The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 4, August 2024
https://doi.org/10.33022/ijcs.v13i4.4171

# The Design of Information Technology Risk Management of The Secretariat of The Cabinet of The Republic of Indonesia

**Wahyu Arief Budiman, Yekti Wirani, Yudho Giri Sucahyo**
wahyu.arief@ui.ac.id, yektiwirani@cs.ui.ac.id, yudho@cs.ui.ac.id
Faculty of Computer Science, Universitas Indonesia

**Article Information**

Received : 21 Jun 2024
Revised : 26 Jun 2024
Accepted : 25 Jul 2024

**Keywords**

Risk Management, Information Technology, ISO 31000:2018, ISO/IEC 27005:2022, ISO/IEC 27002:2022

## Abstract

The Cabinet Secretariat of the Republic of Indonesia (Setkab) as a government institution that is responsible for managing cabinet management needs to implement information technology risk management effectively. In line with the Regulation of the Minister for Empowerment of State Apparatus and Bureaucratic Reform (PermenPAN RB) number 5 of 2020 concerning Guidelines for Risk Management of Electronic-Based Government Systems (SPBE), it is necessary to have a design for handling information technology risks. However, Setkab has not yet implemented information technology risk management, resulting in information technology-related risks are not being identified. This study aims to develop a design for information technology risk management that is suitable for the needs and context of Setkab. The method used in the study is qualitative, collecting data through interviews, document analysis, and observation of information technology risks in the Setkab environment. Data analysis uses thematic analysis method. In developing the design for information technology risk management for Setkab, ISO 31000:2018 standard will be used as the main framework, then referring to ISO/IEC 27005:2022, as guidelines for risk assessment and risk treatment activities, and ISO/IEC 27002:2022 as the information security control reference. This research found 340 risk scenarios, 93 of which needed to be mitigated and 247 risks were acceptable. This research produced a risk management design using a combination of ISO 31000:2018 as a general guide for the risk management framework, ISO/IEC 27005:2022 for guidelines on the information technology risk management process, and ISO/IEC 27002:2022 for determining recommendations for risk treatment controls that is expected to help Setkab manage information technology risks systematically.

## A. Introduction

The adoption of information technology by the Indonesian government is governed by Presidential Regulation (Perpres) number 39 of 2019 concerning One Data Indonesia, emphasizing the importance of integrated and standardized data management at the national level [1]. This program aims to integrate data from various ministries and agencies and make it publicly available for use by all stakeholders. Perpres number 95 of 2018 on Electronic-Based Government Systems (SPBE) introduces the concept of an electronic-based government system, providing the legal framework for government agencies to develop and manage government information systems electronically [2]. Perpres number 132 of 2022 on SPBE Architecture underscores the importance of integrated and standardized information technology architecture to enhance the effectiveness and efficiency of public services [3].

SPBE plays a crucial role in realizing transparent, accountable, and efficient government governance. However, SPBE is not free from various risks that can hinder its effectiveness and accountability. Therefore, strengthening SPBE with risk management becomes necessary to ensure smooth and secure operations. The legal foundation for strengthening SPBE risk management is outlined in the Regulation of the Minister of State Apparatus Empowerment and Bureaucratic Reform (PermenPAN RB) number 5 of 2020 on Guidelines for Risk Management of Electronic-Based Government Systems (SPBE). This regulation mandates government agencies to implement risk management in SPBE, encompassing risk identification, analysis, and control [4]. Relevant ISO standards, such as ISO 31000 on Risk Management and ISO/IEC 27005 on Information Security Risk Management, can serve as guides for developing comprehensive SPBE risk management.

The Secretariat of the Cabinet of the Republic of Indonesia (Setkab) is a government agency that plays a vital role in coordinating between institutions by providing technical and administrative support [5]. One of its main services is providing information and documentation related to policies and decisions made by the President and Vice President. This service includes the preparation and management of official documents, such as presidential decrees, decisions, and various regulations issued by the government. Setkab also provides administrative services to support the activities of the President and Vice President, including coordinating meetings and official events, as well as internal and external communications. Additionally, Setkab disseminates information to the public about government activities and policies through its official website, social media, and public meetings [6].

The adoption of SPBE allows for quicker and more efficient administrative processes, better data management, and enhanced government transparency. PermenPAN RB Number 5 of 2020 mandates that all government agencies, including Setkab, implement risk management for information and electronic technology. This helps ensure the integrity and reliability of public services and aligns with good governance principles. Currently, Setkab's risk management approach is mainly reactive, focusing on incident response and removing resolved incidents from the risk register. This leads to inadequate identification of IT-related risks. Therefore, it is essential for Setkab to develop and implement comprehensive IT risk management to secure strategically valuable information for the state.

One study starts from the necessity of e-Government to realize clean, effective, transparent, and accountable governance as well as quality and reliable public services. The current challenges in implementing e-Government include the absence of derivative regulations, including regulations for e-Government Security. The framework used is COBIT 2019 [7]. Another study addresses the lack of information security risk management plans in the Electronic Certification Institute, using the standards ISO/IEC 27005:2011, ISO/IEC 27002:2013, and NIST SP 800-30 Rev. 1 [8]. Several studies related to the application of information security technology risk in government agencies use standards ISO/IEC 27005:2018, ISO/IEC 27002:2018, and NIST SP 800-30 Rev. 1[9][10]. One study attempts to propose a meta-process model for risk management based on ISO 31000:2018. This meta-model is expected to support the implementation of risk management processes in various types of business processes, fields, and organizational domains. The study proposes a risk management process model based on ISO 31000:2018 and follows ISO 9001:2015 recommendations by integrating risk management modeling [11].

Based on previous relevant studies, it was found that in information technology risk management, several frameworks are commonly used. These include COBIT 2019 to derive proposed design of the e-Government Security Governance System from the 28 core models of COBIT 2019, and ISO 31000:2018. ISO/IEC 27002:2018 is employed as a framework for assessing information security risks, while ISO/IEC 27005:2018 and NIST SP 800-30 Rev. 1 are used as frameworks for information security risk management. The activities conducted aim to build a design for information technology risk management and provide recommendations for risk mitigation.

This research aims to design information technology risk management for government agencies that must comply with the Guidelines for Risk Management of SPBE in accordance with PermenPAN RB number 5 of 2020. These guidelines share several components with ISO 31000:2018, such as the Framework and Process. The risk management process in ISO/IEC 27005:2022 also shows similarities with the SPBE risk management process. Therefore, the chosen framework for the overall design of information technology risk management is ISO 31000:2018, with the information technology risk assessment process referring to ISO/IEC 27005:2022, and the determination of control recommendations referring to ISO/IEC 27002:2022.

## B. Research Method

The information technology risk management framework is based primarily on ISO 31000:2018. The research proceeded through several stages, as illustrated in **Figure 1**. The first stage involved identifying the problem through initial interviews, observations, and analysis of incident reports. In the second stage, a review of both theoretical literature and relevant prior research was conducted to identify the appropriate method. The third stage consisted of conducting interviews guided by the theoretical framework established in the second stage, adhering to the research constraints. These interviews were semi-structured, with the interviewer using a predefined guide during the interviews [12][13]. The interviewees come from various positions in Setkab, namely the Head of the Center of Data and Information Technology, a Senior Computer Expert in the field of System

Development and Implementation, and a Senior Computer Expert in the field of Infrastructure and Networks. Interviews were conducted using a semi-structured method in accordance with Annex A of ISO/IEC 27005:2022. The fourth stage involves analyzing the risk assessment framework outlined in ISO/IEC 27005:2018, while risk treatment is guided by the Guidelines for Risk Management of SPBE and utilizes ISO/IEC 27001:2022 to identify appropriate mitigating controls. The findings from the fourth stage were subsequently verified and confirmed with the risk owner to ensure the accuracy of the analysis derived from the interviews. The conclusions and recommendations were drawn from the results of the fifth stage.

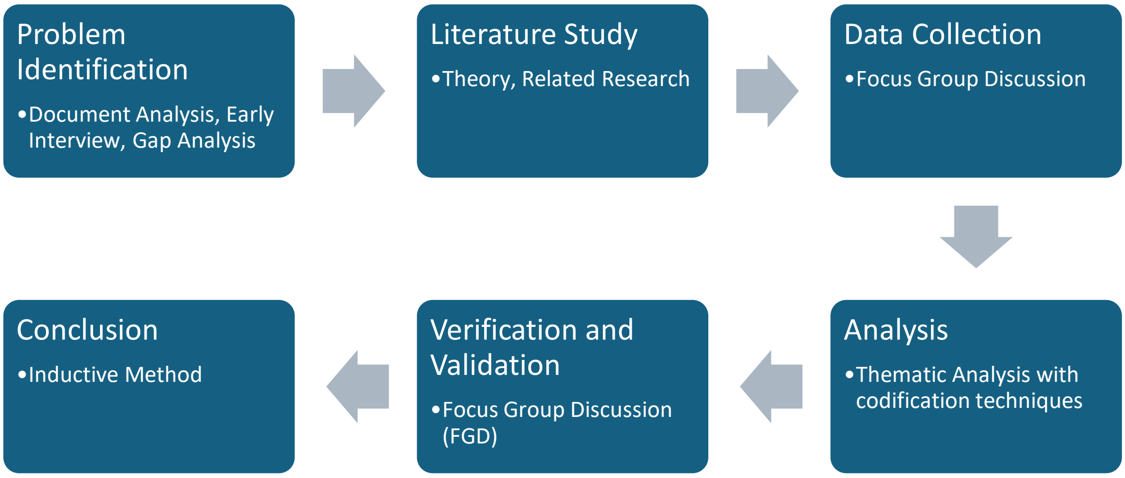
Problem Identification
•Document Analysis, Early Interview, Gap Analysis
Literature Study
•Theory, Related Research
Data Collection
•Focus Group Discussion
Analysis
•Thematic Analysis with codification techniques
Verification and Validation
•Focus Group Discussion (FGD)
Conclusion
•Inductive Method

**Figure 1.** Research Methodology

## C. Result and Discussion

This section details the analysis and discussion involved in the risk management design for Setkab. The research focused on developing an information technology risk management plan, beginning with context establishment, followed by risk assessment, and culminating in risk treatment.

### 1. Context Establishment

In the context-setting stage, the basic criteria for the information technology risk management design process were determined according to the framework used. This process began with identifying the basic criteria for managing risk, followed by defining the boundaries of the information technology risk management scope. The outcome of this stage was the establishment of the basic criteria and the scope boundaries for the information technology risk management at Pusdatin Setkab.

#### 1.1. Base Criteria Establishment

This research utilizes two main regulations as guidelines for conducting risk management, PermenPAN RB Number 5 of 2020 concerning Guidelines for Risk Management of SPBE and Peraturan Sekretaris Kabinet (Perseskab) Number 1 of 2019 concerning Risk Assessment Guidelines within Setkab. From these regulations, the research adopts three basic criteria for assessing risk: impact criteria, likelihood criteria, and risk acceptance criteria.

### 1.1.1. Impact Criteria

This research employs four out of the seven impact criteria established in PermenPAN RB Number 5 of 2020, along with some negative impacts from Perseskab Number 1 of 2019. The selection of these criteria is tailored to the research context and the defined scope. Details regarding these four impact criteria are presented in **Table 1**.

**Table 1.** Impact Criteria

| Impact Area | | Impact Level | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| | | Not Significant | Less Significant | Moderately Significant | Significant | Very Significant |
| Reputation | Negative | Verbal complaints from stakeholders <3 times in one year | Verbal complaints from stakeholders 3-5 times in one year, or written complaints ≤2 times in one year | Verbal complaints from stakeholders 3-5 times in one year, or written complaints ≤2 times in one year | Diplomatic note from a friendly country forwarded by the Ministry of Foreign Affairs to the Cabinet Secretariat | Diplomatic note from a friendly country forwarded by the Ministry of Foreign Affairs to the President |
| Performance | Positive | Performance improvement < 20% | Performance improvement 20% to < 40% | Performance improvement 40% to < 60% | Performance improvement 60% to < 80% | Performance improvement ≥ 80% |
| | Negative | Decrease in performance < 20% | Decrease in performance 20% to < 40% | Decrease in performance 40% to < 60% | Decrease in performance 60% to < 80% | Decrease in performance ≥ 80% |
| Organization-al Services | Positive | Increase in user satisfaction level < 20% | Increase in user satisfaction level 20% to < 40% | Increase in user satisfaction level 20% to < 40% | Increase in user satisfaction level 20% to < 40% | Increase in user satisfaction level 20% to < 40% |
| | Negative | Decrease in user satisfaction level < 20% | Decrease in user satisfaction level < 20% | Decrease in user satisfaction level < 20% | Decrease in user satisfaction level < 20% | Decrease in user satisfaction level < 20% |
| Operations and ICT Assets | Positive | Decrease in resource utilization level < 20% | Decrease in resource utilization level < 20% | Decrease in resource utilization level < 20% | Decrease in resource utilization level < 20% | Decrease in resource utilization level < 20% |
| | Negative | Increase in resource utilization level < 20% | Increase in resource utilization level < 20% | Increase in resource utilization level < 20% | Increase in resource utilization level < 20% | Increase in resource utilization level < 20% |

https://doi.org/10.33022/ijcs.v13i4.4171

### 1.1.2. Likelihood Criteria

Likelihood criteria serve to measure the likelihood of an information technology incident occurring. **Table 2** presents the likelihood criteria utilized in this research, adapted from PermenPAN RB Number 5 of 2020 concerning Guidelines for Risk Management of SPBE.

**Table 2.** Likelihood Criteria

| Likelihood Level | | Percentage Likelihood of Occurrence in One Year | Frequency of Likelihood of Occurrence in One Year |
|---|---|---|---|
| 1 | Almost Never Occurs | X ≤ 5% | X < 2 occurences |
| 2 | Rarely Occurs | 5% < X ≤ 10% | 2 ≤ X ≤ 5 occurences |
| 3 | Occasionally Occurs | 10% < X ≤ 20% | 6 ≤ X ≤ 9 occurences |
| 4 | Frequently Occurs | 20% < X ≤ 50% | 10 ≤ X ≤ 12 occurences |
| 5 | Almost Certain to Occur | X > 50 % | > 12 occurences |

### 1.1.3. Risk Acceptance Criteria

Risk acceptance criteria involve determining the magnitude of risk to assist risk owners in deciding whether to retain or address the risk, and prioritizing risks for risk management. **Table 3** presents a risk analysis matrix, which combines impact levels and likelihood levels. The dashed line represents the risk acceptance threshold.

**Table 3.** Risk Analysis Matrix

| Risk Analysis Matrix | | | Impact Level | | | | |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | Not Significant | Less Significant | Moderately Significant | Significant | Very Significant |
| Likelihood Level | 5 | Almost Certain to Occur | 9 | 15 | 18 | 23 | 25 |
| | 4 | Frequently Occurs | 6 | 12 | 16 | 19 | 24 |
| | 3 | Occasionally Occurs | 4 | 10 | 14 | 17 | 22 |
| | 2 | Rarely Occurs | 2 | 7 | 11 | 13 | 21 |
| | 1 | Almost Never Occurs | 1 | 3 | 5 | 8 | 20 |

**Table 4** presents the risk acceptance criteria established in the risk management process, in accordance with the policies set by the risk owner unit.

**Table 4.** Risk Acceptance Criteria

| Risk Level | | Risk Value Range | Color Coding | Acceptance |
|---|---|---|---|---|
| 1 | Very Low | 1-5 | Blue | Accepted |
| 2 | Low | 6-10 | Green | Escalation / Mitigation / Transfer / Avoidance |
| 3 | Moderate | 11-15 | Yellow | Escalation / Mitigation / Transfer / Avoidance |
| 4 | High | 16-20 | Orange | Escalation / Mitigation / Transfer / Avoidance |
| 5 | Very High | 21-25 | Red | Escalation / Mitigation / Transfer / Avoidance |

### 1.2. Scope and Limitations Establishment

The scope definition aims to ensure that all information technology assets of Data and Information Technology Center (Pusdatin) Setkab are included in the risk assessment process. The scope of information technology risk management in this research is limited to the operational activities of data centers and information technology within Setkab. The assets assessed in this study include information, business processes, hardware, software, networks, personnel, and organization. The research focuses on risk assessment and providing recommendations for information security risk management. Analysis of residual risk and cost of risk mitigation are not within the scope of this research.

## 2. Risk Assessment

The next stage in this research involves assessing the risks associated with all assets identified in the previous stage. Risk assessment is conducted based on the international standard ISO/IEC 27005:2022, which comprises three stages: risk identification, risk analysis, and risk evaluation.

### 2.1. Risk Identification

Risk identification is the process of discovering, recognizing, and describing risks. The goal of risk identification is to generate a list of risks based on events that could hinder, disrupt, or delay the achievement of organizational objectives. Several steps are involved in risk identification, including identifying assets, identifying threats, identifying existing controls, and identifying vulnerabilities [14].

#### 2.1.1. Asset Identification

Assets are defined as everything that has value to the organization [15]. In this study, asset identification involves recording all assets involved in business and operational activities at Pusdatin Setkab. Identified assets are categorized and assigned asset codes for further reference. There are 52 identified assets in total, comprising 12 primary assets and 40 supporting assets. Referring to the asset classification in ISO/IEC 27002:2022, the primary assets consist of eight Information assets and four Business Process assets. The supporting assets include eight

Hardware assets, 20 software assets, six network assets, three personnel assets, two location assets, and one organizational asset.

### 2.1.2. Threat Identification

Threat identification process is carried out by referring to the list of threats listed in Annex A of ISO/IEC 27005:2022. A total of 30 threats were identified, categorized as follows: three Physical Threats, two Natural Threats, three Infrastructure Failures, three Technical Failures, 13 Human Actions, three Compromise of Functionality or Services, and three Organizational Threats.

### 2.1.3. Existing Control Identification

The controls implemented on assets were identified through FGD with reference to the list of controls listed in Annex A of ISO/IEC 27001:2022. Based on the discussion outcomes, 30 controls were found to have been implemented on assets.

### 2.1.4. Vulnerability Identification

The list of vulnerabilities was identified through FGD and analysis of relevant documents. The reference used for identifying vulnerabilities in this process is Annex A of ISO/IEC 27005:2022. Based on the discussion outcomes, 24 vulnerabilities were identified.

## 2.2. Risk Analysis

The risk analysis stage is the next step after completing the risk identification process. In this stage, a total of 340 risks were identified. Based on the risk levels, it was found that there are 247 risks (73%) categorized as very low severity, while two risks (1%) are categorized as very high severity. **Figure 2** illustrates the distribution of risk levels.

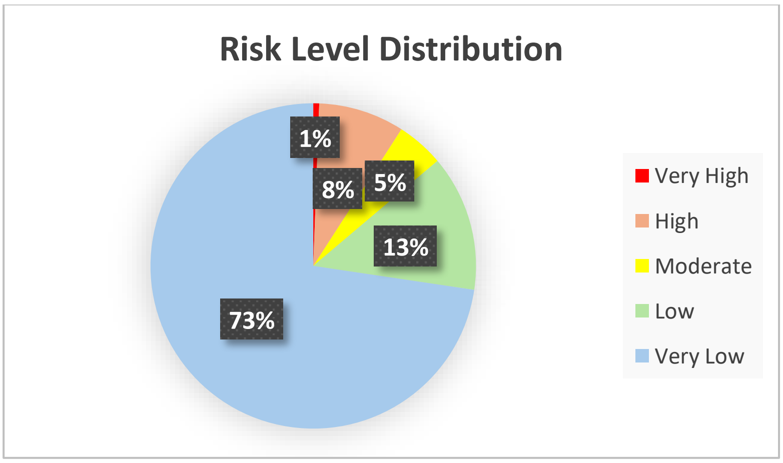

**Figure 2.** Risk Level Distribution

## 2.3. Risk Evaluation

After calculating the risk level and comparing it with the risk evaluation criteria, particularly the risk acceptance criteria [14], decisions regarding risk acceptance and treatment are made. According to PermenPAN RB

Number 5 of 2020, prioritization of risk treatment is determined considering the risk magnitude [4]. Decisions on risk acceptance and treatment are made based on confirmation from each risk owner. Based on the risk evaluation results, there are 93 risks that require mitigation, while 247 risks can be accepted.

## 3. Risk Treatment

The selection of risk treatment options to be mitigated should be based on the results of the risk assessment, estimated costs for implementing these options, and the expected benefits of each option, both individually and in the context of other controls. Risk treatment must be prioritized based on the established risk magnitude, time constraints, required implementation sequence, and the results of previous risk evaluations [14]. In this study, the risk treatment options used are sourced from the Guidelines for Risk Management of SPBE [4], namely: Risk Escalation, Risk Mitigation, Risk Transfer, Risk Avoidance, and Risk Acceptance. The choice of controls to mitigate risks refers to ISO/IEC 27002:2022, with a total of 57 recommended controls established. The recommendation excludes residual risk and cost-benefit analysis. More details on the recommendation are available in **Table 5**.

**Table 5.** Control Recommendations

| Control Code | Control Recommendation | ISO/IEC 27002:2022 Reference |
|---|---|---|
| [C1] | Implementing secure coding practices. | 8.28 Secure coding |
| [C2] | Conducting comprehensive security testing of software during the development phase. | 8.29 Security testing in development and acceptance |
| [C3] | Ensuring that all changes to software and infrastructure are formally tested and approved before implementation into the production environment. | 8.32 Change management |
| [C4] | Developing and implementing change management procedures to ensure that all changes to firewall configurations are identified, documented, tested, approved, and adequately communicated before implementation. | 8.32 Change management |
| [C5] | Developing and implementing change management procedures to ensure that all changes to policies, procedures, and configurations affecting storage media encryption are documented, tested, approved, and effectively communicated before implementation. | 8.32 Change management |
| [C6] | Developing and implementing change management procedures to ensure that all changes to VPN configurations are identified, documented, tested, approved, and adequately communicated before implementation. | 8.32 Change management |
| [C7] | Implementing strict configuration management for firewalls, including maintaining accurate configuration documentation, monitoring configuration changes, and verifying that firewall configurations comply with security policies. | 8.9 Configuration management |
| [C8] | Documenting operational procedures that include steps for managing changes related to storage media | 5.37 Documented operating procedures |

| Control Code | Control Recommendation | ISO/IEC 27002:2022 Reference |
|---|---|---|
| | encryption, ensuring all changes are implemented according to documented procedures. | |
| [C9] | Implementing automated monitoring mechanisms to detect firewall configuration changes and immediately alerting if unauthorized changes occur. | 8.9 Configuration management |
| [C10] | Implementing appropriate cryptographic controls to protect exempted data/information, ensuring storage media is encrypted using strong cryptographic algorithms and managed securely. | 8.24 Use of cryptography |
| [C11] | Implementing encryption to protect sensitive data traffic between clients and servers. Use protocols such as TLS (Transport Layer Security) to ensure data integrity and confidentiality during transmission. | 8.24 Use of cryptography |
| [C12] | Maintaining comprehensive records of all firewall configuration changes, including who made the changes, when, and why the changes were made. | 8.15 Logging |
| [C13] | Monitoring firewall configuration changes in real-time to detect unauthorized or undesired activities and ensure compliance with change management procedures. | 8.16 Monitoring activities |
| [C14] | Implementing continuous network monitoring to detect and respond to attempts of data tampering or modification. | 8.16 Monitoring activities |
| [C15] | Actively monitoring activities on websites & applications to quickly detect and respond to cyber attacks or suspicious behaviors. | 8.16 Monitoring activities |
| [C16] | Implementing continuous network monitoring to detect and respond to attempts of data tampering or modification. | 8.16 Monitoring activities |
| [C17] | Deploying firewall and intrusion detection/prevention systems (IDS/IPS) to protect the network from unauthorized access and malicious activities that could alter data. | 8.20 Networks security |
| [C18] | Conducting regular security testing, including scanning and malware checks. | 8.33 Test information |
| [C19] | Installing and enabling up-to-date and reliable anti-malware software on all devices. | 8.7 Protection against malware |
| [C20] | Ensuring that firewall software and other related firewall operation software are always updated with the latest patches to address known security vulnerabilities. | 8.7 Protection against malware |
| [C21] | Implementing policies and procedures to manage and audit physical access to premises, including recording who has access, when access is granted or revoked, and the reasons for access. | 5.15 Access control |
| [C22] | Implementing role-based access controls to ensure that only authorized personnel can access sensitive documents. Conducting regular reviews and adjustments of access rights. | 5.15 Access control |
| [C23] | Performing security checks on everyone entering storage areas, including identity verification and purpose of visit inspections. | 7.2 Physical entry |
| [C24] | Performing security checks on everyone entering the Data Center, including identity verification and purpose of visit inspections. | 7.2 Physical entry |

| Control Code | Control Recommendation | ISO/IEC 27002:2022 Reference |
|---|---|---|
| [C25] | Implementing door locking systems and access card usage to restrict access to critical areas only to authorized personnel. | 7.3 Securing offices, rooms and facilities |
| [C26] | Installing surveillance cameras in critical areas to monitor activities and enable quick response to threats or incidents. | 7.3 Securing offices, rooms and facilities |
| [C27] | Ensuring the data center rooms are equipped with air drying and good air circulation systems to reduce the risk of humidity that can damage devices. | 7.3 Securing offices, rooms and facilities |
| [C28] | Installing surveillance cameras and physical security monitoring systems to monitor activities in critical areas. | 7.4 Physical security monitoring |
| [C29] | Deploying a physical security monitoring system that continuously monitors the surrounding environment to detect suspicious activities or disaster threats. | 7.4 Physical security monitoring |
| [C30] | Installing sensors and monitoring systems to monitor temperature and humidity conditions inside the Data Center in real-time. Notifications are configured to alert personnel if significant temperature or humidity changes occur. | 7.4 Physical security monitoring |
| [C31] | Installing a real-time power supply monitoring system to detect anomalies or disruptions that may cause power loss. | 7.4 Physical security monitoring |
| [C32] | Installing smoke sensors connected to the monitoring system to promptly detect fires and provide early warnings to personnel on duty. | 7.4 Physical security monitoring |
| [C33] | Installing humidity sensors connected to the monitoring system to provide early warnings if humidity in the data center area exceeds safe thresholds. | 7.4 Physical security monitoring |
| [C34] | Installing surveillance cameras and physical security monitoring systems to monitor activities in critical areas. | 7.4 Physical security monitoring |
| [C35] | Conducting inspection and verification of software code to be installed on operational systems. | 8.19 Installation of software on operational systems |
| [C36] | Develop and implement a Business Continuity Plan (BCP) that includes pandemic scenarios. This plan should outline procedures for handling personnel absences and ensuring business operations continue uninterrupted. | 5.30 ICT readiness for business continuity |
| [C37] | Develop disaster recovery strategies enabling rapid restoration of data center operations following natural disasters. | 5.30 ICT readiness for business continuity |
| [C38] | Plan and train teams to respond quickly and effectively to fire-related disasters to minimize impacts on business operations. | 5.30 ICT readiness for business continuity |
| [C39] | Implement effective identity management processes to manage the employee identity lifecycle, including creation, maintenance, and deletion of identities and access rights. | 5.16 Identity management |
| [C40] | Implement role-based access controls to ensure employees only have access to information and systems necessary for their tasks, including conducting regular reviews and adjustments of access rights. | 5.16 Identity management |

| Control Code | Control Recommendation | ISO/IEC 27002:2022 Reference |
|---|---|---|
| [C41] | Conduct regular training for all employees on the importance of information security. | 6.3 Information security awareness, education and training |
| [C42] | Provide routine training to employees on the importance of "clear desk" and "clear screen" policies and the consequences of policy violations. | 7.7 Clear desk and clear screen |
| [C43] | Establish policies allowing employees to work from home or other secure locations. | 6.7 Remote working |
| [C44] | Create a disaster emergency plan outlining steps to be taken in response to natural disasters such as floods, earthquakes, or storms. | 5.24 Information security incident management planning and preparation |
| [C45] | Develop an emergency response plan covering actions to be taken in the event of cooling or ventilation system failures. | 5.24 Information security incident management planning and preparation |
| [C46] | Develop an emergency plan that includes steps to handle critical service delivery failures, including procedures for quick recovery. | 5.24 Information security incident management planning and preparation |
| [C47] | Create an emergency plan that includes steps to address damage caused by fire, including device evacuation and data recovery. | 5.24 Information security incident management planning and preparation |
| [C48] | Create an emergency plan that includes steps to address damage caused by water, including device evacuation and data recovery. | 5.24 Information security incident management planning and preparation |
| [C49] | Develop a disaster emergency plan outlining steps to be taken in response to natural disasters such as floods, earthquakes, or storms. | 5.24 Information security incident management planning and preparation |
| [C50] | Establish a regular maintenance schedule for cooling and ventilation systems, including routine inspections, preventive maintenance, and repairs as needed. | 7.13 Equipment maintenance |
| [C51] | Establish clear and documented policies for the disposal of exempted data/information, including appropriate procedures to ensure that data/information is securely deleted before its storage media is discarded or recycled. | 7.14 Secure disposal or re-use of equipment |
| [C52] | Encrypt sensitive data before disposing of exempted data/information. | 8.12 Pencegahan kebocoran data |
| [C53] | Conduct comprehensive security testing on websites and applications to identify and address existing security vulnerabilities. | 8.26 Application security requirements |
| [C54] | Regularly scan websites and applications to identify new and existing security vulnerabilities and take appropriate actions. | 8.8 Management of technical vulnerabilities |
| [C55] | Define the roles and responsibilities of each employee related to information security. Ensure employees understand their responsibilities and the importance of adhering to information security policies and procedures. | 5.2 Information security roles and responsibilities |
| [C56] | Segregate critical tasks to prevent misuse of authority. | 5.3 Segregation of duties |
| [C57] | • Separate development, testing, and production environments and ensure testing is conducted in a secure and controlled environment. | 8.31 Separation of development, test and production environments |

| Control Code | Control Recommendation | ISO/IEC 27002:2022 Reference |
|---|---|---|
| | • Restrict access to the production environment to authorized personnel only. | |

## D. Conclusion

The final outcome of this research is the design of information technology risk management for the Setkab. The research method used is qualitative, where data was collected through interviews, discussions, direct observations, and document analysis within the Setkab organization. The design includes steps such as defining the context, risk assessment involving the identification of assets, threats, existing controls, and vulnerabilities, as well as risk analysis, evaluation, and treatment along with the design of its implementation.

The information technology risk management process at Setkab adopts the framework from ISO/IEC 27005:2022, which provides guidance for implementing risk management in the context of information security as per ISO 31000. The fundamental criteria for risk management refer to two main regulations, namely PermenPAN RB Regulation Number 5 of 2020 concerning Guidelines for Risk Management of SPBE and Perseskab Regulation Number 1 of 2019 concerning Risk Assessment Guidelines in the Secretariat Cabinet environment. The risk assessment process continues to follow ISO/IEC 27005:2022 guidelines, while ISO/IEC 27002:2022 is used to establish controls in the risk treatment plan and recommend controls.

## E. References

[1] Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia*. 2019. [Online]. Available: https://jdih.setkab.go.id/PUUdoc/175860/Perpres_Nomor_39_Tahun_2019.pdf

[2] Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*. 2018. [Online]. Available: https://jdih.setkab.go.id/PUUdoc/176771/Salinan_Perpres_Nomor_95_Tahun_2022.pdf

[3] Republik Indonesia, *Peraturan Presiden Republik Indonesia Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik*. 2022. [Online]. Available: https://jdih.setkab.go.id/PUUdoc/176876/Salinan_Perpres_Nomor_132_Tahun_2022.pdf

[4] Kementerian PANRB, *Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik*. 2020. [Online]. Available: https://peraturan.bpk.go.id/Details/143664/permen-pan-rb-no-5-tahun-2020

[5] Sekretaris Kabinet, *Peraturan Sekretaris Kabinet Nomor 1 Tahun 2020 tentang Organisasi dan Tata Kerja Sekretariat Kabinet*. 2020. [Online]. Available:

https://jdih.setkab.go.id/PUUdoc/176658/Perseskab_Nomor_2_Tahun_2022.pdf

[6] Sekretariat Kabinet Republik Indonesia, *Rencana Strategis Renstra Sekretariat Kabinet Tahun 2020-2024*. 2020. Accessed: Sep. 13, 2023. [Online]. Available: https://jdih.setkab.go.id/PUUdoc/176438/Perseskab_Nomor_4_Tahun_2021.pdf

[7] V. S. Kasma, S. Sutikno, and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019: (Trial Implementation in Badan XYZ)," *Proceeding - 2019 International Conference on ICT for Smart Society: Innovation and Transformation Toward Smart Region, ICISS 2019*, Nov. 2019, doi: 10.1109/ICISS48059.2019.8969808.

[8] D. I. Sensuse, A. Syahrizal, F. Aditya, and M. Nazri, "Information security risk management planning of digital certificate management case study: Balai sertifikasi elektronik," *2020 5th International Conference on Informatics and Computing, ICIC 2020*, Nov. 2020, doi: 10.1109/ICIC50835.2020.9288593.

[9] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Comput Sci*, vol. 161, pp. 1206–1215, Jan. 2019, doi: 10.1016/J.PROCS.2019.11.234.

[10] I. M. M. Putra and K. Mutijarsa, "Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005," *3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021*, pp. 14–19, Apr. 2021, doi: 10.1109/EICONCIT50028.2021.9431865.

[11] I. Akkiyat and N. Souissi, "Modelling Risk Management Process According to ISO Standard," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2, Jul. 2019, doi: 10.35940/ijrte.B3751.078219.

[12] J. Recker, *Scientific Research in Information Systems: A Beginner's Guide*. in Progress in IS. Springer International Publishing, 2021.

[13] V. Braun and V. Clarke, *Thematic Analysis: A Practical Guide*. SAGE, 2022.

[14] International Organization for Standardization, *ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. 2022. Accessed: Mar. 25, 2023. [Online]. Available: https://www.iso.org/standard/80585.html

[15] International Organization for Standardization, *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. 2022. Accessed: Mar. 25, 2023. [Online]. Available: https://www.iso.org/standard/75652.html