JURNAL RISET INFORMATIKA **P-ISSN: 2656-1743 |E-ISSN: 2656-1735**
Vol. 7, No. 4. September 2025 DOI: https://doi.org/10.34288/jri.v7i4.394
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

INFORMATION TECHNOLOGY RISK ANALYSIS USING ISO 27005:2022 AT DISKOMINFO TABANAN REGENCY

Ni Kadek Dheananda Astini[-1], Gusti Agung Ayu Putri[-2], Dwi Putra Githa[-3]

Information Technology / Faculty of Engineering
Universitas Udayana
dheanandaastini@student.unud.ac.id[-1], agung.ayuputri@unud.ac.id[-2], dwiputragitha@unud.ac.id[-3]

Abstract

The advancement of information technology (IT) provides significant benefits for organizational operations, including the Department of Communication and Informatics (Diskominfo) of Tabanan Regency. However, IT implementatiocn also brings security risks, such as hacking and cyberattacks, which can threaten the continuity of public services. This study aims to implement risk management based on ISO/IEC 27005:2022 to protect the IT assets owned by Diskominfo Tabanan Regency. The stages carried out include context establishment, risk identification, risk analysis, risk evaluation, and recommendations. In the risk identification stage, 28 IT assets, 57 threats, existing controls for each asset, vulnerabilities of these controls, and potential consequences were identified. In the risk analysis stage, eight respondents were asked to complete a questionnaire to assess the impact of threats and the likelihood of their occurrence, with the average impact and likelihood scores being 3 and 4, respectively. Based on the questionnaire results, the study will proceed with risk level assessment to determine risk levels based on the previous analysis. Subsequently, a risk evaluation will be conducted to provide recommendations for effective mitigation measures. This IT risk analysis study resulted in mitigation recommendations for threats that could potentially impact Diskominfo Tabanan Regency IT assets. The recommendations were developed based on the severity level of each risk after analysis, referring to common practices in both public and private sectors, as well as sources such as research journals, relevant literature, and the ISO/IEC 27005 standard.

Keywords: Diskominfo-1; Information Security-2; Information Technology-3; ISO 27005-4; Risk Management-5

Abstrak

Kemajuan teknologi informasi (TI) memberikan manfaat signifikan bagi operasional organisasi, termasuk Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Tabanan. Namun, penerapan TI juga membawa risiko keamanan, seperti peretasan dan serangan siber, yang dapat mengancam keberlangsungan layanan publik. Penelitian analisa risiko teknologi informasi ini bertujuan untuk menerapkan manajemen risiko berbasis ISO/IEC 27005:2022 guna melindungi aset teknologi informasi yang dimiliki Diskominfo Kabupaten Tabanan. Tahapan yang dilakukan meliputi penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, dan rekomendasi. Pada tahap identifikasi risiko, ditemukan 28 aset teknologi informasi, 57 ancaman, kontrol yang ada pada masing-masing aset, kerentanan dari kontrol tersebut, serta konsekuensi yang mungkin timbul. Pada tahap analisis risiko, delapan responden diminta mengisi kuesioner untuk menilai dampak ancaman dan kemungkinan terjadinya ancaman, dengan hasil rata-rata nilai dampak dan kemungkinan berada pada angka 3 dan 4. Dari hasil kuesioner yang didapatkan, penelitian dilanjutkan dengan penilaian tingkat risiko untuk menentukan level risiko berdasarkan analisis sebelumnya. Selanjutnya, dilakukan evaluasi risiko guna memberikan rekomendasi langkah mitigasi yang efektif. Penelitian analisa risiko TI ini menghasilkan rekomendasi mitigasi untuk ancaman yang berpotensi memengaruhi aset TI Diskominfo Kabupaten Tabanan. Rekomendasi disusun berdasarkan tingkat keparahan risiko setelah analisis, dengan mengacu pada praktik umum di sektor publik dan swasta, serta referensi dari jurnal, literatur, dan standar ISO/IEC 27005.

Kata kunci: Diskominfo-1; ISO 27005-2; Keamanan Informasi-3; Manajemen Risiko-4; Teknologi Informasi-5

INTRODUCTION

Advances in information technology (IT) in the digital era have brought significant impacts on organizational operations, including in the government sector. IT has become a strategic asset that supports the achievement of vision, mission, and public service efficiency (Putri et al., 2020). Its implementation not only optimizes business processes and increases productivity but also reinforces institutional resilience in the face of growing digital dependency (Padmi et al., 2022).

Dinas Komunikasi dan Informatika (Diskominfo) of Tabanan Regency is one of the institutions that rely on IT to manage data and provide digital public services. Systems such as e-letters and public portals have become integral to service delivery. However, incidents such as cyberattacks, fiber optic failures, and the major breach at the Temporary National Data Center (PDNS) on June 20, 2024, which disrupted services for weeks due to the absence of backups, highlight the urgency of structured information security risk management.

Information security risks may arise from both technical and human-related factors. These include system failures, malware, insider threats, or negligence each of which can compromise availability, confidentiality, and integrity of data (Setia Sandi, 2022). Risk is described as a multidimensional concept driven by uncertainty and potential disruptions to organizational goals (Kheradmand et al., 2020) Proactively identifying and mitigating such risks is essential, especially in public organizations where service continuity is critical (Sarjana et al., 2022).

Effective risk management begins with identifying the organization's valuable assets, including hardware, software, data, and human resources (Hikam et al., 2024) (Mardivta et al., 2022). Inadequate asset recognition can lead to unpreparedness in responding to threats. For example, studies in local government settings have revealed that service delivery systems are particularly vulnerable to risks such as server downtime, which can be addressed through structured controls like scheduled data backups and cloud recovery plans (Isnaini et al., 2023).

Previously, the implementation of information security at Diskominfo Tabanan had shown fairly good results. However, there is still room for improvement to achieve a more optimal level of information security. This condition is also in line with findings in various other government institutions, where risk analysis based on ISO/IEC 27005 has identified various potential risks across aspects such as technology, human resources, business processes, and information systems (Nursetyawati et al., 2020) (Sahira et al., 2020).

In sectors with high data sensitivity like health or education, risks have been managed using risk treatments ranging from avoidance and modification to sharing, depending on the severity and likelihood of each scenario. Improving asset maintenance and applying policy-based controls have been shown to be effective in managing medium and high-risk threats in public health IT systems (Jonny et al., 2021). Similarly, in enterprise environments, mitigation has included disaster recovery planning and physical safeguards to protect against environmental and operational threats (Tsany et al., 2020) (Marwati, 2023).

Organizations that implemented ISO/IEC 27005 often paired it with ISO/IEC 27002 for technical control selection, especially when addressing moderate-to-high risk classifications (Eka et al., 2024). These controls typically covered areas such as malware protection, access management, and backup systems. In some cases, organizations enhanced employee awareness and clarified security roles to reduce internal vulnerabilities (Utami, Supramaji, & Isnaini, 2023).

To address the evident gaps and growing challenges in managing IT security risks, this study adopts ISO/IEC 27005:2022 as the guiding framework. The standard supports comprehensive, iterative risk management, including the identification of threats, evaluation of vulnerabilities, analysis of risk levels, and selection of treatment options (Badan Standardisasi Nasional (BSN), 2023). Its flexible and scalable structure allows for alignment with public sector contexts, where risk tolerance and service dependency vary widely.

Building on prior findings across diverse institutions, this research applies the ISO/IEC 27005 methodology holistically to the IT environment of Diskominfo Tabanan. By identifying potential threats, evaluating asset vulnerabilities, and developing actionable mitigation strategies, this study aims to enhance the agency's preparedness and strengthen public confidence in digital government services.

RESEARCH METHODS

This section outlines the approach and procedures used to conduct the research, including the type of research, time and location, research subjects, data collection techniques, and data analysis. The research is designed to align with the ISO/IEC 27005:2022 framework for information

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v7i4.394
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

security risk management and is applied in the context of a case study at Diskominfo Kabupaten Tabanan.

Types of research

This research uses a qualitative descriptive method with a case study approach. The research emphasizes understanding and analyzing risk management processes based on ISO/IEC 27005 standards at Dinas Komunikasi dan Informatika Kabupaten Tabanan.

Time and Place of Research

The research was conducted from October 2024 to Mei 2025 at Dinas Komunikasi dan Informatika Kabupaten Tabanan, Bali, Indonesia.

Research Target / Subject

The target of this research is the Information Technology assets and the stakeholders responsible for IT security at Diskominfo Kabupaten Tabanan. The subjects were selected through purposive sampling, focusing on individuals with direct involvement in the management and security of IT infrastructure, including system administrators, IT security officers, and relevant policy decision-makers.

Procedure

The research follows a structured sequence based on the ISO/IEC 27005 risk management framework. The steps include a series of activities that guide the risk assessment process and can be seen in Figure 1.

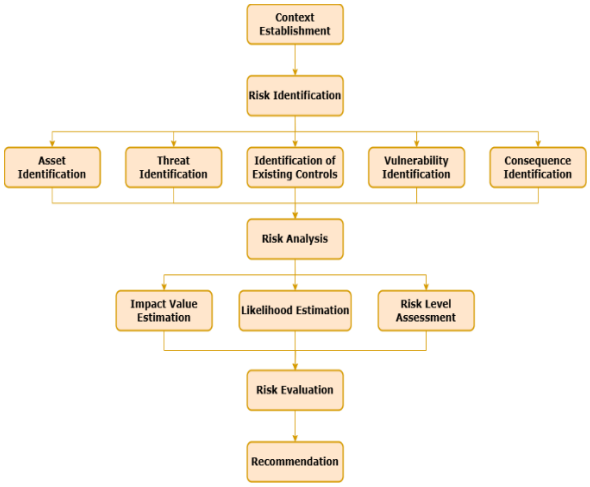

Figure 1. Research Workflow

Each stage is supported by appropriate data collection and assessment techniques to ensure validity and accuracy of results.

Data, Instruments, and Data Collection Techniques

The study utilizes both primary and secondary data. Primary data were obtained through observation, interviews, and questionnaires. Observation was conducted to directly examine the actual IT environment and infrastructure at the research site. Interviews were carried out with key personnel to gain in-depth insights into organizational policies, past risk incidents, and current mitigation strategies. Questionnaires were employed to evaluate the perceived likelihood and impact of potential threats identified during the risk identification phase.

Secondary data were collected from existing documents, internal organizational policies, and technical reports that provide context and support for the primary findings.

The instruments used in this study include structured interview guidelines to ensure consistency in data collection, risk assessment questionnaires using a predefined rating scale to quantify threat impact and likelihood, and observational checklists to document findings systematically during field visits.

Data analysis technique

The data analysis process involves both qualitative interpretation and quantitative risk assessment through a risk matrix approach. Initially, each identified threat is assigned a score based on its potential impact and likelihood, using a scale ranging from 1 to 5. These two scores are then multiplied to generate a composite risk value for each threat. Based on this value, risks are categorized into several risk levels, such as low, medium, high, and very high, to facilitate prioritization.

Subsequently, the analysis involves evaluating existing controls in place to mitigate these risks and identifying any gaps or weaknesses. The findings from this evaluation are then synthesized to develop appropriate risk treatment recommendations.

Ultimately, the analysis results in a prioritized list of risks accompanied by targeted recommendations, aimed at enhancing the protection of the organization's information technology assets.

RESULTS AND DISCUSSION

This section presents the results of risk analysis in the Information Technology (IT) environment at the Department of Communication and Informatics (Diskominfo) of Tabanan Regency

based on ISO/IEC 27005:2022. The analysis includes context establishment, risk identification, control analysis, vulnerability and consequence assessment, risk evaluation, and prioritization.

Context Establishment

This research focuses on the IT environment of Diskominfo Tabanan Regency, where digital public services heavily depend on the availability and security of systems. The scope includes hardware, software, infrastructure, and human resources. Key contextual factors include organizational structure, recent incidents such as national data center outages, and the institution's low maturity in information security management.

Risk Identification

Risk identification is the initial phase in the risk management process, comprising five key steps: asset identification, threat identification, identification of existing controls, vulnerability identification, and consequence assessment. Each step plays a critical role in building a comprehensive understanding of potential risks to IT assets. The result of the first step, asset identification, is presented in Table 1.

Table 1. Identification of IT Assets at Diskominfo Tabanan

Asset Code	Asset Name	Category
AH1	UPS	Hardware
AH4	Laptop	Hardware
AH8	Server	Hardware
AH14	Router	Hardware
AS1	Main Website of Government Units	Software
AS2	SIMKITA Application	Software
AI1	Access Point	Infrastructure
AI2	Network Operations Center (NOC)	Infrastructure
AI3	Technical Operations Center	Infrastructure
AP1	IT Expert (Human Resource)	Human Resource

Table 1 presents the initial identification of information technology assets owned by Diskominfo Tabanan as the first step in IT risk management. A total of 28 assets were identified, including hardware, software, infrastructure, and human resources. Of these, 10 assets were classified as critical, such as servers, routers, web applications, laptops, and core network devices. These assets are essential for service continuity and data integrity. The second step, which involves the identification of threats to these assets, is presented in Table 2.

Table 2. Identification of Threats to IT Assets at Diskominfo Tabanan

Threat Code	Threat Description	Category
TI01	Hardware malfunction	Technical Failure
TI02	Cooling system failure	Technical Failure
TI03	Power outage	Infrastructure Failure
TI04	Router connection failure	Infrastructure Failure
TI05	Overheating of router	Technical Failure
TH07	Laptop theft	Human Action (Deliberate)
TH08	Identity theft via application	Human Action (Deliberate)
TH12	User negligence or human error	Human Action (Unintentional)
TH14	Web-based attack	Human Action (Deliberate)
TH15	Man-in-the-middle attack	Human Action (Deliberate)
TH16	Data integrity compromise	Human Action (Unintentional)
TH02	Lack of staff awareness	Human Action (Unintentional)
TP01	Fire (affecting hardware/network)	Physical Threat
TP06	Power instability/surge	Physical Threat
TN05	Flood	Natural Threat
TT01	Device/system failure	Technical Failure
TT02	Application performance issue	Technical Failure
TO01	IT personnel shortage	Organizational Failure
TO02	NOC resource deficiency	Organizational Failure
TH01	Unauthorized access to server	Human Action (Deliberate)
TP02	Equipment overheating	Physical Threat
TH18	Misuse of asset by internal party	Human Action (Deliberate)
TH19	Loss of device due to	Human Action

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v7i4.394
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

Threat Code	Threat Description	Category
	negligence	(Unintentional)
TP05	Fire in confined infrastructure room	Physical Threat

Table 2 lists threats that are mapped to the assets identified in Table 1. These threats are categorized into technical, organizational, human-related, physical, and natural types. Examples include power outages (TI03), identity theft (TH08), router overheating (TI05), and flooding (TN05). Each threat is assigned a standardized code and category to support a structured risk evaluation. The classification follows the ISO/IEC 27005:2022 standard, which provides a comprehensive catalog of common information security threat sources. The next step is identifying and documenting existing controls to reduce threat impact or likelihood, as shown in Table 3.

Table 3. Identification of Existing IT Asset Control at Diskominfo Tabanan

Asset Code	Asset Name	Existing Controls
AH1	UPS Unit	Regular battery checks, voltage monitoring.
AH4	Laptop	Stored in clean, dust-free areas; used with surge protector.
AH8	Server	Climate-controlled room, antivirus, firewall, periodic maintenance.
AH14	Router	Firmware updates, password protection, restricted admin access.
AS1	Government Website	Content updates, basic access restrictions.
AS2	SIMKITA Application	Routine maintenance, security module updates.
AI1	Access Point	Firmware updates, bandwidth monitoring.
AI2	Network Ops Center (NOC)	Regular network monitoring, access restriction policies.
AI3	Technical Ops Center	System performance tracking, routine hardware checks.
AP1	IT Expert	Periodic training; information security workshops.

Table 3 details the existing controls implemented to protect each asset. These include voltage monitoring for UPS units, antivirus and firewall configurations for servers, access restrictions for applications, and regular training for IT staff. These controls form a baseline to assess residual risks and identify areas that require further improvement. The subsequent step is to identify vulnerabilities that remain despite the implementation of these controls, as shown in Table 4.

Table 4. Identification of Vulnerability to IT Assets at Diskominfo Tabanan

Asset Code	Vulnerability Description
AH1	Overheating risk, battery degradation, lacks automatic failover system.
AH4	Susceptible to theft, vulnerable to power fluctuation, lacks encrypted storage.
AH8	Vulnerable to cyberattack, sensitive to temperature spikes, single point of failure risk.
AH14	Outdated firmware risks, default credentials may not be changed consistently.
AS1	Prone to web attacks (e.g., XSS, SQL Injection), insufficient logging of suspicious access.
AS2	Security documentation is weak; insufficient input validation.
AI1	Weak Wi-Fi password policies, unencrypted transmissions, firmware update delay.
AI2	Reliance on manual monitoring; response delay due to staff shortage.
AI3	Unstructured fault response plan; technical bottlenecks under load.
AP1	Lack of certified training, risk of misconfiguration due to human error.

Table 4 identifies vulnerabilities that persist despite existing controls. Examples include battery degradation in UPS units, outdated firmware on routers, insufficient input validation in web applications, and delayed threat detection due to limited staffing. These weaknesses increase the likelihood of successful threat exploitation. The next step is to assess the potential consequences that may arise if these vulnerabilities are exploited, which is described in Table 5.

Table 5. Identification of Consequence to IT Assets at Diskominfo Tabanan

Asset Code	Consequence
AH1	Sudden shutdown of critical systems, risk of corrupted operations and lost data.
AH4	Device loss or data theft, inability to perform mobile or remote work.
AH8	Server downtime, exposure of sensitive data; operational collapse of IT systems.
AH14	Unauthorized access to the network, potential man-in-the-middle attacks.
AS1	Leakage of public service data, defaced site content; reputational damage.
AS2	Unauthorized data modification, user identity misuse, service disruption.
AI1	Wi-Fi hijacking, data interception; disruption of staff connectivity.
AI2	Prolonged outage due to slow threat detection, failure to restore network operations quickly.
AI3	Loss of control over core systems, inability to mitigate real-time technical faults.
AP1	Delayed incident handling, misconfiguration of critical systems.

Table 5 evaluates the potential consequences if these vulnerabilities are exploited. The impacts range from server outages and data breaches to service interruptions and loss of public trust. For example, a failure in the NOC could result in widespread service disruption due to delayed incident response.

Risk Analysis

Risk analysis is carried out by assessing the potential impact and likelihood of each identified threat exploiting existing vulnerabilities in IT assets. This step helps quantify the level of risk associated with each asset-threat-vulnerability combination. The risk value is calculated using a risk matrix, where scores are derived from qualitative judgments supported by field data. The results of the risk analysis can be seen in Table 6.

Table 6. Risk Level Assessment

Asset Code	Threat Code	Likelihood	Impact	Risk Value	Risk Level
AH1	TI01	4	3	12	2
AH1	TI03	4	4	16	1
AH1	TH12	3	3	9	3
AH4	TT01	4	4	16	1
AH4	TH07	4	4	16	1
AH4	TP06	4	3	12	2
AH8	TN05	4	4	16	1
AH8	TT01	4	4	16	1
AH8	TP01	3	4	12	2
AH14	TI05	4	4	16	1
AH14	TI04	3	4	12	2
AH14	TH15	4	4	16	1
AS1	TH14	4	4	16	1
AS1	TT02	3	4	12	2
AS2	TH08	4	4	16	1
AS2	TH16	4	3	12	1
AI1	TN05	4	4	16	1
AI1	TP01	3	4	12	2
AI2	TO02	4	4	16	1
AI2	TP01	3	4	12	2
AI3	TI02	4	4	16	1
AI3	TP01	3	4	12	2
AP1	TO01	4	4	16	1
AP1	TH02	3	4	12	2

Risk Evaluation

Risk evaluation involves comparing the analyzed risk levels against predefined criteria to determine their acceptability and prioritize treatment efforts. This process helps in distinguishing which risks require immediate action and which can be tolerated or monitored. The outcomes of the risk evaluation are presented in Table 7.

Table 7. IT Asset Risk Evaluation at Diskominfo Kabupaten Tabanan

Asset Code	Threat Code	Risk Level	Risk Evaluation
AH1	TI03	1	Power outage may cause the UPS to fail, interrupting key systems during a blackout.
AH4	TT01	1	Device/system failure on laptop disrupts mobile work or key presentations.
AH4	TH07	1	Laptop theft may lead to data loss and operational disruption.

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v7i4.394
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

Asset Code	Threat Code	Risk Level	Risk Evaluation
AH8	TN05	1	Flooding could damage the server and result in data and service loss.
AH8	TT01	1	Server failure disrupts access to core services and data.
AH14	TI05	1	Router hardware failure disables network communication.
AH14	TH15	1	Man-in-the-middle attack compromises data integrity and confidentiality.
AS1	TH14	1	Web-based attacks on public websites may disrupt availability and compromise data.
AS2	TH08	1	Identity theft in SIMKITA could allow unauthorized access and data manipulation.
AS2	TH16	1	Unauthorized processing of personal data violates data protection regulations.
AI1	TN05	1	Flooding may damage the Access Point, disrupting network access.
AI2	TO02	1	Lack of resources at NOC affects incident monitoring and response capacity.
AI3	TI02	1	Cooling system failure causes overheating and damage to TOC components.
AP1	TO01	1	Shortage of skilled personnel delays response and weakens information security management.
AH1	TI01	2	Power supply failure may prevent UPS from functioning as a backup, disrupting critical operations.
AH4	TP06	2	Dust and corrosion may damage sensitive laptop components.
AH8	TP01	2	Fire hazard could damage server hardware and stop essential services.
AH14	TI04	2	Telecom network failure leads to connectivity loss across systems.
AS1	TT02	2	System saturation impacts website responsiveness and availability.
AI1	TP01	2	Fire hazard could destroy network equipment and cause outages.
AI2	TP01	2	Fire may cause physical damage to the NOC, affecting network operations.
AI3	TP01	2	Fire risk may impair TOC's operational functions and system control.
AP1	TH02	2	Social engineering attacks may lead to unauthorized access and data breaches.
AH1	TH12	3	Hardware damage to UPS risks loss of backup functionality and operational reliability.

Table 7 provides qualitative descriptions of the top-ranked risk scenarios. Each scenario combines an asset, a threat, and the rationale behind its risk level. For example, flooding (TN05) affecting servers is noted for potentially causing severe data and service loss, while lack of skilled IT personnel could delay incident response and weaken security management.

Recommendation

This section provides recommended risk treatment actions to address the identified high and very high risks. The recommendations are formulated based on the results of the risk evaluation, considering the nature of the threat, asset criticality, and existing control effectiveness. Each recommendation aims to reduce the risk to an acceptable level through technical, organizational, or procedural measures. The detailed recommendations can be seen in Table 8.

Table 8. Recommendations for handling IT asset risks in the Diskominfo Kabupaten Tabanan

Asset Code	Threat Code	Risk Level	Recommendation
AH1	TI03	1	Install redundant UPS

Asset Code	Threat Code	Risk Level	Recommendation
			systems and perform regular power failure simulation tests.
AH2	TI03	1	Implement automatic genset switching and power failure notifications (Rozak, Kiswanta, Setiawan, Triyanto, & Nurtiyanto, 2021).
AH3	TI03	1	Install UPS at each workstation and enable auto-save for critical apps.
AH4	TT01	1	Install diagnostic software and regularly monitor laptop hardware (Hasnan & Willy, 2022).
AH7	TH06	1	Apply full disk encryption to all external hard drives (Fathiyana, 2021).
AH8	TN05	1	Place servers on waterproof racks with minimum height elevation.
AH11	TP03	1	Install thermal shields and anti-radiation filters on monitors.
AH14	TI05	1	Provide backup routers and automatic network failover systems.
AH15	TI05	1	Prepare alternative communication lines (e.g., VoIP mobile) for emergencies (Handoko, 2020).
AH17	TP03	1	Add heat sinks and external ventilation near the video processor.
AH18	TP03	1	Protect the AC unit from direct heat exposure using a thermal cover.
AS1	TT03	1	Implement automatic audit scripts to detect unauthorized changes.
AS2	TH08	1	Use multi-factor authentication and enable user activity logging.
AI1	TN05	1	Elevate access point devices and install water sensors.
AI2	TN05	1	Elevate NOC equipment and install flood detection sensors.
AI3	TN05	1	Install portable waterproof covers on TOC equipment.
AI4	TO03	1	Apply biometric access control to LAN facilities (Novinaldi & Putra, 2023).
AI6	TO03	1	Provide an alternative internet connection (dual ISP/4G failover) (Azmi & Razi, 2022).
AP1	TO01	1	Plan IT workforce proactively based on workload and project projections (Khaeruman, Mukhlis, Bahits, & Tabroni, 2023).

Table 8 contains targeted risk treatment actions for each critical asset-threat combination. The recommended actions include infrastructure improvements such as the installation of waterproof server racks and the implementation of redundant UPS systems, the application of enhanced security controls such as multi-factor authentication and data encryption, as well as capacity-building measures including staff planning and regular training programs. Each recommendation is designed to address high-priority risks effectively, with reference to relevant standards and supporting literature.

CONCLUSIONS AND SUGGESTIONS

Conclusion

The application of ISO/IEC 27005:2022 at Diskominfo Tabanan revealed numerous risks to the organization's critical IT assets. Risk levels ranged from moderate to very high, especially for threats like natural disasters, infrastructure failures, and cyberattacks. Despite the presence of some controls, many assets were still vulnerable due to outdated systems or insufficient policies. The study identified the most significant risks and provided tailored recommendations to improve resilience, particularly for server operations, network infrastructure, and human resource readiness.

Suggestion

Based on the IT risk analysis using ISO 27005 at Diskominfo Tabanan, it is recommended that the agency prioritize mitigation of high-severity risks and implement the proposed measures gradually to optimize resource use. Regular risk reviews are essential due to evolving threats and technology changes. Ongoing awareness and training for staff should be conducted to strengthen collective responsibility for IT asset security. These recommendations can serve as a basis for future research to assess the effectiveness of ISO 27005-based risk management. Expanding the scope to include more assets, divisions, or activities, and integrating other frameworks like NIST SP 800-30 or OCTAVE, may also enhance the depth and breadth of future risk analyses.

REFERENCES

Azmi, K., & Razi, F. (2022). *Studi Penggunaan Dua Isp Dengan Load Balancing Dan Failover Untuk Meningkatkan Kinerja Jaringan Berbasis*. *06*(02), 176–183.

Badan Standardisasi Nasional (BSN). (2023). *SNI ISO/IEC 27005:2022*. Badan Standardisasi Nasional (BSN).

Eka, D., Hidayatullah, R., Kunthi, R., & Harwahyu, R. (2024). *Design and Analysis of Information Security Risk Management Based on ISO 27005 : Case Study on Audit Management System (AMS) XYZ Internal Audit Department*. (September), 395–413.

Fathiyana, R. Z. (2021). Analisis Keamanan Perangkat Lunak Enkripsi Media Penyimpanan DiskCryptor. *Journal of Informatics and Communication Technology (JICT)*, *3*(1), 20–30. https://doi.org/10.52661/j_ict.v3i1.64

Gina Cahya Utami, Aden Bahtiar Supramaji, & Khairunnisak Nur Isnaini. (2023). Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *8*(1), 47–56. https://doi.org/10.32528/justindo.v8i1.219

Handoko, D. (2020). Pemanfaatan Voip Phone System Sebagai Sarana Komunikasi Jaringan Lokal. *Jurnal Teknik Informatika Kaputama (JTIK)*, *4*(2), 187–193.

Hasnan, A., & Willy, A. (2022). Sistem Pakar Diagnosa Kerusakan Hardware Laptop Menggunakan Meode Forward Chaining Berbasis Web. *Jurnal Surya Informatika*, *12*(2), 1–7. https://doi.org/10.48144/suryainformatika.v12i2.1364

Hikam, M. L. B., Dewi, F., & Praditya, D. (2024). Analisis Manajemen Risiko Informasi Menggunakan Iso/Iec 27005:2018 (Studi Kasus: PT. XYZ). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(2), 728–734. https://doi.org/10.29100/jipi.v9i2.4709

Isnaini, K., Nofita Sari, G. J., & Kuncoro, A. P. (2023). Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa. *Jurnal Eksplora Informatika*, *13*(1), 37–45. https://doi.org/10.30864/eksplora.v13i1.696

Jonny, Ambarwati, A., & Darujati, C. (2021). Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005. *Jurnal Sistem Informasi*, 13-25. https://doi.org/10.46576/rjpkm.v2i2.1104

Khaeruman, Mukhlis, A., Bahits, A., & Tabroni. (2023). Strategi Perencanaan Sumber Daya Manusia Untuk Meningkatkan Kinerja Organisasi. *Jurnal Riset Bisnis Dan Manajemen Tirtayasa (JRBMT)*, *7*(1), 41–50. http://dx.doi.org/10.48181/jrbmt.v7i1.23910

Kheradmand, Y., Honarbakhsh, A., Movahedifar, S. M., & Afshari, A. R. (2020). Development of a risk management model for using interpretive structural modeling. *International Journal of Nonlinear Analysis and Applications*, *11*(Special Issue), 31–52. https://doi.org/10.22075/ijnaa.2020.4486

Mardivta, H., Izman Herdiansyah, M., Bina Darma, U., Jenderal Ahmad Yani No, J., & Sur-el, P. (2022). Analisis Dan Perancangan Sistem Informasi Pengelolaan Aset (Studi Kasus: Satuan Kerja Teknologi Informasi PT. Bukit Asam, TBK). *Jurnal Ilmiah MATRIK*, *24*(1). https://doi.org/10.33557/jurnalmatrik.v24i1.1634

Marwati, F. (2023). Penerapan Manajemen Risiko Keamanan Smartphone Menggunakan ISO/IEC 270005 Di Organisasi. *Engineering and Technology International Journal*, *5*(02), 126–137. https://doi.org/10.55642/eatij.v5i02.348

Novinaldi, N., & Putra, I. (2023). Implementasi Teknologi Biometrical Identification untuk Login Hotspot. *Jurnal Pustaka Robot Sister (Jurnal Pusat Akses Kajian Robotika, Sistem Tertanam, Dan Sistem Terdistribusi)*, *1*(1), 11–13.

https://doi.org/10.55382/jurnalpustakarobotsister.v1i1.358

Nursetyawati, E., Fauzi, R., & Nugraha, R. A. (2020). *Perancangan Manajemen Keamanan Informasi Menggunkan Metode Analisis Risiko ISO 27005:2008 Pada Dinas Komunikasi Dan Informatika Jawa Barat*.

Padmi, I. A. A., Githa, D. P., & Susila, A. A. N. H. (2022). Audit Tata Kelola Teknologi Informasi Rumah Sakit Umum X Menggunakan Framework Cobit 2019. *JITTER-Jurnal Ilmiah Teknologi Dan Komputer*, *3*(1), 894–901.

Putri, E. N., Sukarsa, I. M., & Susila, A. A. N. H. (2020). IT Governance Improvement at Communication and Information Office using COBIT 5. *International Journal of Recent Technology and Engineering (IJRTE)*, *9*(1), 1402–1408. https://doi.org/10.35940/ijrte.a2396.059120

Rozak, O. A., Kiswanta, Setiawan, J., Triyanto, A., & Nurtiyanto, W. A. (2021). Implementasi Automatic Switching Genset PLN di Masjid Al Hikam Putat Nutug Ciseeng Bogor. https://doi.org/10.46576/rjpkm.v2i2.1104

Sahira, S., Fauzi, R., & Santosa, I. (2020). *Analisis Manajemen Risiko Pada Aplikasi E-Office Yang Dikelola Oleh Pt Telkom Indonesia Menggunakan Standar ISO/IEC 27005:2018 Analysis Of Risk Management In E-Office Application Managed By Pt Telkom Indonesia Using Iso/Iec 27005:2018 Standard*.

Sarjana, S., Nardo, R., Hartono, R., Siregar, Z. H., Irmal, Sohilauw, M. I., … Badrianto, Y. (2022). *Manajemen Risiko* (H. Fajar Ningrum, Ed.). Media Sains Indonesia.

Setia Sandi, A. A. (2022). *Manajemen Risiko TI* (H. Jayusman, Ed.). CV. Elvaretta Buana.

Tsany, M., Nur, M. A., Darmawan, I., & Fauzi, R. (2020). *Implementation Of Risk Assessment On Information Technology Division In PT. XYZ Uses ISO 27005:2008*.