IJTIS

International Journal of Technological Innovation for Society (IJTIS)
https://journals.telkomuniversity.ac.id/ijtis

Vol. 1, No.1, 1-15, 2025
Publisher: Telkom University Journals

RESEARCH ARTICLE

Integrated Cybersecurity Capability Maturity Assessment Across Ten Domains Using C2M2 V2.1 in the Digital Banking Sector

Muhamad Irsan[1*] **and Muhamad Hasbi Kurniawan**[1]

[1]*School of Computing, Telkom University, Bandung, Indonesia*
[*]*Corresponding author*

Abstract
The rapid adoption of digital banking and public cloud infrastructure has significantly increased the cybersecurity exposure of financial institutions, particularly through application programming interface (API) vulnerabilities, privileged-access weaknesses, third-party dependencies, and inadequate protection of backup data. Conventional compliance audits generally rely on binary assessments and therefore provide limited insight into the institutional maturity and consistency of cybersecurity practices. This study evaluates the cybersecurity capability maturity of PT Bank Finansial Digital (BFD) across ten cybersecurity domains using the Cybersecurity Capability Maturity Model (C2M2) Version 2.1. A hybrid maturity-to-compliance assessment approach was applied by integrating the C2M2 evaluation results with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) Version 1.1, NIST Privacy Framework 1.1, and Indonesian Law No. 27 of 2022 concerning Personal Data Protection. The assessment was conducted using the official C2M2 HTML-Based Self-Evaluation Tool based on organizational documentation and technical configuration evidence as of May 23, 2026. The results show that seven of the ten assessed domains achieved Maturity Indicator Level 2 (MIL 2), whereas ACCESS, RESPONSE, and THIRD-PARTIES remained at MIL 1. Ten critical capability gaps classified as Partially Implemented were identified, with the RESPONSE domain representing the most significant weakness. Major findings included the absence of centralized privileged access management and multi-factor authentication, incomplete assessment of cloud sub-vendors, insufficiently formalized incident escalation procedures, outdated cloud incident-response procedures, and disabled encryption for data at rest in the Network-Attached Storage backup environment. These deficiencies potentially increase operational, privacy, regulatory, and reputational risks. A six-month remediation roadmap consisting of technical hardening, policy formalization, and crisis validation is therefore proposed to support the organization in achieving a consistent MIL 2 maturity level.

Keywords: C2M2 V2.1, Cybersecurity Maturity, Digital Banking, GRC, Incident Response, NIST CSF, NIST Privacy Framework, Personal Data Protection

Corresponding author:
irsanfaiz@telkomuniversity.ac.id

Received: 07 August 2026
Accepted: 08 August 2026
Available online: 08 August 2026

1. Introduction

Digital transformation has significantly changed the operational landscape of the banking industry. Financial institutions increasingly rely on cloud computing, mobile banking applications, interconnected services, and Application Programming Interfaces (APIs) to provide real-time financial services [6]. This transformation improves operational efficiency and service accessibility; however, it also expands the cybersecurity attack surface. Modern digital banking architectures commonly employ a Core API Gateway as an external interface connecting mobile

banking applications with core banking platforms. Consequently, vulnerabilities affecting authentication, authorization, privileged access, cloud infrastructure, and API security may expose sensitive banking systems to unauthorized access.

The aggressive migration from traditional infrastructure to public cloud environments may also create a gap between technological adoption and organizational cybersecurity capability. Technical vulnerabilities such as broken object-level authentication, inadequate privileged-account controls, and insufficient protection of backup infrastructure can become significant attack vectors. Moreover, highly interconnected cloud ecosystems introduce additional dependencies on vendors and sub-vendors, creating cybersecurity risks that may not be directly controlled by the financial institution.

The issue becomes increasingly important in the context of personal data protection. Indonesian Law No. 27 of 2022 concerning Personal Data Protection imposes obligations on organizations acting as personal data controllers. Therefore, cybersecurity weaknesses are no longer solely technical problems but may also generate regulatory, legal, operational, and reputational consequences [2].

Traditional compliance-oriented cybersecurity assessments generally determine whether a particular control exists through binary responses such as compliant or non-compliant. Although useful for regulatory auditing, this method provides limited information about whether cybersecurity practices are consistently implemented, documented, funded, maintained, and institutionalized throughout the organization.

A cybersecurity maturity model provides a broader perspective by measuring not only the existence of cybersecurity controls but also the organizational capability supporting their implementation. The Cybersecurity Capability Maturity Model (C2M2) Version 2.1 provides such an approach by evaluating cybersecurity practices across multiple organizational domains and assigning maturity levels according to their degree of institutionalization [3].

This study therefore applies C2M2 V2.1 to evaluate the cybersecurity maturity of PT Bank Finansial Digital (BFD). The assessment covers all ten C2M2 cybersecurity domains and focuses on the operational functions associated with the Security Operations Center (SOC) and Cyber Security Incident Response Team (CSIRT) [4].

Unlike a standalone maturity evaluation, this study further introduces a hybrid Maturity-to-Compliance Impact approach. Cybersecurity capability gaps identified through C2M2 are mapped horizontally to the NIST Cybersecurity Framework (NIST CSF) V1.1, NIST Privacy Framework 1.1, and Indonesian Personal Data Protection Law. This approach provides a broader understanding of how internal cybersecurity maturity deficiencies may translate into operational and regulatory risks.

Accordingly, the objectives of this study are:

1. to determine the Maturity Indicator Level (MIL) achieved by each of the ten C2M2 domains;
2. to identify cybersecurity capability gaps preventing the organization from achieving the targeted maturity level;
3. to analyze the relationship between internal cybersecurity maturity gaps and external cybersecurity and privacy requirements; and
4. to formulate a practical six-month remediation roadmap to improve the organization's cybersecurity maturity toward MIL 2.

The primary contribution of this study is the integration of a cybersecurity capability maturity assessment with cybersecurity, privacy, and regulatory compliance perspectives. The resulting assessment is intended to support cybersecurity governance and management decision-making in the digital banking environment.

2. Literature Review

2.1. Cybersecurity Capability Maturity Model Version 2.1

The Cybersecurity Capability Maturity Model (C2M2) is a cybersecurity capability assessment framework developed by the U.S. Department of Energy (DOE) in cooperation with cybersecurity and critical-infrastructure stakeholders. Unlike traditional compliance frameworks that primarily determine whether individual security controls exist, C2M2 evaluates the extent to which cybersecurity practices have been institutionalized within an organization [5].

C2M2 Version 2.1 evaluates cybersecurity capabilities through ten major domains:

a) Asset, Change, and Configuration Management (ASSET);
b) Threat and Vulnerability Management (THREAT);
c) Risk Management (RISK);
d) Identity and Access Management (ACCESS);
e) Situational Awareness (SITUATION);
f) Event and Incident Response, Continuity of Operations (RESPONSE);
g) Third-Party Risk Management (THIRD-PARTIES);
h) Cybersecurity Workforce Management (WORKFORCE);
i) Cybersecurity Architecture (ARCHITECTURE); and
j) Cybersecurity Program Management (PROGRAM).

Cybersecurity capability maturity is represented through Maturity Indicator Levels ranging from MIL 0 to MIL 3. MIL 0 – Not Performed indicates that cybersecurity practices have not been implemented or formally considered. MIL 1 – Initiated indicates that cybersecurity activities are performed but may remain informal, ad hoc, or highly dependent on specific individuals. MIL 2 – Performed represents a condition in which cybersecurity practices are regularly and consistently implemented and supported through resources, procedures, and organizational processes. MIL 3 – Managed represents a more mature state in which cybersecurity practices are formally governed, monitored, and continuously evaluated through organizational policies and performance measurements.

An important characteristic of the model is its cumulative maturity principle. An organization cannot achieve a higher maturity level when practices required at preceding levels have not been sufficiently implemented. Consequently, a relatively small number of partially implemented practices can prevent an entire domain from achieving its targeted maturity level. This characteristic makes C2M2 particularly relevant for identifying capability bottlenecks that might otherwise remain obscured in conventional compliance assessments.

2.2. NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a structured approach to managing cybersecurity risk. NIST CSF Version 1.1 organizes cybersecurity activities into five major functions: the Identify function focuses on understanding organizational assets, risks, business environments, governance arrangements, and supply-chain dependencies; the Protect function includes identity management, access control, awareness, data security, protective technology, and maintenance activities; the Detect function addresses mechanisms required to identify anomalous activities and cybersecurity incidents; the Respond function covers response planning, communication, analysis, mitigation, and improvement following cybersecurity incidents; and the Recover function focuses on restoring services and organizational capabilities after disruption. In this study, NIST CSF is not used as the primary maturity-scoring instrument. Instead, it provides an external cybersecurity reference for interpreting the implications of capability gaps identified through C2M2 [1].

2.3. NIST Privacy Framework

The NIST Privacy Framework provides organizations with a structured approach to identifying and managing privacy risks arising from data processing activities. Privacy management is particularly important in digital banking because financial institutions continuously process personally identifiable and financially sensitive information. Cybersecurity deficiencies involving access control, backup infrastructure, incident response, and third-party service providers may therefore generate both security and privacy consequences. Within the proposed hybrid assessment, the NIST Privacy Framework is employed to determine whether identified C2M2 maturity gaps also represent weaknesses in privacy governance, data protection, communication, or privacy-control mechanisms [7].

2.4. Indonesian Personal Data Protection Law

Indonesian Law No. 27 of 2022 concerning Personal Data Protection establishes obligations concerning the processing and protection of personal data. Financial institutions are particularly affected because banking activities involve extensive processing of customer identity, transactional, and financial information. Therefore, inadequate security safeguards may expose the institution to regulatory consequences in addition to direct cybersecurity losses. The report evaluated in this study particularly associates cybersecurity deficiencies with provisions concerning the protection of personal data, accountability, security of data processing, supervision of processors, and breach-notification requirements. It also identifies potential exposure to administrative sanctions, including financial penalties. Consequently, integrating cybersecurity maturity with privacy and regulatory requirements provides a more comprehensive understanding of cybersecurity risk than analyzing cybersecurity controls independently [2].

2.5. Cybersecurity Maturity and Compliance Integration

Cybersecurity maturity and regulatory compliance address related but different questions. Compliance primarily asks whether an organization satisfies defined requirements, whereas maturity evaluates how reliably, consistently, and institutionally cybersecurity practices are performed. An organization may technically possess a cybersecurity control while still having a low level of operational maturity. For example, an incident-response procedure may exist but remain outdated, unsigned, inadequately tested, or inconsistently followed. A conventional compliance checklist might recognize the existence of the document, while a capability maturity assessment may reveal weaknesses in its implementation. The integration of cybersecurity maturity and compliance analysis therefore provides a stronger basis for Governance, Risk, and Compliance (GRC) decision-making. This concept forms the foundation of the Maturity-to-Compliance Impact approach applied in the present study [8].

3. Research Method

3.1. Research Design

The evaluation was conducted on the cybersecurity operational environment of PT Bank Finansial Digital, with particular emphasis on SOC and CSIRT activities. The assessment was limited to the organizational and technical cybersecurity evidence available during the evaluation period. The research consisted of four major stages, illustrated in Figure 1: C2M2 self-evaluation, maturity gap identification, cross-framework compliance mapping, and remediation roadmap development.

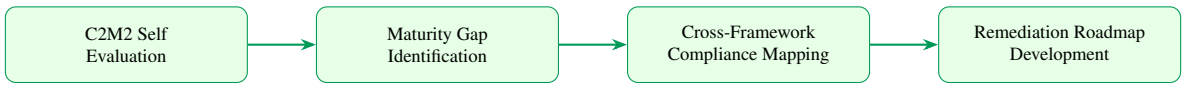

Figure 1: The research consisted of four major stages.

3.2. C2M2 Self Evaluation

A total of 356 cybersecurity practice items contained within the C2M2 assessment instrument were evaluated. Responses were determined based on available organizational documentation and examination of relevant technical configurations within the banking environment. Each practice was assessed according to its implementation condition. Particular attention was given to practices categorized as Partially Implemented (PI) because these practices represented potential barriers to achieving the targeted Maturity Indicator Level. The maturity target used by the organization was MIL 2 across all ten cybersecurity domains.

3.3. Maturity Gap Analysis

Following completion of the C2M2 assessment, the results were analyzed at both domain and practice levels. The analysis first identified the achieved maturity level of each domain. Subsequently, all practices categorized as partially implemented and preventing achievement of MIL 2 were extracted. The gap analysis focused on three dimensions:

a. deficiencies in technical controls;
b. deficiencies in procedural and governance mechanisms; and
c. deficiencies in third-party cybersecurity oversight.

The analysis subsequently determined which gaps represented the most significant operational risks to the digital banking environment.

3.4. Hybrid Maturity to Compliance Mapping

The identified C2M2 maturity gaps were mapped horizontally to three external references:

a. NIST Cybersecurity Framework Version 1.1;
b. NIST Privacy Framework 1.1; and
c. Indonesian Law No. 27 of 2022 concerning Personal Data Protection.

For example, a C2M2 deficiency involving protection of backup data was mapped to the NIST CSF data-security category, the relevant NIST privacy protection function, applicable personal data protection provisions, and finally its operational consequence for the bank. This approach enabled the study to distinguish between a simple maturity deficiency and a capability deficiency with wider compliance implications.

3.5. Development of the Remediation Roadmap

After the maturity and compliance analysis, a six-month remediation roadmap was developed. The roadmap prioritized corrective actions according to their technical urgency, governance requirements, and need for subsequent validation. The remediation program was divided into three phases:

a. Phase I – Technical Hardening, Months 1–2. Technical vulnerabilities with immediate security implications are addressed.
b. Phase II – Policy Formalization, Months 3–4. Policies, procedures, incident-escalation mechanisms, and supporting documentation are formalized.
c. Phase III – Crisis Validation, Months 5–6. The effectiveness of the implemented controls is evaluated through exercises, compliance testing, and measurement.

4. Results and Discussion

4.1. Overall C2M2 Maturity Profile

The C2M2 assessment showed that the cybersecurity capability of PT BFD was not uniformly mature across the ten evaluated domains. Seven domains achieved the targeted MIL 2, while three domains remained at MIL 1, as shown in Table 1.

Table 1: C2M2 V2.1 Cybersecurity Maturity Profile

No	C2M2 Domain	Target	Achieved	Status	Main Observation
1	Asset	MIL-2	MIL-2	Achieved	Automated cloud asset inventory
2	Threat	MIL-2	MIL-2	Achieved	Periodic scanning and cloud patching SLA
3	Risk	MIL-2	MIL-2	Achieved	Cyber risk integrated with enterprise risk management
4	Access	MIL-2	MIL-1	Not Achieved	Centralized PAM and MFA deficiencies
5	Situation	MIL-2	MIL-2	Achieved	24/7 SIEM-based security monitoring
6	Response	MIL-2	MIL-1	Not Achieved	Seven identified MIL 2 capability gaps
7	Third-Parties	MIL-2	MIL-1	Not Achieved	Incomplete cloud sub-vendor assessment
8	Workforce	MIL-2	MIL-2	Achieved	Mandatory awareness training and certified personnel
9	Architecture	MIL-2	MIL-2	Achieved	Documented perimeter and network-segmentation architecture
10	Program	MIL-2	MIL-2	Achieved	CISO-led cybersecurity strategy and dedicated resources

The result demonstrates that 70% of the evaluated domains reached the targeted maturity level, whereas 30% remained below the target. Although most domains reached MIL 2 individually, the report classifies the overall organizational maturity as being constrained at MIL 1 because critical partially implemented practices remained in ACCESS, RESPONSE, and THIRD-PARTIES. This finding is important because it illustrates the cumulative nature of maturity assessment. High maturity in cybersecurity architecture, threat management, asset management, or monitoring does not automatically compensate for significant weaknesses in identity management or incident response.

4.2. Access Management Capability Gaps

The ACCESS domain remained at MIL 1 because several access-control practices had not been sufficiently implemented. The assessment specifically identified weaknesses associated with ACCESS-2a and ACCESS-2c. The legacy core banking system continued to operate without comprehensive centralized privileged-access controls and multi-factor authentication. The absence of a centralized Privileged Access Management (PAM) mechanism increases the difficulty of controlling highly privileged administrative accounts. Privileged accounts represent particularly sensitive attack targets because compromise of such credentials may provide extensive access to critical banking systems.
The lack of MFA further increases the likelihood that compromised credentials can be successfully exploited. From an operational perspective, the combination of insufficient privileged-access management and incomplete MFA creates exposure to credential-stuffing and unauthorized privileged-access attacks. Thus, the ACCESS maturity deficiency should not be interpreted solely as a procedural weakness. It represents a potential attack pathway into critical banking infrastructure.

4.3. Incident Response as the Primary Maturity Bottleneck

Among the ten assessed domains, the RESPONSE domain represented the most significant cybersecurity maturity weakness. The source assessment identified seven partially implemented capabilities at MIL 2 within this domain. The documented findings particularly emphasized deficiencies concerning incident escalation, regulatory communication, incident-response documentation, backup protection, communication records, and crisis exercises.
One critical weakness concerned RESPONSE-2c. The organization's incident-escalation criteria were documented in Incident Escalation Criteria v0.1, but the document had not received formal approval from the Board of Directors. The lack of executive authorization creates uncertainty regarding who has authority to declare an incident as a corporate cybersecurity emergency. During a major breach, such ambiguity may delay managerial decisions, escalation, communication, containment, and regulatory response.
Another significant deficiency was associated with RESPONSE-3d. The organization's incident-handling procedure, SOP-Penanganan-Insiden-2023, had become outdated and did not adequately address cloud-native attack scenarios. This issue is particularly relevant because PT BFD operates digital banking services relying on cloud and API infrastructure. Incident-response procedures developed primarily for traditional infrastructure may be inadequate for attacks involving API Gateways, cloud identities, cloud services, and rapidly changing cloud workloads.

4.4. Backup Data Protection

One of the most critical technical findings involved RESPONSE-4j. The evaluation identified that encryption for data at rest had been disabled on the local Network-Attached Storage (NAS) backup server. Furthermore, administrative-access controls on the backup infrastructure were insufficient. This weakness creates an alternative attack path to customer information. Even where production databases are appropriately protected, unencrypted backup repositories may provide attackers with accessible copies of sensitive information.
The issue demonstrates an important cybersecurity principle: the confidentiality of customer data depends not only on protection of the primary production environment but also on all secondary copies of the information. The corresponding hybrid analysis associated this gap with NIST CSF PR.DS-3, privacy-protection requirements, and personal-data protection obligations. Operationally, successful exploitation could allow an attacker to extract customer database information directly from the backup repository.

4.5. Third Party and Cloud Supply Chain Risk

The THIRD-PARTIES domain also remained at MIL 1. The study found that cybersecurity assessments were primarily conducted for direct or major vendors but did not comprehensively include sub-vendors supporting public cloud-hosting infrastructure. The relevant gap was identified in the report as THIRD-PARTIES/SCRM-2b. This condition represents an important cybersecurity risk in cloud-based banking systems because the effective technology supply chain can extend beyond contractual first-tier vendors.
A vulnerability introduced through a sub-vendor can potentially affect the security of infrastructure supporting the bank's API environment even when the bank's internal security controls are functioning as intended. The finding was mapped to NIST CSF ID.SC-3, which addresses cybersecurity supply-chain risk management. This result reinforces the importance of extending cybersecurity governance beyond the organizational perimeter.

4.6. Hybrid Compliance Impact Analysis

The cross-framework analysis demonstrates that C2M2 maturity gaps can be translated into operational and compliance risks, as summarized in Table 2.
The analysis demonstrates that cybersecurity maturity weaknesses have consequences beyond C2M2 scoring. For instance, a partially implemented incident-communication process may initially appear to be an internal procedural problem. However, when mapped against regulatory breach-notification obligations, the same deficiency becomes a potential compliance risk. Similarly, an unencrypted backup repository represents not merely a technical configuration weakness but also a possible personal-data exposure. Consequently, the Maturity-to-Compliance Impact approach provides management with greater context for remediation prioritization.

4.7. Interpretation of the Overall Maturity Condition

The maturity profile indicates an important imbalance. PT BFD demonstrated relatively strong capabilities in structural and preventive domains. These include asset management, threat management, risk management, situational awareness, workforce capability, cybersecurity architecture, and program governance. However, weaknesses were concentrated in areas that become particularly important when preventive controls fail. This can be illustrated as:

Table 2: Hybrid Maturity-to-Compliance Impact Mapping

C2M2 Gap	NIST CSF V1.1	Privacy Perspective	PDP Law	Potential Banking Impact
ACCESS-2a / ACCESS-2c	PR.AC-4	Weak administrative access protection	Art. 35	Privileged account compromise
RESPONSE-2c	RS.AN-1	Insufficient governance alignment	Art. 39	Delayed declaration and escalation of major incidents
RESPONSE-2g	RS.CO-2	Inadequate external communication readiness	Art. 46	Delayed breach reporting
RESPONSE-3d	RS.RP-1	Inadequate cloud-oriented crisis control	Art. 35	Increased attacker dwell time
RESPONSE-4j	PR.DS-3	Backup information inadequately protected	Art. 35, 36	Customer database exposure
SCRM-2b	ID.SC-3	Third-party privacy risk insufficiently governed	Art. 37, 38	Cloud supply-chain compromise

Strong Preventive Capability + Weak Response Capability = Residual Organizational Cyber Risk

An organization may therefore possess advanced SIEM monitoring, formal cybersecurity architecture, and qualified personnel while remaining vulnerable to severe operational consequences when incident escalation, communication, backup protection, and response procedures are insufficiently mature. This is particularly critical in banking because the impact of a cybersecurity incident may develop rapidly and involve customer data, financial transactions, business continuity, regulatory requirements, and public confidence simultaneously.

4.8. Proposed Six-Month Cybersecurity Remediation Roadmap

Based on the capability gaps, the study proposes a sequential six-month remediation roadmap, summarized in Table 3.

4.8.1. Phase I: Technical Hardening – Months 1–2

The first phase addresses technical controls with immediate security implications. The activities include enabling data-at-rest encryption for the NAS backup server, implementing centralized PAM, enforcing MFA for critical and privileged systems, and extending cybersecurity assessment to cloud-hosting sub-vendors. These actions are prioritized because they directly reduce exposure to unauthorized access, credential compromise, backup-data theft, and supply-chain attacks.

4.8.2. Phase II: Policy Formalization – Months 3–4

Following technical remediation, the second phase strengthens governance and operational procedures. The primary activities include obtaining formal executive approval for cybersecurity incident-escalation criteria, updating the incident-response procedure into a cloud-native incident-response playbook, defining clearer roles and escalation authorities, and migrating incident communication records to a formal ticketing platform. Formalization is important because mature incident response requires not only technical competence but also documented authority, repeatable procedures, and auditable communication.

4.8.3. Phase III: Crisis Validation – Months 5–6

The final phase validates whether the implemented improvements operate effectively under realistic conditions. Activities include conducting executive-level cybersecurity Tabletop Exercises (TTX), testing organizational readiness to meet the required breach-notification timeframe identified in the source assessment, evaluating response coordination between SOC, CSIRT, management, and relevant stakeholders, and measuring the effectiveness of remediation controls.

Table 3: Proposed Six-Month Remediation Roadmap

Months 1–2: Technical Hardening	Months 3–4: Policy Formalization	Months 5–6: Crisis Validation
Enable NAS encryption	Approve incident escalation criteria	Conduct cybersecurity TTX
Implement PAM	Develop cloud-native incident playbook	Test notification readiness
Implement MFA	Formalize incident communication	Evaluate remediation effectiveness
Audit cloud sub-vendors	Implement formal ticketing/logging	Reassess C2M2 maturity

At the conclusion of the remediation period, a reassessment using the C2M2 instrument should be performed to determine whether the previously partially implemented practices have reached an implementation state sufficient for MIL 2.

5. Conclusion

This study evaluated the cybersecurity capability maturity of PT Bank Finansial Digital using the Cybersecurity Capability Maturity Model Version 2.1 across ten cybersecurity domains. The analysis was further integrated with the NIST Cybersecurity Framework Version 1.1, NIST Privacy Framework 1.1, and Indonesian Personal Data Protection Law through a hybrid Maturity-to-Compliance Impact assessment.

The assessment indicates that seven of the ten C2M2 domains achieved the targeted MIL 2. These domains were ASSET, THREAT, RISK, SITUATION, WORKFORCE, ARCHITECTURE, and PROGRAM. In contrast, ACCESS, RESPONSE, and THIRD-PARTIES remained at MIL 1. The assessment identified ten partially implemented critical capabilities across these three domains, preventing consistent achievement of MIL 2.

The RESPONSE domain emerged as the most significant maturity bottleneck. Major weaknesses included insufficiently formalized incident escalation, incomplete incident communication readiness, outdated incident-response procedures, and inadequate protection of backup infrastructure. The absence of data-at-rest encryption on the NAS backup server represented one of the most critical technical risks because it could expose customer information independently of protections implemented in the production environment. The ACCESS domain demonstrated weaknesses associated with centralized PAM and MFA, whereas the THIRD-PARTIES domain revealed insufficient cybersecurity oversight of cloud sub-vendors. These findings indicate that cybersecurity maturity in digital banking must extend beyond traditional perimeter security and encompass identity governance, incident management, data protection, and technology supply-chain dependencies.

The hybrid mapping further indicates that internal cybersecurity capability deficiencies can create broader cybersecurity, privacy, operational, and regulatory consequences. Therefore, cybersecurity maturity assessment should not be treated solely as an internal technical evaluation but should be incorporated into the organization's Governance, Risk, and Compliance strategy. To address the identified gaps, this study proposes a six-month remediation roadmap consisting of three stages: technical hardening, policy formalization, and crisis validation. Implementation of the roadmap followed by a C2M2 reassessment is expected to provide a structured pathway toward achieving a consistent MIL 2 maturity level across all ten domains.

For future research, the maturity assessment can be extended through longitudinal evaluation following implementation of the remediation roadmap. Future studies may also incorporate quantitative metrics such as incident response time, Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), percentage of privileged accounts protected by MFA, encryption coverage, third-party assessment coverage, and tabletop-exercise performance to provide empirical evidence of cybersecurity capability improvement.

Article Information

Author's Contributions: Muhamad Irsan designed the research, supervised the assessment, and led the writing and revision of the manuscript. Muhamad Hasbi Kurniawan conducted the C2M2 self-evaluation, performed the maturity gap and hybrid compliance mapping analysis, and drafted the manuscript. Both authors read and approved the final manuscript.

Acknowledgments: The authors thank the School of Computing, Telkom University, for institutional support during this research.

Conflict of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

Support Section: Not applicable.

Ethical Approval: It is declared that during the preparation process of this study, scientific and ethical principles were followed and all the studies benefited from are stated in the bibliography. Organizational data used in this study were anonymized under the pseudonym PT Bank Finansial Digital (BFD).

Availability: Not applicable / or link

Artificial Intelligence Statement: No artificial intelligence tools were used to generate the research findings of this article.

Plagiarism Statement: This article has been scanned by iThenticate™.

References

[1] O. Aljumaiah, W. Jiang, S. Reddy Addula, M. Amin Almaiah, *Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework*, Journal of Cyber Security and Risk Auditing, **2025**(2) (2025). https://doi.org/10.63180/jcsra.thestap.2025.2.2

[2] B. Christine, C. S. T. Kansil, *Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*, Syntax Literate: Jurnal Ilmiah Indonesia, **7**(9) (2023). https://doi.org/10.36418/syntax-literate.v7i9.13936

[3] J. D. Christopher, D. Gonzalez, D. W. White, J. Stevens, J. Grundman, N. Mehravari, P. Curtis, T. Dolan, *Cybersecurity Capability Maturity Model (C2M2) version 1.1*, Department of Homeland Security, (2014).

[4] L. Dwiaji, A. M. Widodo, G. Firmansyah, B. Tjahyono, *Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector*, Asian Journal of Social and Humanities, **2**(6) (2024). https://doi.org/10.59888/ajosh.v2i6.261

[5] A. A. Garba, M. M. Siraj, S. H. Othman, *An explanatory review on cybersecurity capability maturity models*, Advances in Science, Technology and Engineering Systems, **5**(4) (2020). https://doi.org/10.25046/AJ050490

[6] M. A. Hossain, Md. A. Raza, J. Y. Rahman, *Investigating the Cybersecurity Implications of Open Banking and Application Programming Interfaces (APIs) in the Financial Sector*, Jurnal Ekonomi Dan Bisnis Digital, **4**(1) (2025). https://doi.org/10.55927/ministal.v4i1.13370

[7] National Institute of Standards and Technology, *NIST Privacy Framework: a tool for improving privacy through enterprise risk management*, NIST Special Publication, (2020).

[8] M. Salam, K. A. A. Bakar, A. H. M. Aman, *Building Cyber-Resilient Universities: A Tailored Maturity Model for Strengthening Cybersecurity in Higher Education*, International Journal of Advanced Computer Science and Applications, **16**(5) (2025). https://doi.org/10.14569/IJACSA.2025.0160510