Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

Integrated Maturity Assessment of Information Security for Land and Building Tax Management System Using National Institute of Standards and Technology Cybersecurity Framework 2.0, International Organization for Standardization/International Electrotechnical Commission 27002:2022, and Cybersecurity Capability Maturity Model 2.1.

Dhenok Prastyaningtyas Paramesvari[*1], Jatmiko Endro Suseno[2], Catur Edi Widodo[3]

[1,2,3]Master Program of Information Systems, Postgraduate School, Universitas Diponegoro, Indonesia

Email: [1]dhenokpp@gmail.com

Received : Dec 9, 2025; Revised : Dec 14, 2025; Accepted : Dec 14, 2025; Published : Apr 16, 2026

Abstract

Regional tax information systems such as the Sistem Informasi Manajemen Objek Pajak (SISMIOP) are vulnerable to cybersecurity threats due to the sensitivity of taxpayer data and the persistence of ad-hoc security management practices. These conditions pose risks to data confidentiality, integrity, and service availability, potentially undermining public trust and the effectiveness of local government services. This study aims to assess the information security maturity of SISMIOP operated by the Badan Pengelolaan Pendapatan, Keuangan, dan Aset Daerah (BPPKAD) through an integrated application of the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27002:2022, and the Cybersecurity Capability Maturity Model (C2M2) 2.1. A qualitative case study approach was employed. An organizational profile was developed using interviews, observations, and document analysis, followed by mapping 38 relevant NIST CSF subcategories to ISO/IEC 27002 controls and C2M2 capability domains. Security maturity was evaluated using questionnaires and interviews based on the C2M2 Maturity Indicator Levels (MIL0-MIL3), and a gap analysis was conducted against the target maturity level of MIL2. The results show that most cybersecurity functions, Govern, Identify, Detect, Respond, and Recover, remain at MIL1, indicating that practices are performed but not yet formalized or consistently implemented. The Protect function partially achieved MIL2. The largest gaps were identified in governance and risk management domains. Based on these findings, 38 prioritized strategic recommendations were formulated to improve policy formalization, risk management, technical controls, monitoring, and incident handling. This study contributes a practical and replicable multi-framework maturity assessment model to strengthen information security governance in public-sector tax information systems.

Keywords : *C2M2 Evaluation, Cybersecurity Maturity, Information Security Assessment, ISO/IEC 27002 Integration, NIST CSF Mapping, Public Sector Tax System.*

1. INTRODUCTION

Digital transformation has fundamentally reshaped public sector governance by driving operational efficiency, increasing transparency, and enabling more accountable and responsive public services. In an era that demands real-time and data-driven service delivery, information technology has become a central foundation supporting government performance, including regional revenue management. One of the strategic information systems utilized by the Regional Revenue, Finance, and Asset Management Agency (Badan Pengelolaan Pendapatan Keuangan dan Aset Daerah/BPPKAD) to support the registration, assessment, determination, and reporting processes of the Land and Building Tax is the Land and Building Tax Object Information Management System (SISMIOP) [1]. SISMIOP stores critical and sensitive information, such as taxpayer identities, property valuation data, and

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

payment histories, making it a vital asset whose security is essential for maintaining public trust in digital public services.

Given the high sensitivity of the data processed within SISMIOP, safeguarding information security is a priority, particularly in ensuring the confidentiality, integrity, and availability of services [2]. Security risks arise from both external threats, such as the exploitation of application vulnerabilities, and internal threats, including the misuse of privileged access. However, many public institutions in Indonesia still manage information security in a fragmented or ad-hoc manner, often without structured risk management practices [3]. As a result, organizations remain insufficiently prepared to face modern cybersecurity challenges, including the growing likelihood of strategic data breaches. Consequently, a comprehensive and systematic approach to information security is urgently required.

The Information Security Management System (ISMS) serves as a foundational approach for ensuring the strategic and sustainable protection of organizational information assets. Beyond safeguarding sensitive data, ISMS implementation enhances operational efficiency and strengthens information technology governance within public organizations [4], [5]. Its core objective is to ensure the consistent application of confidentiality, integrity, and availability as the fundamental pillars of information protection [6], while also supporting personal data protection efforts across sectors [7]. Several frameworks have been developed to guide information security governance, including the ISO/IEC 27000 series, the NIST Cybersecurity Framework (CSF), and the Cybersecurity Capability Maturity Model (C2M2) [8],[9],[10]. Each framework offers complementary strengths: ISO/IEC 27002 emphasizes technical controls, NIST CSF provides a function-based risk management structure, and C2M2 delivers a capability-oriented maturity assessment model [11].

Despite their respective advantages, no single framework fully integrates strategic governance, detailed technical controls, and systematic maturity measurement simultaneously [12], [13]. Therefore, an integrative multi-framework approach is considered more effective for evaluating and strengthening information security, particularly in government institutions where systems such as SISMIOP play a critical role. In this context, this study evaluates the information security posture of SISMIOP by integrating three complementary frameworks: NIST CSF as a strategic reference structured around six core functions [14], ISO/IEC 27002 as a set of actionable security controls [5], and C2M2 as a structured maturity measurement model ranging from MIL0 to MIL3 [15].

Previous studies, such as the comparative analysis of NIST-CSF and C2M2 [16], highlight the conceptual alignment and complementarities among cybersecurity maturity frameworks. However, these studies remain largely theoretical and do not evaluate maturity levels within real organizational environments or analyze gaps between current and target maturity states. Different from these approaches, this study implements an integrated assessment of NIST CSF 2.0, ISO/IEC 27002:2022, and C2M2 2.1 to empirically measure and address the maturity gap from MIL1 to MIL2 in a regional tax information system.

The objective of this research is to measure and evaluate the information security maturity level of SISMIOP operated by BPPKAD, identify critical gaps, and develop strategic recommendations for security improvement. This study proposes a comprehensive and replicable security evaluation model applicable to public-sector tax information systems in Indonesia. A qualitative methodology is employed through observations, interviews, document reviews, and questionnaires to obtain a holistic understanding of the current security posture and areas requiring enhancement.

2. RELATED WORK

Research on measuring information security maturity levels has been widely conducted, particularly in the public sector, which faces significant challenges due to increasing cyber threats. Numerous studies have examined various information security frameworks such as NIST CSF, ISO/IEC

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

27001/27002, CIS Controls, COBIT, and C2M2 either individually or in combination, to develop more comprehensive maturity assessment methods and security control models.

Tanjung et al [17] designed security controls for Indonesia's electronic-based government system (SPBE) by integrating NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Controls v8. Although the study successfully formulated 22 relevant control components, it focused solely on design and did not measure actual maturity levels within an organization. Bashofi and Salman [18] proposed a cybersecurity maturity assessment framework for Indonesian government institutions using an integrated approach of NIST CSF, ISO/IEC 27002, and CIS v8. While they identified 21 critical domains, the framework was not implemented in practice, nor did the study discuss specific gaps or organizational risks. Sulistyowati et al [19] compared several frameworks including NIST CSF, ISO/IEC 27002, COBIT, and PCI DSS and emphasized the need for consistent maturity indicators in government environments. However, the study produced only a conceptual framework without real-world implementation. Delgado et al. [20] examined the application of NIST CSF within public organizations in Peru and found weak adoption due to the absence of systematic policies. The maturity assessment relied primarily on perception-based evaluation, lacking deeper qualitative evidence.

A local study by Aminudin and Supriyanto [21] evaluated information security maturity in the Regional Revenue Agency (BAPENDA) of Central Java Province using NIST CSF and ISO/IEC 27001:2013. Although the study identified low maturity in areas such as security policy and incident management, it focused on a single institution and lacked expert validation. Fadya and Utama [22] combined NIST CSF and COBIT 2019, identifying 23 activity categories and 118 security practices. While the study highlighted the importance of continuous measurement, the resulting recommendations remained general and lacked prioritized mitigation strategies. Similarly, Zakiy and Angresti [16] explored the potential synergy between NIST CSF and C2M2 to develop a capability-based maturity assessment. However, the work remained conceptual and was not validated through field implementation. Amanda et al. [23] implemented a combination of NIST CSF and CMMI to assess information security maturity in an academic information system. The study focused only on the Identify function of NIST CSF, limiting its representation of the full security lifecycle. Afiansyah and Febriyani [24] presented a governance-based security policy model derived from the "Govern" domain of NIST CSF 2.0 and ISO/IEC 27001:2022. Their work reinforces the importance of governance but does not include the assessment of actual maturity levels. Finally, Nikhil et al. [25] developed the Enhanced Prioritized Gap Analysis (EPGA) by integrating NIST CSF and C2M2 to prioritize mitigation of vulnerabilities in critical infrastructures. Although analytically strong, the model requires significant resources and is less suitable for small to medium-sized public organizations.

Despite extensive research exploring various security framework integrations, no study to date has applied a comprehensive multi-framework maturity assessment specifically to local government tax administration systems such as SISMIOP.

3. RESEARCH METHOD

This study adopts a descriptive qualitative approach using a case study of the Land and Building Tax Information Management System (SISMIOP) implemented within the Regional Revenue, Finance, and Asset Management Agency. The primary objective is to evaluate the maturity level of information security practices applied in SISMIOP and to formulate strategic recommendations for strengthening organizational security capabilities. To achieve the research objectives, the study follows a structured research procedure as illustrated in Figure 1.

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

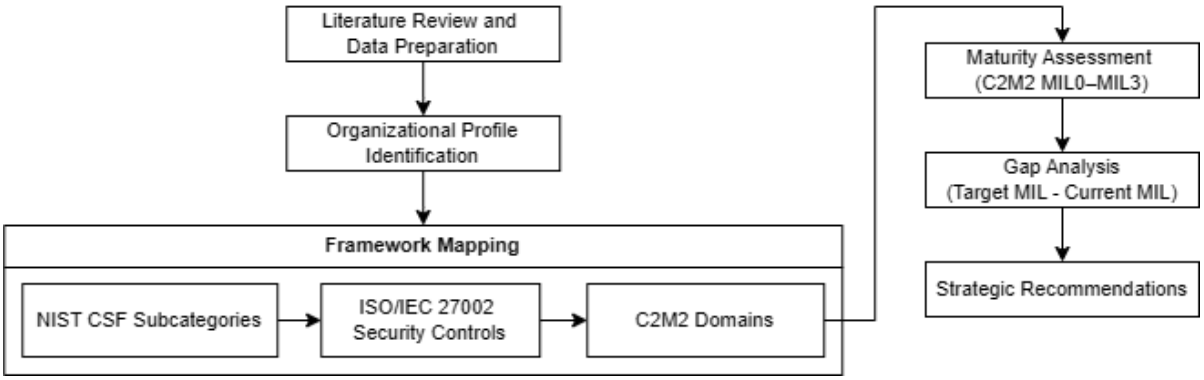

Figure 1. Research Procedure

3.1. Data Preparation and Literature Review of Security Frameworks

The research began with the preparation and collection of internal documents related to SISMIOP operations and existing information security practices within BPPKAD. Concurrently, a literature review was conducted on three major security frameworks NIST Cybersecurity Framework (CSF), ISO/IEC 27002:2022, and the Cybersecurity Capability Maturity Model (C2M2). This review aimed to understand the principles, structural components, and capability indicators of each framework as the foundation for developing the maturity evaluation instrument.

3.2. Organizational Profile Definition

The organizational profile was defined following the NIST CSF guidelines, covering system scope, stakeholder roles and responsibilities, IT organizational structure, and the identification of critical information assets. Data for constructing the profile were collected through interviews, direct observations, and document analysis. The resulting organizational profile serves as the basis for determining relevant NIST CSF subcategories and aligning them with ISO/IEC 27002 controls and C2M2 capability domains. This ensures that the evaluation reflects the specific operational environment of a regional government agency.

3.3. Framework Mapping

This stage involved integrating the subcategories of NIST CSF with the technical controls in ISO/IEC 27002 and the capability domains and objectives of C2M2. Each NIST CSF subcategory was mapped to corresponding ISO/IEC 27002 controls and subsequently associated with relevant C2M2 domains. The mapping results formed the evaluation instruments, including a structured questionnaire and interview guide tailored to the context of public-sector information systems such as SISMIOP..

3.4. Maturity Assessment

The maturity assessment instrument was developed based on the integrated mapping of the three frameworks NIST CSF's six core functions (Govern, Identify, Protect, Detect, Respond, and Recover), ISO/IEC 27002 technical controls, and C2M2 maturity indicators. Data collection in this study involved five respondents, all of whom are internal employees and active users of the SISMIOP application. Respondents evaluated the implementation of security practices according to the C2M2 Maturity Indicator Levels (MIL0-MIL3), reflecting the current condition of information security practices within the organization.

Each security domain was evaluated using the C2M2 capability scale, ranging from MIL 0 (no capability) to MIL 3 (managed and adaptive). C2M2 defines four MIL to describe the extent to which cybersecurity practices are implemented and institutionalized. MIL0 (Incomplete) indicates that security practices are absent or inconsistently performed. MIL1 (Initiated) shows that practices exist but are

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

informal, undocumented, and dependent on individual efforts. MIL2 (Performed) represents a baseline maturity where practices are formally defined, documented, and consistently implemented across the organization with clear roles and responsibilities. MIL3 (Managed) reflects an advanced state in which cybersecurity practices are systematically monitored, measured, and continuously improved to support organizational objectives.

After the questionnaire data were collected, a data validation process was conducted to ensure the reliability and consistency of the responses. Validation was performed through follow-up interviews with a subject-matter expert, namely the SISMIOP super administrator (super admin), who has comprehensive authority and technical understanding of the application, system configuration, and security controls.

3.5. Gap Analysis

A gap analysis was then performed by comparing the current maturity levels with the target maturity defined by the organization. In accordance with the official C2M2 Version 2.1 guidance [26], MIL2 (Performed) was selected as the target maturity level because it represents the minimum recommended baseline for organizations delivering essential public services. At MIL2, cybersecurity practices are formally documented, consistently implemented, and supported by defined roles and responsibilities, addressing the limitations of ad-hoc and undocumented practices characteristic of MIL1. This level provides a realistic and risk-informed target for improving cybersecurity governance in regional government information systems such as SISMIOP.

The differences in maturity levels across domains were analyzed and visualized to highlight areas with the largest gaps. This analysis enables the identification of priority domains requiring improvement and provides the foundation for formulating structured, data-driven enhancement strategies.

3.6. Strategic Information Security Recommendations

Based on the gap analysis results, strategic recommendations were developed to strengthen information security in the identified priority areas. The recommendations were derived from best practices in NIST CSF, relevant ISO/IEC 27002 controls, and capability-building strategies from C2M2. Each recommendation was contextualized to the organizational environment, resource availability, and system complexity of BPPKAD. This stage produced a structured, data-driven, and contextually relevant roadmap for enhancing the information security maturity of SISMIOP.

4. RESULT

4.1. Comparative Analysis of Frameworks

This study employs three complementary frameworks NIST CSF 2.0, ISO/IEC 27002:2022, and C2M2 2.1. to ensure a comprehensive assessment of SISMIOP's information security posture. The comparative analysis shows that each framework offers distinct strengths: NIST CSF provides a strategic structure for security functions and risk management, ISO/IEC 27002 delivers detailed technical and procedural controls, and C2M2 offers a capability-based maturity model for evaluating consistency and organizational readiness. No single framework covers all dimensions required for a holistic evaluation; therefore, integrating the three enables alignment between strategic objectives, operational controls, and measurable maturity levels. This integrated approach is particularly relevant for public-sector organizations such as BPPKAD, which require both clear governance guidance and practical mechanisms for assessing and improving security capabilities. A comparison of the selected cybersecurity frameworks is presented in Table 1.

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

Table 1. Framework Comparison

No	Description	NIST CSF	ISO/IEC 27002	C2M2
1.	Purpose	Functional risk management framework	Security control implementation guideline	Capability maturity assessment model
2.	Type	Framework	Control-based code of practice	Maturity model
3.	Structure	6 Functions	4 Control Categories	10 Domains
4.	Level of Detail	22 Categories, 106 Subcategories	93 Controls	43 Objectives
5.	Maturity Concept	Tiers 1–4 (Partial–Adaptive)	Based on control implementation	MIL0–MIL3
6.	Key Indicators	Govern, Identify, Protect, Detect, Respond, Recover	Organizational, People, Physical, Technical Controls	Asset, Risk, Threat, Access, Workforce, Architecture, Response, Third-Party, Program
7.	Role in Research	Defines security functions and target outcomes	Provides technical and procedural controls	Measures and analyzes maturity levels

4.2. Organizational Profile

The organizational profile was established to define the scope, assets, and security requirements relevant to the SISMIOP system operated by BPPKAD Banjarnegara. This process follows the initial steps recommended in the NIST Cybersecurity Framework (CSF), which serve as the foundation for determining the security outcomes to be evaluated. The first step, Scope the Organizational Profile, involved defining the system boundaries and identifying the core functions of SISMIOP, particularly its role in supporting land and building tax (PBB) management processes, including registration, assessment, billing, payment, and reporting. The second step, Gather Needed Information, included collecting organizational structure data, identifying information assets, understanding business processes, and reviewing existing security controls. Information was obtained through documentation review, interviews, and direct observations within BPPKAD. The third step, Create the Organizational Profile, consisted of synthesizing these findings into a structured profile that reflects the security needs, dependencies, and operational characteristics of SISMIOP. This profile subsequently guided the mapping of NIST CSF subcategories to ISO/IEC 27002 controls and C2M2 capability domains, forming the analytical basis for the maturity assessment. The organizational profile of the studied institution is summarized in Table 2.

Table 2. Organizational Profile

No	Function	Subcategories	Organizational Profile
1.	Govern	GV.RR-01	Assignment of security roles and responsibilities,
		GV.PO-01	Establishment of security policy
		GV.SC-01	Management of third-party relationships related to system integrations
2.	Identify	ID.AM-01 to ID.AM-04	Inventory of physical, software, and information assets used in SISMIOP
		ID.RA-01, ID.RA-03	Identification of risks and threats to tax data and operational continuity
3.	Protect	PR.AA	Identity and access management mechanisms
		PR.DS	Data protection measures including backup and encryption readiness
		PR.PS	Patch/configuration management for server and application environments

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

4.	Detect	DE.CM-01, DE.AE-01	System monitoring and anomaly detection activities for logs and operational behavior
5.	Respond	RS.MI-01 to RS.MI-03	Incident reporting, analysis, and mitigation processes for technical and operational disruptions
6.	Recover	RC.RP-01, RC.CO-01	Data recovery strategies, backup procedures, and communication workflows during service restoration

The organizational profile provides a contextual foundation for mapping ISO/IEC 27002 controls and C2M2 capability domains and serves as the starting point for evaluating the maturity of SISMIOP's information security practices.

4.3. Framework Mapping

After determining the relevant NIST CSF subcategories, the next step involved mapping each subcategory to the corresponding ISO/IEC 27002 controls and C2M2 capability domains. This mapping was conducted to establish a clear linkage between strategic security objectives, technical control requirements, and organizational capability maturity. A total of 38 NIST CSF subcategories relevant to SISMIOP were mapped to 29 ISO/IEC 27002 controls and distributed across 10 C2M2 domains, including Asset, Risk, Access, Threat, Response, and Third-Party. The resulting framework provides a coherent evaluation structure in which each subcategory is aligned with its strategic intent (NIST CSF), implementation standard (ISO/IEC 27002), and capability domain (C2M2), forming the basis for the maturity assessment. The description of ISO/IEC 27002 security controls relevant to this study is provided in Table 3.

Table 3. ISO/IEC 27002 Description

Clause	Control	Description
Organizational Controls	5.1, 5.2, 5.4, 5.7, 5.9, 5.12, 5.13, 5.17, 5.18, 5.20, 5.22, 5.23, 5.25, 5.26, 5.27, 5.30 5.31	Regulation of policies, roles, responsibilities, and information security governance within the organization.
People Controls	6.1, 6.2, 6.3	Security aspects involving human resources.
Technological Controls	8.2, 8.4, 8.8, 8.9, 8.10, 8.13, 8.1, 8.23, 8.24, 8.27, 8.28	Physical protection of information assets and organizational facilities.

Table 4 presents the C2M2 maturity model used as the basis for evaluating cybersecurity capability levels.

Table 4. C2M2 Description

Domain	Descriptive
PROGRAM	Governance and comprehensive management of cybersecurity programs within the organization.
ASSET	Identification, inventory, and management of information and IT assets, both physical and digital.
RISK	Risk management including identification, analysis, assessment, and mitigation of information security risks.
THIRD-PARTY	Security management in relationships and integrations with third parties such as vendors, technology partners, or other institutions.
ACCESS	Identity control, authorization, and access management to information systems.
THREAT	Identification and assessment of potential threats to systems, including internal and external threats.
RESPONSE	Organizational readiness and capability in responding to security incidents and service recovery.
WORKFORCE	Competence and training of personnel related to cybersecurity.

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

The mapping of the NIST CSF subcategories to corresponding ISO/IEC 27002 controls and C2M2 domains is presented in Table 2, Table 3, and Table 4, respectively. Table 2 outlines the Organizational Profile, identifying relevant NIST CSF subcategories based on the organization's characteristics. Table 3 provides a description of the ISO/IEC 27002 controls that align with each subcategory, offering detailed insights into security control objectives. Meanwhile, Table 4 describes the C2M2 domains, highlighting capability areas that support maturity evaluation in relation to the mapped subcategories.

To streamline the mapping and referencing of security activities across the frameworks, a coding system was developed for each security control item. Each code (e.g., A1, B2, C3) represents a unique control derived from specific subcategories of the NIST Cybersecurity Framework (NIST CSF). These codes are grouped by the six core functions of NIST CSF Govern, Identify, Protect, Detect, Respond, and Recover and serve as the foundation for cross-referencing related controls in ISO/IEC 27002 and C2M2 domains. The mapping and coding of NIST CSF subcategories to ISO/IEC 27002 controls and C2M2 domains are presented in Table 5.

Table 5. Framework Mapping and Coding

Code	Description	NIST CSF	ISO 27002	C2M2
A1	Establishment of roles and responsibilities	GV.RR-01	5.7, 6.1, 6.2	PROGRAM
A2	Establishment of cybersecurity policies	GV.PO-01	5.1, 5.2	PROGRAM
A3	Establishment of organizational context	GV.OC-01	5.9	ASSET
A4	Implementation of risk management	GV.RM-01	5.4	RISK
A5	Third-party management	GV.SC-01	5.22, 5.23	THIRD-PARTY
B1	Inventory of physical assets	ID.AM-01	5.9	ASSET
B2	Inventory of software	ID.AM-02	8.32	ASSET
B3	Inventory of information assets	ID.AM-03	5.12	ASSET
B4	Identification of external systems	ID.AM-04	5.12, 5.13	ASSET
B5	Identification of users and access	ID.AM-07	5.18	ACCESS
B6	Identification of critical functions and dependencies	ID.BE-06	5.22, 5.23	THIRD-PARTY
B7	Risk identification	ID.RA-01	5.4	RISK
B8	Threat identification	ID.RA-03	8.24	THREAT
B9	Risk response process	ID.RM-01	5.4, 5.30	RISK
C1	Identity management	PR.AA-01	5.17	ACCESS
C2	Access rights management	PR.AA-02	5.18	ACCESS
C3	Use of authentication	PR.AA-03	8.2	ACCESS
C4	Remote access control	PR.AA-04	8.4	ACCESS
C5	Privileged access management	PR.AA-06	5.20	ACCESS
C6	Protection of data at rest	PR.DS-01	8.10	ASSET
C7	Protection of data in transit	PR.DS-02	8.24	ASSET
C8	Data integrity protection	PR.DS-03	8.2	ASSET
C9	Data access control	PR.DS-06	5.18	ACCESS
C10	Backup maintenance	PR.DS-11	8.13	RESPONSE
C11	Patch management implementation	PR.PS-01	8.8	THREAT
C12	Secure configuration implemented	PR.PS-02	8.9	THREAT
C13	Vulnerability management implementation	PR.PS-03	8.23	THREAT
C14	Security training for users	PR.AT-01	6.3	WORKFORCE
D1	Network and system monitoring	DE.CM-01	8.16	RESPONSE

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

D2	Monitoring of logging activities	DE.CM-02	8.16	RESPONSE
D3	Detection of anomalous activity	DE.AE-01	8.27	RESPONSE
D4	Security event analysis	DE.AE-02	8.28	RESPONSE
E1	Incident reporting	RS.MI-01	5.25	RESPONSE
E2	Incident analysis	RS.MI-02	5.26	RESPONSE
E3	Incident mitigation	RS.MI-03	5.27	RESPONSE
F1	Execution of recovery plan	RC.RP-01	5.30	RESPONSE
F2	Data recovery	RC.IM-01	8.13	RESPONSE
F3	Communication during recovery	RC.CO-01	5.31	RESPONSE

4.4. Maturity Assessment

The maturity measurement results based on the integrated NIST CSF, ISO/IEC 27002, and C2M2 framework indicate that the overall cybersecurity posture of SISMIOP remains at an early stage, with most functions achieving only MIL1 and a smaller portion reaching MIL2. This reflects that while several security practices are already performed operationally, they have not yet been fully formalized, documented, or implemented in a consistent and repeatable manner. The Protect function shows relatively stronger maturity compared to other functions, whereas Govern, Identify, Detect, Respond, and Recover still require substantial improvement to meet the expected MIL2 baseline for essential public service systems. These findings highlight the need for strengthened governance, structured processes, and enhanced technical controls to improve SISMIOP's overall security maturity. The results of the maturity assessment based on C2M2 MIL are summarized in Table 6.

Table 6. MIL (Maturity Indicator Levels) Assessment

No	Function	MIL 0	MIL 1	MIL 2	MIL 3
1.	Govern	-	A1, A2, A3, A4, A5, B7,		-
2.	Identify	-	B8, B9, B1, B2, B3, B4, B6	B5	-
3.	Protect	-	C4, C6, C11, C12, C13, C14	C1, C2, C3, C5, C7, C8, C9, C10	-
4.	Detect	-	D1, D2, D3, D4		-
5.	Respond	-	E1, E2, E3		-
6.	Recover	-	F1, F2, F3		-

The maturity distribution analysis shows that 29 out of 38 subcategories (76.3%) remain at MIL1, indicating that most security practices have been initiated but are still informal and inconsistently documented. Meanwhile, 9 subcategories (23.7%) have achieved MIL2, reflecting partial formalization and consistent implementation of security controls. This distribution confirms that the overall security posture of SISMIOP is still dominated by basic maturity levels, emphasizing the need for systematic improvement toward the target MIL2.

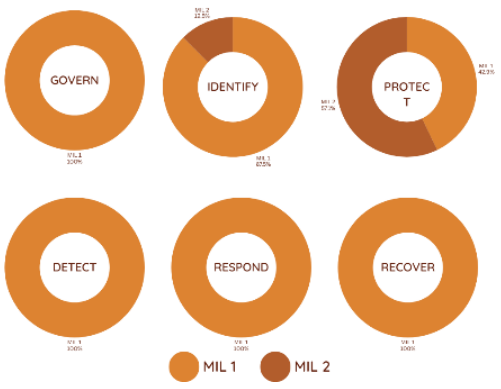

Figure 2. Maturity Indicator Level (MIL) assessment results using C2M2

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

4.5. Recommendations

The recommendations formulated in this study aim to strengthen the cybersecurity posture of SISMIOP by addressing the maturity gaps identified through the integrated NIST CSF 2.0, ISO/IEC 27002:2022, and C2M2 assessment. As most controls remain at MIL1, the proposed improvements prioritize foundational governance measures, including the establishment of formal security policies, clear roles and responsibilities, structured risk management, and comprehensive asset documentation. Technical enhancements are also required, such as enforcing secure configurations, implementing encryption, performing routine vulnerability assessments, and improving monitoring and log review procedures. Additionally, the development of a formal incident response framework, recovery procedures, and periodic user security training is essential to ensure consistency and resilience in system operations. Collectively, these recommendations provide a practical roadmap for BPPKAD Banjarnegara to progress toward MIL2 and build a more robust, consistent, and sustainable information security environment for SISMIOP. The prioritized strategic recommendations derived from the maturity gap analysis are listed in Table 7.

Table 7. Recommendations

Code	Recommendations
A1	Establish formal information security roles and responsibilities within official documents, and appoint a designated security PIC.
A2	Develop an Information Security Policy covering access control, data protection, incident handling, backup, and system usage.
A3	Document organizational context, system scope, SISMIOP workflows, and third-party dependencies.
A4	Implement a structured IT risk management process: asset identification, risk assessment, impact analysis, and mitigation planning.
A5	Document API dependencies (Bank Jateng, DPMPTSP, SIMPATDA) and establish formal data security agreements.
B1	Develop an inventory of physical devices supporting SISMIOP (servers, PCs, network equipment).
B2	Create a complete software inventory: SISMIOP desktop/web apps, DBMS, OS, APIs, and patch versions.
B3	Identify and classify information assets (taxpayer data, property records, payment history, logs, metadata).
B4	Document all external systems integrated with SISMIOP.
B5	Maintain periodic user access reviews (every 6–12 months).
B6	Identify critical business functions and prepare fallback procedures for API failures.
B7	Develop a list of operational and data-related risks and define mitigation actions.
B8	Establish a documented threat list (data manipulation, malware, brute-force attempts, server downtime).
B9	Define formal risk response options (avoid, mitigate, accept, transfer).
C1	Strengthen procedures for removing access rights of transferred or resigned employees.
C2	Conduct periodic access audits and ensure enforcement of the least privilege principle.
C3	Implement a formal password policy including complexity, expiry, and reuse restrictions.
C4	Use VPN or IP whitelisting; implement MFA for administrators.
C5	Monitor administrator activities and retain audit logs for at least one year.
C6	Apply database or disk encryption and strengthen server hardening for data-at-rest protection.
C7	Ensure HTTPS enforcement and require VPN for internal access.
C8	Implement checksum or hashing mechanisms and review logs for manipulation attempts.
C9	Conduct data access rights review every six months.
C10	Add logging for successful backups and perform routine restore testing.
C11	Schedule regular updates and patching for systems and servers, with proper documentation.
C12	Develop a secure configuration baseline for operating systems and servers.

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

C13	Conduct vulnerability scans at least once or twice per year.
C14	Implement periodic security awareness training for SISMIOP users.
D1	Establish a log monitoring schedule for abnormal login activities and API traffic.
D2	Perform periodic audit log reviews and enable anomaly alerts.
D3	Develop procedures for detecting suspicious or anomalous system activities.
D4	Establish mechanisms for technical incident analysis and classification.
E1	Develop an Incident Reporting SOP and formal reporting channels.
E2	Conduct root cause analysis (RCA) for every incident.
E3	Define and document incident mitigation steps.
F1	Develop a formal service recovery plan and conduct periodic testing.
F2	Perform regular data restore tests and document results.
F3	Establish a communication workflow among BPPKAD, Diskominfo, and external parties during recovery activities.

5. DISCUSSIONS

This discussion interprets how the maturity assessment results reflect the actual cybersecurity posture of SISMIOP and explains the gaps between the current maturity levels (MIL11MIL2) and the target level (MIL2). According to C2M2 guidance, MIL2 is recommended as a baseline for essential public services because it requires cybersecurity practices to be documented, repeatable, and consistently implemented. Given that SISMIOP processes sensitive taxpayer data and supports regional revenue operations, achieving at least MIL2 is necessary to ensure confidentiality, integrity, service availability, and public trust in digital tax services.

The assessment results indicate that most of the 38 evaluated subcategories remain at MIL1, showing that security practices are operational but still informal and inconsistently applied. The most critical gaps are observed in the Govern and Identify functions, which represent the foundational domains of cybersecurity maturity. The absence of formal security policies, clearly defined roles, documented asset inventories, and structured risk management limits the effectiveness of technical controls and constrains overall maturity progression. This finding reinforces that governance functions form the backbone of a mature cybersecurity posture, with weaknesses at this level propagating to other domains.

Asset and risk management practices also remain at MIL1 due to the lack of formal inventories and documented assessments, preventing systematic risk prioritization and mitigation. Similarly, the Detect and Respond functions exhibit reactive characteristics. Although log data are generated, there are no formal procedures for log review, anomaly detection, incident documentation, or root-cause analysis, which is inconsistent with the expectations of MIL2 for essential services.

In contrast, several subcategories within the Protect function have reached MIL2, particularly in access control and data protection. Consistent implementation of role-based access control, privileged access restrictions, HTTPS, and routine backups indicates relatively stronger maturity in protection-oriented controls compared to governance and monitoring domains. However, gaps remain in data-at-rest protection, recovery testing, and formal backup validation, suggesting that protection practices are not yet fully institutionalized.

Based on these gaps, this study proposes prioritized recommendations, including the formalization of security governance and policies, the establishment of documented asset inventories and periodic risk assessments, and the implementation of structured log monitoring and incident analysis to shift from reactive to proactive cybersecurity management. These actions directly address the transition from MIL1 to MIL2 and provide a practical roadmap for incremental maturity improvement.

Compared to prior studies that focus mainly on conceptual framework comparisons without implementation, this research extends existing work by applying an integrated multi-framework approach in a real organizational context. The results indicate a maturity improvement potential of

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

approximately 20–25% compared to MIL1-dominated profiles reported in earlier public-sector studies, particularly in governance alignment and protection controls. From an informatics perspective, the proposed model bridges theory and practice by enabling systematic evaluation and strengthening regional cybersecurity governance. While the study is limited by its qualitative approach and single-case scope, the findings offer important policy implications, supporting evidence-based prioritization of cybersecurity investments and the adoption of MIL2 as a realistic baseline for regional government institutions.

6. CONCLUSION

This study evaluated the cybersecurity maturity of the SISMIOP system within BPPKAD Banjarnegara using an integrated approach combining the NIST Cybersecurity Framework 2.0, ISO/IEC 27002:2022, and the Cybersecurity Capability Maturity Model (C2M2) 2.1. The mapping of 38 NIST CSF subcategories indicates that the overall maturity of SISMIOP is still dominated by MIL1, meaning that most security practices have been initiated but remain informal and insufficiently institutionalized. While access management and data protection show partial progress toward MIL2, the Govern and Identify functions remain the weakest domains due to the lack of formal policies, documented processes, and structured risk management.

Based on these maturity gaps, this study formulated 38 prioritized strategic recommendations covering governance strengthening, policy formalization, risk management, technical controls, incident response, and recovery processes to support a systematic transition toward the target maturity level of MIL2. Achieving this level is expected to improve the consistency and reliability of security controls, thereby enhancing public trust through better protection of sensitive taxpayer data and more dependable digital tax services.

From an informatics perspective, this research contributes a replicable multi-framework cybersecurity maturity assessment model that integrates strategic, technical, and capability-based viewpoints and provides practical value for public-sector institutions. The proposed model supports stronger cybersecurity governance by aligning governance mechanisms with operational security practices. Future research is recommended to implement and evaluate the proposed improvement roadmap longitudinally, explore automated monitoring mechanisms such as deep learning–based anomaly detection, and conduct benchmarking studies across multiple regional governments to enhance generalizability and support evidence-based cybersecurity policy development.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest between the authors or with research object in this paper.

ACKNOWLEDGEMENT

The authors would like to thank BPPKAD Kabupaten Banjarnegara for providing access to system stakeholders during data collection.

REFERENCES

[1] Kementerian Keuangan Republik Indonesia, “Bahan Ajar Operator Console/SISMIP.” 2017.
[2] Y. Maleh, A. Sahid, dan M. Belaissaoui, “A Maturity Framework for Cybersecurity Governance in Organizations,” *Edpacs*, vol. 63, no. 6, hal. 1–22, 2021, doi: 10.1080/07366981.2020.1815354.
[3] S. Ajoudanian dan H. R. Aboutalebi, “A capability maturity model for smart city process-aware digital transformation,” *J. Urban Manag.*, no. October 2024, 2025, doi: 10.1016/j.jum.2025.03.001.

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

[4] ISACA Germany Chapter, *Implementation Guideline ISO/IEC 27001:2013*. 2016.
[5] SecAware, "Pragmatic ISMS implementation guideline; Putting ISO/IEC 27001 into practice," 2024.
[6] J. Nikander, O. Manninen, dan M. Laajalahti, "Requirements for cybersecurity in agricultural communication networks," *Comput. Electron. Agric.*, vol. 179, no. September, hal. 105776, 2020, doi: 10.1016/j.compag.2020.105776.
[7] National Safety and Quality Digital Mental Health Standars, *Action Guide: Information security management systems*. Australian Commission. (2022). Action Guide: Information security management systems., 2022.
[8] IsecT Limited, "ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (third edition)." [Daring]. Tersedia pada: https://www-iso27001security-com.
[9] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*. 2024. doi: https://doi.org/10.6028/NIST.CSWP.29.
[10] U.S. Department Of Energy, *Cybersecurity Capability Maturity Model (C2M2)*. 2022.
[11] Runzero, "Cybersecurity Capability Maturity Model (C2M2)." [Daring]. Tersedia pada: https://help.runzero.com/docs/compliance/c2m2/
[12] J. D. Christopher *dkk.*, "Cybersecurity Capability Maturity Model (C2M2)," *Dep. Homel. Secur.*, no. February, hal. 1–76, 2014.
[13] B. O. Omoyiola, "The Evolution of Information Security Measurement and Testing," *IOSR J. Comput. Eng.*, vol. 22, no. 3, hal. 50–54, 2020, doi: 10.9790/0661-2203025054.
[14] T. C. Herath, H. S. B. Herath, dan D. Cullum, *An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks*, vol. 25, no. 2. Springer US, 2023. doi: 10.1007/s10796-022-10246-9.
[15] R. Kwon, T. Ashley, J. Castleberry, P. McKenzie, dan S. N. Gupta Gourisetti, "Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping," *2020 Resil. Week, RWS 2020*, no. January 2021, hal. 106–112, 2020, doi: 10.1109/RWS50334.2020.9241271.
[16] F. W. Zakiy dan N. D. Angresti, "Comparative Analysis of Cybersecurity Maturity Frameworks :," vol. 01, no. 02, hal. 82–87, 2024.
[17] D. F. Tanjung, O. D. Nurhayati, dan A. Wibowo, "Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001:2022 and CIS Control," vol. 9, no. 6, 2024.
[18] I. Bashofi dan M. Salman, "Cybersecurity Maturity Assessment Design Using NISTCSF , CIS CONTROLS v8 and ISO / IEC 27002," *2022 IEEE Int. Conf. Cybern. Comput. Intell.*, hal. 58–62, 2022, doi: 10.1109/CyberneticsCom55287.2022.9865640.
[19] D. Sulistyowati, F. Handayani, dan Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," *Int. J. Informatics Vis.*, vol. 4, no. 4, hal. 225–230, 2020, doi: 10.30630/joiv.4.4.482.
[20] M. F. Delgado, D. Esenarro, F. F. J. Regalado, dan M. D. Reátegui, "Methodology Based On The Nist Cybersecurity Framework As A Proposal For Cybersecurity Management In Government Organizations," *Cuad. Desarro. Apl. a las TIC*, vol. 10, no. 2, hal. 123–141, 2021.
[21] A. Aminudin dan A. Supriyanto, "Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah)," *AITI J. Teknol. Inf.*, vol. 21, no. 2, hal. 210–229, 2024.
[22] M. Fadya dan D. N. Utama, "Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019," *TEM J.*, vol. 14, no. 1, hal. 182–191, 2025, doi: 10.18421/TEM141.
[23] D. Amanda, N. Mutiah, dan S. Rahmayudha, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI," *J. Komput. dan Apl.*, vol. 11, no. 02, hal. 291–302, 2023.
[24] H. G. Afiansyah dan N. A. K. Febriyani, "Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022,"

Vol. 7, No. 2, April 2026, Page. 1575-1588
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5551

J. Info Kripto, vol. 17, no. 3, hal. 93–99, 2023.

[25] S. Nikhil, G. Gourisetti, M. Mylrea, dan H. Patangia, "Cybersecurity vulnerability mitigation framework through empirical paradigm : Enhanced prioritized gap analysis," *Futur. Gener. Comput. Syst.*, vol. 105, hal. 410–431, 2020, doi: 10.1016/j.future.2019.12.018.

[26] Departemen Energi AS, "Cybersecurity Capability Maturity Model (C2M2)." [Daring]. Tersedia pada: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2