JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. x, No. x, April 2025, pp. x-x p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

INFORMATION SECURITY RISK MATURITY ASSESSMENT OF CENTRAL JAVA DATA CENTER BASED ON GOVERNMENT REGULATIONS AND ISO 27001:2022

Fajar Andy Daniarta[1], Aji Supriyanto[2*]

[1,2] Magister Teknologi Informasi, Universitas STIKUBANK, Semarang, Indonesia
Email: [1]fajarandy0015@mhs.unisbank.ac.id, [*2]ajisup@edu.unisbank.ac.id

(Received: ... Oktober 2025, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

The rapid development of Information and Communication Technology (ICT) has significantly transformed public administration through the implementation of Electronic-Based Government Systems (SPBE). SPBE aims to establish open, participatory, and accountable governance and enhance public service quality through integrated digital infrastructures. However, such integration also introduces potential information security risks related to the confidentiality, integrity, and availability of public data. This study evaluates the maturity level of information security risk management at the Central Data Center of Central Java Province, Indonesia, using the Indonesian Government Regulation (PermenPANRB No. 5/2020) on SPBE Risk Management and the international standard SNI ISO/IEC 27001:2022. A qualitative descriptive approach was applied through observation, interviews, and survey-based assessments using a questionnaire aligned with ISO/IEC 27001:2022 control domains. The maturity model used consists of five levels: Level 1 (Initial) – ad hoc and undocumented processes; Level 2 (Repeatable but Intuitive) – basic yet informal processes; Level 3 (Defined Process) – standardized and documented processes; Level 4 (Managed and Measurable) – processes are monitored and measured; and Level 5 (Optimized) – continuous improvement and innovation are systematically implemented. Findings show that the Data Center's information security maturity lies between "Managed and Measurable" (Level 4) and "Optimized" (Level 5) across most sub-controls. This indicates that security policies and procedures are effectively and measurably implemented, though continuous evaluation and improvement remain essential. The results emphasize the importance of enhancing human resource capabilities, strengthening risk management mechanisms, and maintaining a culture of continuous improvement to achieve optimal information security maturity.

Keywords: *SPBE, information security, risk management, ISO/IEC 27001:2022, maturity assessment, Central Data Center*

**Corresponding Author: Author1*

1. INTRODUCTION

The rapid development of Information and Communication Technology (ICT) has significantly transformed public administration through the implementation of the Electronic-Based Government System (SPBE). The primary objective of SPBE is to realize open, participatory, innovative, and accountable governance while improving the quality of public services. The implementation of SPBE is regulated under Presidential Regulation No. 95 of 2018, which emphasizes the utilization of information technology to support digital public services. However, the implementation of SPBE also introduces various risks, particularly related to information security and the continuity of digital government services [1][2].

To mitigate these risks, the government issued Ministerial Regulation of Administrative and Bureaucratic Reform (PermenPANRB) No. 5 of 2020 concerning Guidelines for SPBE Risk Management. This regulation serves as a systematic framework for government institutions to identify, analyze, and control risks arising from SPBE implementation. It also emphasizes the importance of cultivating a risk-aware culture and establishing a measurable and

accountable risk management structure [3]. In this context, information security has become a critical issue. According to the National Cyber and Crypto Agency (BSSN, 2024), the most frequent cybersecurity incidents include data breaches and ransomware attacks, with the government administration sector being the most affected. Therefore, assessing the level of information security maturity is essential to maintain confidentiality, integrity, and availability of information [4].

Previous research conducted at the Regional Revenue Agency (Bapenda) of Central Java Province by Aminudin & Supriyanto in 2024 adopted the NIST Cybersecurity Framework and the ISO/IEC 27001:2013 standard to assess information security maturity. However, this framework is relatively generic and not fully aligned with the specific context of Indonesian digital governance [5]. Hence, this study employs the PermenPANRB No. 5 of 2020 framework as the primary reference for SPBE risk management tailored to the Indonesian government context, while information security controls are based on SNI ISO/IEC 27001:2022, an updated version of the 2013 standard that is more adaptable to current cybersecurity challenges [2][6].

Furthermore, this research integrates the Information Security Index (KAMI Index) developed by BSSN as a quantitative instrument to measure the readiness and maturity level of information security implementation in government agencies. The integration of PermenPANRB No. 5/2020, the KAMI Index, and SNI ISO/IEC 27001:2022 enables a comprehensive and complementary process of risk identification, maturity measurement, and implementation of security controls [7][8][9]. This integrated approach is expected to strengthen information security governance, particularly within the Central Java Provincial Data Center, in supporting the sustainability of secure, efficient, and accountable digital government services.

2. RESEARCH METHOD

Broadly speaking, this study follows the framework of Ministerial Regulation of the State Apparatus Empowerment and Bureaucratic Reform (Permen PANRB) Number 5 of 2020 concerning Risk Management in Government Agencies, with the aim of assessing the level of information security at the Central Java Provincial Data Center. Data collection was conducted through three main methods: observation, interviews, and surveys. Observations were conducted to identify actual conditions and potential security gaps, interviews were conducted with managers and stakeholders to gain an in-depth understanding of the implemented security system, while surveys were conducted to obtain quantitative data regarding perceptions and levels of understanding of information security practices based on the ISO/IEC 27001:2022 standard and Ministerial Regulation of the State Apparatus Empowerment and Bureaucratic Reform (Permen PANRB) Number 5 of 2020 [10].

The results of the three methods were then analyzed through several stages, from implementation and problem analysis to information asset risk assessment and mitigation. The assessment process was conducted by combining the approaches of Ministerial Regulation of Administrative and Bureaucratic Reform (PermenPANRB) 5/2020 and the ISO/IEC 27001:2022 standard to determine the level of vulnerability and the priority of risks that must be addressed. Mitigation was carried out by implementing controls contained in Annex ISO/IEC 27001:2022 to effectively manage information security risks. The final result of the study, an information asset assessment, provides an overview of the effectiveness of mitigation and the level of security achieved, and serves as a basis for formulating recommendations for future improvements to the information security system [11].

2.1 Data Collection

Data collection began with the distribution of questionnaires. The questionnaires were distributed and collected online using Google Forms to facilitate access for respondents from various locations. Data collection and completion time were one week, from the date of distribution until all responses were collected.

The instrument used in this study was a closed-ended questionnaire developed based on indicators from SNI ISO/IEC 27001:2022 and national regulations related to information security, such as the Minister of Administrative and Bureaucratic Reform's Regulation on SPBE and guidelines from the BSSN.

The questionnaire consists of 60 statements, which are divided based on the following sub-controls:

Table 1. Questions based on subcontrols

Subkontrol	Sumber Acuan
Kebijakan Keamanan Informasi	ISO/IEC 27001:2022, Annex A.5
Pengorganisasian Keamanan Informasi	Annex A.6
Manajemen Aset	Annex A.8
Kontrol Akses	Annex A.9
Kriptografi	Annex A.10
Keamanan Operasional	Annex A.12
Keamanan Komunikasi	Annex A.13
Akuisisi, Pengembangan, dan Pemeliharaan Sistem	Annex A.14
Hubungan dengan Pihak Ketiga	Annex A.15
Manajemen Insiden Keamanan Informasi	Annex A.16
Aspek Keamanan Informasi dalam Manajemen Keberlanjutan Bisnis	Annex A.17
Kepatuhan	Annex A.18
Keamanan Sumber Daya Manusia	Annex A.7

Keamanan Fisik dan Lingkungan	Annex A.11
Keamanan Jaringan	Annex A.13
Keamanan Informasi	ISO/IEC 27001:2022
Keamanan Data	ISO/IEC 27001:2022
Manajemen Risiko SPBE	PermenPANRB No. 5 Tahun 2020
Struktur Manajemen Risiko	PermenPANRB No. 5 Tahun 2020
Budaya Sadar Risiko	PermenPANRB No. 5 Tahun 2020
Pencatatan dan Pelaporan	PermenPANRB No. 5 Tahun 2020
Audit dan Review Sistem Keamanan Informasi	PermenPANRB No. 5 Tahun 2020
Penanganan Insiden SPBE	PermenPANRB No. 5 Tahun 2020
Pengelolaan Kontinuitas Layanan (BCM)	ISO/IEC 22301:2019, PermenPANRB No. 5 Tahun 2020

2.2 Maturity Level Scale

The CMMI Product Team, in its 2010 technical report on Improving Processes for Developing Better Products and Services, explained that maturity levels are well-defined stages of evolution toward achieving a mature software process. Each level encompasses a set of process areas that indicate an organization's focus on improving its processes.

The maturity level measurement scale used is outlined in Table 2 below [12].

Table 2. Maturity Level Scale

Level	Skala Maturity Index
0 - Non Existens	0% - 18%
1 - Initial /Adhoc	19% - 36%
2 - Repeateable but Intuitive	37% - 54%
3 – Defined	55% - 72%
4 - Managed and Measurable	73% - 90%
5 – Optimized	91% - 100%

2.3 Data Analysis Techniques

The data analysis technique process can be seen in Figure 1 below:

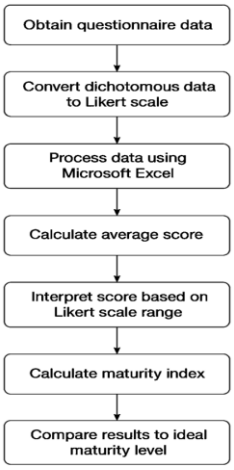

Figure 1. Data Analysis Techniques Flow

Data obtained from the questionnaires were analyzed quantitatively using descriptive and inferential approaches. Descriptive analysis was used to describe the level of information security management system implementation based on respondents' perceptions, while inferential analysis was used to examine relationships or differences between variables, if necessary.

Before analysis is carried out, the questionnaire data is first converted and normalized:

To maintain consistency with the data, the dichotomous data was converted to a Likert scale using the following guidelines [13][14]:

a) A "No" (0) response was converted to a value of 1 (Disagree)
b) A "Yes" (1) response was converted to a value of 5 (Strongly Agree)

This way, all respondent data could be analyzed using a uniform numeric scale (1–5).

Next, the converted data was processed using Microsoft Excel software to perform the following:

a) Calculate the average score (mean) for each indicator and variable. Each statement item was scored based on the respondent's answer. The average score (mean) was calculated for each sub-control and control domain, resulting in an aggregate score reflecting the maturity level of information security implementation.
b) Interpret the result categories based on the Likert scale range (e.g., disagree, somewhat agree, agree, strongly agree).

The maturity level analysis was conducted based on the five-level maturity model (5-Level Maturity Model) based on ISO/IEC 27001 and the SPBE guidelines from PermenPANRB No. 5 of 2020. To interpret the quantitative results, the average score for each sub-control was converted into a maturity level category according to the maturity level scale score range [15].

Then the calculation is carried out from the Maturity Value to the Maturity Index (%) because it refers to the maturity level scale table.

$$Maturity\ Index\ (\%) = \frac{Maturity\ Value}{5} \times 100 \qquad (1)$$

The average results for each sub-control and domain are used to determine the institution's information security maturity level. The overall score is obtained by averaging all sub-controls.

The final results are compared to the ideal maturity level (Level 5) to identify gaps and areas for improvement. The analysis is performed using statistical software such as Microsoft Excel to obtain accurate and measurable results.

3. RESULT AND DISCUSSION

3. 1 Maturity Level Analysis and Information Security Risks

The data collection process through distributing questionnaires to respondents is complete, the next step is data analysis. This analysis begins with a data cleaning process to ensure data accuracy and consistency. This involves removing incomplete data (noise) and transposing the data to conform to the analysis format. Next, qualitative data in the form of nominal answer choices is converted into numeric data according to a predetermined rating scale, allowing for quantitative processing. After the data transformation process is complete, a maturity level is calculated for each sub-control to measure the extent to which the implementation of policies and procedures complies with information security standards.

After analyzing the questionnaire distribution results, the average participant response was calculated for each section. This average was then used to determine the overall maturity level of the external respondents, as follows:

Table 3. Maturity Responder Results

Subcontrol	Maturity	Expected Maturity	GAP
1	4,66	4	-0,66
2	4,68	4	-0,68
3	4,56	4	-0,56
4	4,64	4	-0,64
5	3,68	4	0,32
6	4,56	4	-0,56
7	4,52	4	-0,52
8	4,56	4	-0,56
9	4,6	4	-0,6
10	4,8	4	-0,8
11	4,12	4	-0,12
12	4,36	4	-0,36
13	4,02	4	-0,02
14	4,76	4	-0,76
15	4,6	4	-0,6
16	4,44	4	-0,44
17	4,56	4	-0,56
18	4,68	4	-0,68
19	4,76	4	-0,76
20	4,56	4	-0,56
21	4,5	4	-0,5
22	4,26	4	-0,26
23	4,38	4	-0,38
24	4,04	4	-0,04
25	4,48	4	-0,48

From the results of the responder maturity calculations in 25 sub-controls which can be seen in Table 3, the average maturity calculation was then carried out in all sub-controls. The average result was 4,4712.

The visualization of the results of the maturity level is displayed in the form of a radar chart:

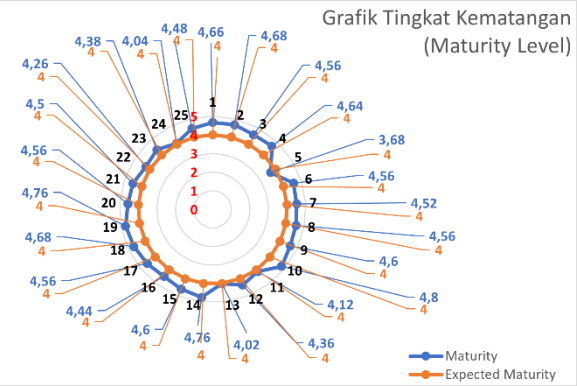

Figure 2. Maturity Level Chart

After obtaining the maturity level results for each sub-control, the next stage is to convert them to a maturity index (%). The overall maturity index (%) results for each sub-control.

Table 4. Maturity Index (%) Responder Results

Subcontrol	Maturity Index (%)
Kebijakan Keamanan Informasi	93,2
Pengorganisasian Keamanan Informasi	93,6
Manajemen Aset	91,2
Kontrol Akses	92,8
Kriptografi	73,6
Keamanan Operasional	91,2
Keamanan Komunikasi	90,4
Akuisisi, Pengembangan, dan Pemeliharaan Sistem	91,2
Hubungan dengan Pihak Ketiga	92
Manajemen Insiden Keamanan Informasi	96
Aspek Keamanan Informasi dalam Manajemen Keberlanjutan Bisnis	82,4
Kepatuhan	87,2
Keamanan Sumber Daya Manusia	80,4
Keamanan Fisik dan Lingkungan	95,2
Keamanan Jaringan	92
Keamanan Informasi	88,8
Keamanan Data	91,2
Manajemen Risiko SPBE (Sistem Pemerintahan Berbasis Elektronik)	93,6
Struktur Manajemen Risiko	95,2
Budaya Sadar Risiko	91,2
Pencatatan dan Pelaporan	90
Audit dan Review Sistem Keamanan Informasi	85,2
Penanganan Insiden SPBE (Permen PANRB 5/2020)	87,6
Pengelolaan Kontinuitas Layanan (BCM - Business Continuity Management)	80,8
Peningkatan Berkelanjutan (Continuous Improvement)	89,6

Next, determine the maturity level for each sub-control. The maturity index scale is measured (%).

Table 5. Maturity Level Scale

Level	Skala Maturity Index	Keterangan
0	0% - 18%	Non-Exixted
1	19% - 36%	Initial/Ad Hoc
2	37% - 54%	Repeatable But Invinitive
3	55% - 72%	Defined Process
4	73% - 90%	Managed and Measurable
5	91% - 100%	Optimized

3. 2 Research Result

Based on the ISO 27001:2022 standard, the expected maturity level in Indonesia is level four. The maturity score is obtained from the average respondent's answers to each sub-control. The results can be seen in the table below.

Table 6. Domain Maturity Level Scale According to ISO/IEC 27001:2022

Subcontrol	Maturity Level
Kebijakan Keamanan Informasi	Optimized
Pengorganisasian Keamanan Informasi	Optimized
Manajemen Aset	Optimized
Kontrol Akses	Optimized
Kriptografi	Managed and Measurable
Keamanan Operasional	Optimized
Keamanan Komunikasi	Managed and Measurable
Akuisisi, Pengembangan, dan Pemeliharaan Sistem	Optimized
Hubungan dengan Pihak Ketiga	Optimized
Manajemen Insiden Keamanan Informasi	Optimized
Aspek Keamanan Informasi dalam Manajemen Keberlanjutan Bisnis	Managed and Measurable
Kepatuhan	Managed and Measurable
Keamanan Sumber Daya Manusia	Managed and Measurable
Keamanan Fisik dan Lingkungan	Optimized
Keamanan Jaringan	Optimized
Keamanan Informasi	Managed and Measurable
Keamanan Data	Optimized
Manajemen Risiko SPBE (Sistem Pemerintahan Berbasis Elektronik)	Optimized
Struktur Manajemen Risiko	Optimized
Budaya Sadar Risiko	Optimized
Pencatatan dan Pelaporan	Managed and Measurable
Audit dan Review Sistem Keamanan Informasi	Managed and Measurable
Penanganan Insiden SPBE (Permen PANRB 5/2020)	Managed and Measurable
Pengelolaan Kontinuitas Layanan (BCM - Business Continuity Management)	Managed and Measurable
Peningkatan Berkelanjutan (Continuous Improvement)	Managed and Measurable

4. CONCLUSION

Based on the assessment results of 25 information security sub-controls referring to SNI ISO 27001:2022 and PANRB Regulation Number 5 of 2020, it can be concluded that the overall level of information security system maturity at the Central Java Provincial Data Center is in the Managed and Measurable category with an average value approaching the optimal level. These results indicate that most information security processes have been implemented systematically, documented, and performance measurements are conducted periodically. Several aspects, such as SPBE Risk Management, Risk Management Structure, and Risk Awareness Culture, have reached the Optimized level, indicating the implementation of best practices and continuous improvement. However, several sub-controls still require strengthening, particularly in the areas of incident management, continuous improvement, and human resource security awareness. Therefore, although the foundation of information security governance has been well established, improvement efforts through regular training, internal audits, and continuous policy updates are still needed to achieve the Optimized level of overall maturity and ensure the sustainability of information security within the regional government environment.

5. REFERENCE

[1] Presiden Republik Indonesia, "Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik," *Menteri Huk. Dan Hak Asasi Mns. Republik Indones.*, p. 110, 2018.

[2] D. Harisdayanti, R. Fauzi, and R. Mulyana, "Perancangan Manajemen Risiko Operasional Pada Spbe/E-Gov Berdasarkan Permen Panrb Nomor 5 Tahun 2020: Studi Kasus Pemerintah Kabupaten Bandung Operational Risk Management Design on E-Gov/Spbe Based on Permen Panrb Nomor 5 Tahun 2020: Case Study Government," vol. 7, no. 2, pp. 7348–7353, 2020.

[3] MenPANRB RI, "PermenPAN RB Nomor 5 Tahun 2020," *MenPAN RB, JDIH*, vol. 5, no. 261, pp. 1689–1699, 2020.

[4] Badan Siber dan Sandi Negara, "Laporan Monitoring Keamanan Siber Bulan Agustus 2024," 2024, [Online]. Available: https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

[5] A. Aminudin and A. Supriyanto, "Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah)," *Aiti*, vol. 21, no. 2, pp. 210–229, 2024, doi: 10.24246/aiti.v21i2.210-229.

[6] S. N. Indonesia, "privasi — Sistem manajemen keamanan informasi — Persyaratan Information security , cybersecurity and privacy protection — Information security management systems — Requirements," vol. 2022, 2023.

[7] Z. S. Nadine, I. Aknuranda, and H. Farizi, "Evaluasi Pengelolaan Keamanan Informasi Berbasis," vol. 9, no. 10, pp. 1–12, 2025.

[8] A. R. Nugroho and N. Legowo, "Risk Assessment at it Company by Focusing on Information Security Area Using Iso 27001:2022," vol. 07, no. 12, 2022.

[9] A. Supriyanto, A. Jananto, J. A. Razaq, B. Hartono, and F. Damaryanti, "Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation," *Cybern. Inf. Technol.*, vol. 25, no. 2, pp. 173–192, 2025, doi: 10.2478/cait-2025-0018.

[10] T. Ramadhane, "Public Value Based E-Government Maturity Model: a Literature Review," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 1, pp. 62–71, 2023, doi: 10.33387/jiko.v6i1.5898.

[11] A. La Adu, "Evaluation of Spbe Service Maturity Level in Central Maluku District Government Using Spbe 2020 Framework," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 1, pp. 13–20, 2023, doi: 10.33387/jiko.v6i1.5422.

[12] C. Development, "CMMI ® for Development, Version 1.3," no. November, 2010.

[13] V. H. Pranatawijaya, W. Widiatry, R. Priskila, and P. B. A. A. Putra, "Penerapan Skala Likert dan Skala Dikotomi Pada Kuesioner Online," *J. Sains dan Inform.*, vol. 5, no. 2, pp. 128–137, 2019, doi: 10.34128/jsi.v5i2.185.

[14] A. Suárez-García, M. Álvarez-Hernández, E. Arce, and J. R. Ribas, "Exploring the Efficacy of Binary Surveys versus Likert Scales in Assessing Student Perspectives Using Bayesian Analysis," *Appl. Sci.*, vol. 14, no. 10, 2024, doi: 10.3390/app14104189.

[15] Nurbojatmiko *et al.*, "Risk Assessment Maturity Level of Academic Information System Using Iso 27001 System Security Engineering-Capability Maturity Model," *J. Appl. Eng. Technol. Sci.*, vol. 5, no. 2, pp. 941–954, 2024, doi: 10.37385/jaets.v5i2.2971.