categorized as Partial and None. The assessment was based on interviews with five respondents from Diskominfo Tabanan Regency, generating risk scores that served as the basis for determining improvement urgency levels.

Based on the calculation results, information security controls were grouped into three urgency levels: high, medium, and low. Controls with the highest risk scores (critical category, score 16–25) were predominantly found in Organizational Controls, particularly those directly related to service continuity and sensitive data protection. These controls include information classification, authentication information, cloud service security, security during disruptions, ICT readiness for business continuity, and personal data protection. This indicates that the most significant weaknesses lie in governance aspects, incident preparedness, and the organization’s ability to maintain critical services during disruptions.

The medium urgency category (score 11–15) was largely dominated by Technological Controls and some People Controls. This suggests that technical mechanisms such as vulnerability management, data loss prevention, cryptographic implementation, backup processes, and activity monitoring have been implemented but remain suboptimal and require stronger procedures and more comprehensive documentation. From a human resource perspective, improving security awareness and training programs is essential to minimize human error risks.

The low urgency category (score 6–10) was mostly identified in Physical Controls, indicating that physical protection of facilities, devices, and the working environment is relatively

adequate. Risks in this category tend to have limited impact on core operations and can be managed through routine maintenance and periodic monitoring.

Overall, the risk assessment results demonstrate that improvement priorities should focus first on high-urgency controls related to governance and service continuity. Subsequent enhancement efforts should address medium-urgency controls involving technical and human resource aspects, followed by continuous maintenance of low-urgency controls to ensure comprehensive and sustainable information security implementation at Diskominfo Tabanan Regency.

4.4 Recommendations

Recommendations for enhancing information security at Diskominfo Tabanan Regency were formulated based on the risk analysis results and ISO/IEC 27002:2022 guidelines. For high-urgency controls, improvements focus on strengthening authentication mechanisms, securing cloud services, protecting personal data, and implementing Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) to ensure the continuity of critical services.

For medium-urgency controls, reinforcement efforts include integrating security into ICT project management, improving data classification and labeling, strengthening access control, enhancing incident management processes, and upgrading technical safeguards such as Endpoint Detection and Response (EDR), patch management, network segmentation, backup systems, and implementing Secure Software Development Life Cycle (SSDLC) practices.

For low-urgency controls, improvements emphasize administrative measures such as policy updates, formal assignment of security roles, employee screening procedures, vendor compliance monitoring, strengthening physical controls, securing storage media, and improving Standard Operating Procedure (SOP) documentation.

By gradually implementing these recommendations, Diskominfo's information security posture is expected to become stronger, more measurable, and fully aligned with ISO/IEC 27001:2022 standards.

Table 2. Information Security Improvement Recommendations

Urgency	Control Focus	Core Recommendations (Summary)
High	Authentication, Cloud, Service Continuity, Data Privacy	Implement MFA for all critical accounts; ensure cloud security aligned with ISO 27017/27018; establish comprehensive DRP & BCP; apply AES-256/TLS 1.3 encryption; implement DLP & ACL for personal data protection; ensure system redundancy.
Medium	ICT Projects, Classification/Labeling, Data Transfer, System Access, Incident Management, Technical Controls (Malware, Vulnerability, Backup, Network)	Integrate security into all ICT projects; implement data classification & labeling; secure data transfer via VPN/SFTP; enforce RBAC & periodic access audits; establish CSIRT & incident response SOP; deploy EDR, patch management, DLP, automated backup; implement VLAN segmentation; apply cryptography; adopt SSDLC & OWASP guidelines.
Low	Policies, SOP, Roles, Vendors, Physical Security, Media, Human Resources	Update security policies; formally assign security roles; enforce segregation of duties; conduct employee screening; implement NDA agreements; perform vendor audits; strengthen physical access controls; enforce clean desk policy; maintain asset inventory; ensure secure device disposal; conduct independent audits & improve SOP documentation.

4.5 Discussion

The risk assessment results indicate that most ISO/IEC 27001:2022 controls at the Communication and Informatics Office of Tabanan Regency (Diskominfo) are categorized as Partial, meaning that they still require significant strengthening. The highest risks were identified in controls related to authentication mechanisms, cloud service security, personal data privacy,

and service continuity during disruptions. These high-risk controls demonstrate that information security governance and critical data protection are not yet fully adequate. Such conditions may potentially disrupt the stability of government services, particularly digital services that heavily depend on the confidentiality, integrity, and availability of information.

Controls classified under medium urgency are predominantly associated with technical and human resource aspects, including vulnerability management, network security, data backup, data loss prevention, and employee security awareness. This finding suggests that technical mechanisms are already in place; however, their implementation remains inconsistent and requires further standardization through formal SOPs, comprehensive documentation, and optimized use of supporting technologies.

Meanwhile, controls under the low urgency category mainly involve physical and administrative aspects, such as policy updates, procedural documentation, facility security, employee screening, and asset management. This indicates that foundational information security measures have been reasonably implemented, although periodic updates and regular evaluations are still necessary to maintain compliance.

Overall, the study reveals that information security improvement priorities at Diskominfo Tabanan Regency should first focus on high-urgency controls, particularly those concerning personal data protection, critical account authentication, and preparedness for incidents or service disruptions. Once these critical areas are reinforced, subsequent improvements should target medium-urgency controls by enhancing technological safeguards, strengthening staff capacity, and refining operational SOPs. Low-urgency controls can be improved through routine maintenance and periodic evaluations to ensure sustained alignment with ISO/IEC 27001:2022 standards and consistent implementation of information security practices.

5. Conclusion

Based on the results of the gap analysis and risk assessment of ISO/IEC 27001:2022 control implementation at the Communication and Informatics Office of Tabanan Regency (Diskominfo), it can be concluded that the overall level of information security implementation falls within a moderate category, yet still requires significant improvement in several key areas. Of the total controls assessed, only 1 control was categorized as Complete, while 83 controls were classified as Partial and 9 controls as None, indicating that the majority of controls have not been optimally implemented.

The implementation score calculation shows that People Controls (31.25%) and Technological Controls (44.11%) have the lowest levels of implementation, reflecting weaknesses in technical capacity, operational procedures, and employee information security awareness. In contrast, Physical Controls (50%) and Organizational Controls (48.64%) demonstrate relatively better implementation levels, although further strengthening is still necessary to achieve full compliance with the standard.

The risk assessment results indicate that several controls fall into the high-urgency category, particularly those related to authentication mechanisms, data classification, cloud service security, disruption preparedness, and personal data protection. This suggests that Diskominfo's primary weaknesses lie in information security governance and digital service resilience. Controls categorized under medium and low urgency also require improvement through enhanced procedures, employee training, and routine maintenance.

Overall, this study emphasizes that Diskominfo Tabanan Regency must undertake gradual and structured improvement measures, starting with controls associated with the highest risk levels. Strengthening information security implementation in alignment with ISO/IEC 27001:2022 will help ensure data protection, maintain the continuity of public services, and enhance public trust in the regional government's information systems.

References

[1] H. Afiansyah and N. Febriyani, "Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022," Jurnal Info Kripto, vol. 17, no. 3, pp. 93–99, 2023.

[2] L. Agung Surya, Perancangan Sistem Assessment Keamanan Informasi Rumah Sakit Menggunakan Framework ISO 27001 (Studi Kasus: RSUD Arifin Achmad), Skripsi, 2018.

[3] H. Akbar and R. Saputra, "Evaluasi Kinerja Tata Kelola Teknologi Informasi Terhadap Tools Internal Framework COBIT 2019," Sebatik, vol. 27, no. 2, pp. 589–605, 2023.

[4] J. Alberto and C. Karyati, “Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan),” Jurnal Ilmiah Komputasi, vol. 22, no. 4, pp. 493–504, 2024.
[5] B. Aurabillah, L. Putri, N. Fadhlilla, and A. Wulansari, “Implementasi Framework ISO 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review),” Jurnal Mahasiswa Teknik Informatika, vol. 8, no. 1, pp. 454–460, 2024.
[6] Badan Standardisasi Nasional, SNI ISO/IEC 27001:2022, 2023.
[7] L. Jelita, M. Azam, and A. Nugroho, “Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022,” Jurnal Saintekom, vol. 14, no. 1, pp. 84–94, 2024.
[8] M. Mulana, Audit Keamanan Sistem Informasi Pada Dinas Komunikasi Dan Informatika Kabupaten Bogor Menggunakan Standar ISO/IEC 27001:2013 dan COBIT 5, Skripsi, 2019.
[9] N. Octariza, Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Pusat PT Jasa Marga, Skripsi, 2019.
[10] F. Pujiani and R. Bisma, “Strategi Optimalisasi Manajemen Konfigurasi untuk Keamanan Informasi Berdasarkan ISO/IEC 27001:2022,” Journal of Emerging Information Systems and Business Intelligence, vol. 5, no. 3, pp. 223–228, 2024.
[11] Robere, “Update ISO/IEC 27001:2022, Persiapan Transisi dan Pentingnya Adopsi Standar Baru,” 2024. [Online]. Available: robere.co.id.
[12] R. Rudiyanto and V. Suryani, “Analisis Sistem Manajemen Keamanan Informasi Pada Dinas Komunikasi Informasi Dan Statistik Kabupaten Lampung Tengah Menggunakan ISO/IEC 27001,” e-Proceeding of Engineering, vol. 10, no. 2, pp. 2039–2047, 2023.
[13] M. Sari, Y. Saintika, and W. Prabowo, “Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto,” Jurnal Sistem dan Teknologi Informasi, vol. 10, no. 4, pp. 423–428, 2022.
[14] I. Sina, Metodologi Penelitian, Bandung: Widina Bhakti Persada, 2022.
[15] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D, Bandung: Alphabet, 2020.
[16] Suriyadi and F. Azmi, “Pengembangan Manajemen Resiko Pada Instansi Pendidikan,” Warta Dharmawangsa, vol. 16, no. 3, pp. 543–553, 2022.
[17] R. Syafira, Audit Teknologi Informasi Dengan Framework COBIT 4.1 Untuk Manajemen Risiko Pada PUSTIPD UIN Raden Fatah Palembang, Skripsi, 2020.
[18] M. Waruwu, “Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Kuantitatif dan Mixed Method,” Jurnal Pendidikan Tambusai, vol. 7, no. 1, pp. 2896–2910, 2023.