JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. 9, No. 1, April 2026, pp. 10-14 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v9i1.10965 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] Master of Information Technology, Faculty of Information Technology and Industry, Universitas Stikubank, Semarang, 50241, Indonesia
Email: [1]fajarandy0015@mhs.unisbank.ac.id, *[2]ajisup@edu.unisbank.ac.id

(Received: 07 November 2025, Revised: 09 December 2025, Accepted: 17 December 2025)

Abstract

The increasing use of E-government (SPBE) has accelerated digital change in public administration but has also created real risks to information security. This study aims to evaluate the level of information security risk management maturity at the Central Java Provincial Data Center by merging the Indonesian SPBE Risk Management framework (PermenPANRB No. 5/2020) with SNI ISO/IEC 27001:2022. The evaluation utilized a descriptive qualitative method, backed by observations, interviews, and a survey-based maturity assessment that aligns with the control areas of ISO/IEC 27001. Findings reveal that the overall maturity sits between "Managed and Measurable" (Level 4) and "Optimized" (Level 5), indicating that most procedures are organized, documented, and consistently observed; however, some sub-controls still need enhancement, especially those related to incident response, ongoing improvement, and staff awareness. This research emphasizes the necessity for a more flexible security governance approach and contributes by integrating national regulatory guidelines with global information security frameworks to enhance the maturity assessment of government data centers.

Keywords: *SPBE, information security, ISO/IEC 27001:2022, risk maturity, government data center*

**Corresponding Author: Aji Supriyanto*

1. INTRODUCTION

The use of e-Governemnt (Electronic-Based Government Systems /SPBE) has accelerated the shift to digital practices in Indonesian public administration. Nevertheless, this change also raises the risk of information security threats, especially concerning the confidentiality, integrity, and accessibility of public sector information. According to the National Cyber and Crypto Agency (BSSN, 2024), government agencies continue to be one of the most commonly attacked areas in cybersecurity events, including data leaks and ransomware strikes.

To mitigate these challenges, the Indonesian government released PermenPANRB No. 5/2020, which sets up an organized system for managing SPBE risks. Nevertheless, current studies typically depend on broad frameworks like the NIST Cybersecurity Framework or the older ISO/IEC 27001:2013 standard, which do not adequately capture the regulatory and operational environment of Indonesian e-government. Moreover, earlier investigations seldom combine national guidelines (PermenPANRB No. 5/2020), global standards (ISO/IEC 27001:2022), and local maturity assessment tools such as the KAMI Index, leading to a gap between policy requirements and actual execution at government data centers.

This research addresses these shortcomings by merging PermenPANRB No. 5/2020, ISO/IEC 27001:2022, and the KAMI Index into a unified maturity assessment framework for government data centers. This combined strategy offers a more relevant assessment and aligns with both regulatory requirements and global best practices.

Consequently, this research intends to:

1. Assess the level of maturity in information security according to SPBE and ISO/IEC 27001:2022 standards.
2. Recognize discrepancies between anticipated and current maturity levels.
3. Offer suggestions for enhancing the governance of information security in governmental data centers.

2. RESEARCH METHOD

This research utilizes a qualitative descriptive method, along with quantitative maturity assessments. The evaluation framework combines the SPBE Risk Management Guidelines (PermenPANRB No. 5/2020) and SNI ISO/IEC 27001:2022 to analyze the maturity of information security at the Data Center of the Central Java Province.

2.1 Data Collection

Information was gathered using three methods:

1. Observations to recognize current security methods and the state of the infrastructure.
2. Semi-structured discussions with leaders and key stakeholders to gather information about governance and risk management procedures.
3. Survey questionnaires sent out through Google Forms to security professionals and administrators of information systems. The tool included 60 statements aligned with 25 sub-controls based on ISO/IEC 27001:2022 and PermenPANRB 5/2020.

All replies to the questionnaire utilized a 1 to 5 Likert scale. Responses with two options (Yes/No) were transformed according to Pranatawijaya et al. (2019), assigning Yes a value of 5 and No a value of 1, to maintain uniformity in the data.

The questionnaire consists of 60 statements, which are divided based on the following sub-controls in Table 1.

Table 1. Questions based on subcontrols

Subcontrol	Reference Source
Information Security Policy	ISO/IEC 27001:2022, Annex A.5
Information Security Organization	Annex A.6
Asset Management	Annex A.8
Access Control	Annex A.9
Cryptography	Annex A.10
Operational Security	Annex A.12
Communication Security	Annex A.13
System Acquisition, Development, and Maintenance	Annex A.14
Third-Party Relationships	Annex A.15
Information Security Incident Management	Annex A.16
Information Security Aspects in Business Continuity Management	Annex A.17
Compliance	Annex A.18
Human Resource Security	Annex A.7
Physical and Environmental Security	Annex A.11
Network Security	Annex A.13
Information Security	ISO/IEC 27001:2022
Data Security	ISO/IEC 27001:2022
SPBE Risk Management	PermenPANRB No. 5 Tahun 2020
Risk Management Structure	PermenPANRB No. 5 Tahun 2020
Risk Awareness Culture	PermenPANRB No. 5 Tahun 2020
Recording and Reporting	PermenPANRB No. 5 Tahun 2020
Information Security System Audit and Review	PermenPANRB No. 5 Tahun 2020
SPBE Incident Handling	PermenPANRB No. 5 Tahun 2020
Service Continuity Management (BCM)	ISO/IEC 22301:2019, PermenPANRB No. 5 Tahun 2020

2.2 Maturity Measurement

The maturity level was assessed using a five-level scale based on ISO/IEC 27001 and SPBE risk management guidelines in Table 2.

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%

For every sub-control, the average score was determined, transformed into a maturity index (%), and aligned with the maturity level index. The anticipated maturity level for government organizations in Indonesia is identified as Level 4 (Managed and Measurable).

2.3 Data Analysis Techniques

The data analysis technique process can be seen in Figure 1.

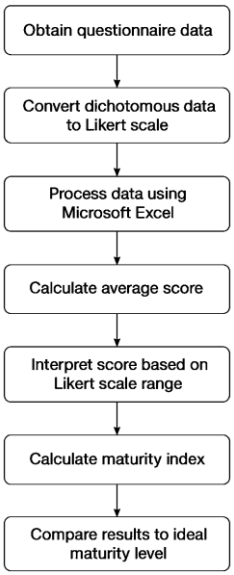

Figure 1. Data Analysis Techniques Flow

Following the cleaning and standardization of data, Microsoft Excel was used to handle the findings by:

- Calculating average scores for each sub-control.
- Turning values into maturity indexes.
- Recognizing discrepancies between actual and anticipated levels.
- Representing the findings with radar graphs.

The results were assessed by comparing them to regulatory benchmarks, ISO guidelines, and earlier research to recognize advantages, disadvantages, and

opportunities for enhancement.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 Results

Following the evaluation of 25 information security sub-controls, the total maturity rating was 4.47, categorizing it as "Managed and Measurable," nearing Level 5 (Optimized). The majority of the sub-controls have been methodically implemented and are backed by monitoring and policy documentation. Specific sub-controls such as Risk Management Structure, SPBE Risk Management, and Risk-Aware Culture have attained Level 5, reflecting high-level implementation and conformity with industry best practices. Nevertheless, there are several aspects that are still at Level 4, especially in incident management, continuous improvement, and awareness of human resource security, indicating the need for regular assessments and enhancement of capabilities.

In relation to the SPBE maturity standards set by PermenPANRB No. 5/2020, the data center currently satisfies the basic criteria for Level 4 (Managed and Measurable). However, there are still ways to enhance its performance for complete optimization.

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:

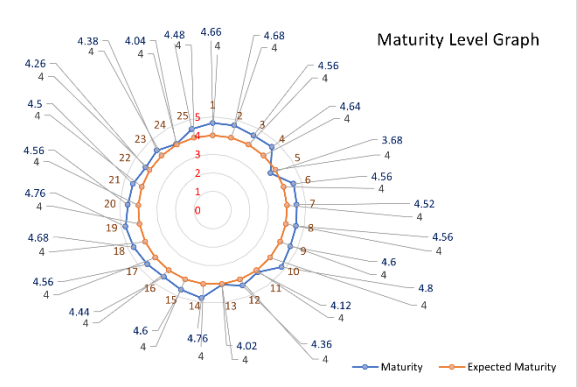

Figure 2. Maturity Level Graph

After obtaining the maturity level results for each sub-control, the next stage is to convert them to a maturity index (%). The results of the overall maturity index (%) for each sub-control can be seen in Table 4.

Table 4. Maturity Index (%) Responder Results

Subcontrol	Maturity Index (%)
Information Security Policy	93,2
Information Security Organization	93,6
Asset Management	91,2
Access Control	92,8
Cryptography	73,6
Operational Security	91,2
Communication Security	90,4
System Acquisition, Development, and Maintenance	91,2
Third-Party Relationships	92
Information Security Incident Management	96
Information Security Aspects in Business Continuity Management	82,4
Compliance	87,2
Human Resource Security	80,4
Physical and Environmental Security	95,2
Network Security	92
Information Security	88,8
Data Security	91,2
SPBE Risk Management	93,6
Risk Management Structure	95,2
Risk Awareness Culture	91,2
Recording and Reporting	90
Information Security System Audit and Review	85,2
SPBE Incident Handling	87,6
Service Continuity Management (BCM)	80,8

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 5.

Table 5. Domain Maturity Level Scale According to ISO/IEC 27001:2022

Subcontrol	Maturity Level
Information Security Policy	Optimized
Information Security Organization	Optimized
Asset Management	Optimized
Access Control	Optimized
Cryptography	Managed and Measurable
Operational Security	Optimized
Communication Security	Managed and Measurable
System Acquisition, Development, and Maintenance	Optimized
Third-Party Relationships	Optimized
Information Security Incident Management	Optimized
Information Security Aspects in Business Continuity Management	Managed and Measurable
Compliance	Managed and Measurable
Human Resource Security	Managed and Measurable
Physical and Environmental Security	Optimized
Network Security	Optimized
Information Security	Managed and Measurable
Data Security	Optimized
SPBE Risk Management	Optimized
Risk Management Structure	Optimized
Risk Awareness Culture	Optimized
Recording and Reporting	Managed and Measurable
Information Security System Audit and Review	Managed and Measurable
SPBE Incident Handling	Managed and Measurable
Service Continuity Management (BCM)	Managed and Measurable

3. 2 Comparison with Previous Studies

The results correspond with the work of [5], who indicated maturity ratings ranging from Level 3 to 4 when applying the NIST-CSF and ISO/IEC 27001:2013 framework within a provincial government organization. In contrast to that study, this research employs the revised ISO/IEC 27001:2022 standard and includes the SPBE regulation, offering a more relevant evaluation for Indonesian public sector settings.

Moreover, earlier research utilizing the KAMI Index such as [7] primarily concentrated on readiness scores while neglecting to incorporate regulatory risk management aspects. This research enhances that strategy by merging the KAMI Index with ISO/IEC 27001:2022 and PermenPANRB 5/2020, resulting in a more thorough maturity assessment.

Studies conducted by [10][11] highlighted the importance of aligning the governance frameworks of the public sector with maturity assessment models but fell short of providing a unified measurement that incorporates SPBE regulations and ISO standards. This study addresses that deficiency by implementing both frameworks within a cohesive measurement model.

Consequently, the significance of this research is in showcasing how regulatory and international standards can be consolidated into an effective maturity assessment model for government data centers – a methodological improvement not found in earlier studies.

4. CONCLUSION

This research evaluated the level of information security risk management maturity at the Central Java Provincial Data Center utilizing a blended framework of PermenPANRB No. 5/2020 alongside SNI ISO/IEC 27001:2022. The findings indicate that the overall maturity status is classified as Level 4 (Managed and Measurable), with various sub-controls reaching Level 5 (Optimized). These results validate that a majority of security procedures are executed in a systematic manner, are monitored, and are backed by proper documentation. Nonetheless, there is a need for enhancements in areas such as incident response, ongoing monitoring, and awareness of security to reach full optimization.

This study adds to methodology by merging national regulatory standards with global information security guidelines, thereby presenting a tailored maturity assessment model specifically for government data centers—a strategy that has not been utilized in earlier research.

On a practical level, the outcomes serve as a basis for decision-makers to focus on developing capacity, refining policies, and initiating internal audit processes. From an academic standpoint, this study broadens the scope of SPBE risk management research by showing how regulatory frameworks and ISO standards can be integrated in maturity analysis.

The limitations of this research include reliance on perception-based metrics and the focus on a single institutional case. Future studies could consider comparisons across multiple sites, the use of automated maturity assessment techniques, or the incorporation of quantitative risk analysis methods.

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.