GIJEA
Greenation International Journal of Economics and Accounting
+62 81210467572 https://research.e-greenation.org/GIJEA greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijea.v3i1

An Evaluation of Cybersecurity Risk Management Implementation at Bank Pembangunan XYZ

Ratna Ditha Apsari[1], Tubagus Muhamad Yusuf Khudri[2]
[1]Universitas Indonesia, Jakarta, Indonesia, ratna.ditha@ui.ac.id
[2]Universitas Indonesia, Jakarta, Indonesia, yusufkh@ui.ac.id

Corresponding Author: ratna.ditha@ui.ac.id[1]

Abstract: Cybersecurity risk management in the financial sector is crucial for mitigating cybersecurity threats. The main objective of this study is to evaluate the implementation of cybersecurity risk management at Bank Pembangunan Daerah XYZ. This research employs a qualitative method with a case study strategy, using primary and secondary data sources through semi structured interviews and surveys conducted with employees and managers of Bank Pembangunan Daerah XYZ. The data is processed using narrative analysis techniques. The findings of this study reveal gaps in the implementation of cybersecurity risk management at Bank Pembangunan Daerah XYZ in accordance with the NIST Cybersecurity Framework, across six components: Govern, Identify, Protect, Detection, Response, and Recovery.

Keyword: Bank, Cybersecurity Risk Management, NIST, Cybersecurity Framework.

INTRODUCTION

The financial sector is one of the primary targets of cyberattacks globally, with nearly 30% of incidents targeting financial institutions (IBM 2023). In Indonesia, according to the Financial Services Authority (OJK), there has been an increase in cyber incidents in the banking sector, including data theft and attacks on mobile banking applications. These risks not only result in financial losses but also damage the reputation of financial institutions and public trust in the banking system. Cyber risks encompass threats to the security, integrity, and availability of an organization's information systems. Types of cyber threats include malware attacks, social engineering and phishing, Man-in-the-Middle attacks, Denial of Service (DoS) attacks, zero-day exploits, password attacks, Internet of Things attacks, and injection attacks (IBM, 2024). Therefore, it is essential to implement risk management within an organization, especially in the face of cyber threats.

Bank Pembangunan XYZ, as a regional financial institution that has implemented risk management since 2007, faces these complex threats directly. A data breach resulting in the loss of Rp 21.59 billion in 2023 due to the exploitation of security vulnerabilities highlights the need for a more thorough evaluation. Such exploits can occur due to system vulnerabilities, such as weak security configurations, lack of monitoring of suspicious activities, or abuse of access by internal actors (Radar Bali, 2023). Given these phenomena, a more comprehensive evaluation of the implementation of cybersecurity risk management is required, including an in-depth assessment of the bank's preparedness in facing cyber threats.

Previous research on the evaluation of cybersecurity risk management implementation, such as that by Arenas et al. (2023), found an interactive model that helps organizations identify security weaknesses and provide improvement recommendations through the development of a cybersecurity maturity model to prevent attacks on web-based applications using ISO 27032 and NIST CSF. Research by Cobos et al. (2024) focused on analyzing ransomware threats in the financial sector through a cybersecurity maturity model consisting of six maturity levels and 20 security domains, such as risk mitigation, access control, and post-incident recovery, and found that this model is relevant for improving the resilience of the financial sector against ransomware risks. Additionally, research by Gunawan et al. (2024) identified and managed risks (including cyberattack risks) and recommended enhancing network security, strengthening backup systems, and providing user training to mitigate risks. The presence of this prior research and the case background at Bank XYZ validates the importance of risk management in addressing cyber risks in the financial sector.

Although it shares the same topic, this study is more focused on Bank Pembangunan XYZ, considering its strategic role as a provider of financial services at the regional level. In addition to the case study, this research provides an update to the discourse on risk management in the regional banking sector concerning cybersecurity risks through the Cybersecurity Maturity Model (CMM) approach based on the NIST Cybersecurity Framework (NIST CSF). NIST CSF is a framework to help organizations systematically manage and reduce cybersecurity risks by enhancing organizational resilience to cyber threats, minimizing the impact of security incidents, and ensuring the protection of critical assets, including data and IT infrastructure (National Institute of Standards and Technology, 2024). The use of this approach also represents a gap in previous research.

The urgency of this study lies in the need to address increasingly complex cyber threats that could disrupt operational stability, data security, and the reputation of financial institutions. As an institution with significant responsibilities towards the public and the regional economy, Bank Pembangunan XYZ must ensure that its cybersecurity risk management practices not only meet regulatory standards but also remain responsive to new threats arising from the digitalization of financial services. Based on this, the goal of this research is to evaluate the implementation of cybersecurity risk management and provide recommendations for its improvement at Bank Pembangunan XYZ.

METHOD

This research employs a qualitative method with a case study strategy. The qualitative method is used with the aim of providing an interpretation of how cybersecurity risk management is implemented at Bank Pembangunan XYZ. The case study approach is utilized to collect and analyze data regarding a specific phenomenon, focusing on the context of evaluating the implementation of a system that has been applied and providing recommendations for follow-up actions to improve or maintain its performance (Yin, 2014).

The data sources used in this study include both primary and secondary data. Primary data is obtained through semi-structured interviews and surveys conducted with employees and management of Bank Pembangunan Daerah XYZ. Interviews were held with several key informants representing the Risk Management Division (MRO), Compliance Division (KPN), Strategic Planning Division (RENSTRA), Information Technology Division (TIF), Human Resources Division (SDM), and the IT Governance, Risk & Compliance (ITGRC) unit. The interviews addressed various aspects of risk management, focusing on the dimensions of Govern, Identify, Protect, Detect, Respond, and Recover. Secondary data is obtained through observation of the documentation published by Bank Pembangunan Daerah XYZ on its official website.

In terms of data analysis techniques, this study uses narrative analysis, which is applied to process the results of the interviews. Narrative analysis is used to understand the data by focusing on specific segments that can provide insights related to the research questions.

RESULT AND DISCUSSION

Analysis of Cybersecurity Risk Management Implementation at Bank Pembangunan Daerah XYZ According to NIST Cybersecurity Framework Components

The analysis of cybersecurity risk management implementation at Bank Pembangunan Daerah XYZ is carried out using the NIST CSF approach, which consists of six key components: govern, identify, protect, detect, respond, and recover. Below are the results of the analysis of these NIST components applied to the cybersecurity risk management implementation at Bank Pembangunan Daerah XYZ.

a) Govern

In the Govern analysis, aspects such as Organizational Context, Risk Management Strategy, Roles, Responsibilities & Authorities, Policy, Oversight, and Cyber Supply Chain Risk Management are covered. In the Organizational Context, the Bank formulates its cybersecurity risk strategy and policies using a top-down approach based on its vision and mission as a safe, resilient, and adaptive financial institution in the face of digital transformation. The process begins with reviewing the Bank's strategic direction in its Business Plan (RBB), which is then integrated with its cybersecurity risk management policy. Additionally, the Bank was listed as part of the Computer Security Incident Response Team (CSIRT) under BSSN in 2021.

"We conduct critical asset mapping through annual risk assessments, including identifying services that depend on external systems such as cloud providers and payment switching. This is important so we know which systems need backup and recovery plans." (MRO, 2025)

"Our CSIRT team is trained to respond quickly. We've addressed several critical vulnerabilities based on external reports." (MRO, 2025)

In terms of governance under Risk Management Strategy, the Bank integrates cybersecurity risk management as part of its Enterprise Risk Management (ERM) policy. Every risk policy includes IT risks. For example, operational risk policies include indicators for cybersecurity incidents as part of the Key Risk Indicator (KRI). The Bank also integrates risk mapping into a dashboard to ensure that interconnected risks are effectively monitored. Additionally, the Bank identifies and manages strategic opportunities using a risk-based opportunity management approach in technology planning.

"In every technology-based strategic opportunity, we always conduct a risk analysis first. For example, in developing Open API services, we manage business expansion opportunities by building strict API security standards, sandboxing, and endpoint protection." (TIF, 2025)

On third-party partnerships, the Bank has established third-party risk standards that must be met before engaging in collaborations with suppliers and third-party partners, such as data center providers, cloud services, and payment gateways. These partnerships are subject to regular security assessments. Communication routes are regulated in Service Level Agreements (SLA) and Memoranda of Understanding (MoU), including obligations to report cybersecurity incidents within 24 hours. Technical coordination is generally carried out through regular forums between the IT department and vendors, and the monitoring results are overseen by the Risk Management and Compliance Divisions.

"The role of the Board of Directors and Senior Management in ensuring accountability for cybersecurity risks is critical. They are responsible for setting policies, overseeing the implementation of controls, and ensuring regular reviews and monitoring of all IT security initiatives. Through the Risk Management Committee and IT Steering Committee, the Board is directly involved in strategic decision-making and resource allocation for cybersecurity risk mitigation." (TIF, 2025)

Under the Policy aspect, the Bank develops and socializes its policies with employees in several integrated and comprehensive stages. This process includes a thorough identification of potential cybersecurity threats and risks, benchmarking internal policies against applicable standards and recommendations from regulators, and conducting internal discussions involving strategic units such as the IT Division, Risk Management Division, and Audit Division to ensure the policies align with operational conditions.

Furthermore, the Bank has a policy that requires an annual review and update of its cybersecurity policy. The Bank also conducts incidental reviews in response to significant changes in regulations and guidelines from regulators regarding cybersecurity incidents either internally or across the banking industry. The policy review and update process is conducted through collaboration between the IT Division and the Risk Management Division to ensure that the cybersecurity policy remains up-to-date and effective in addressing emerging threats.

"At least once a year, we review our cybersecurity policy, but we also respond quickly to sudden changes, such as new regulations, significant security incidents, or audit findings. This review process involves cross-division collaboration so we can quickly and effectively adjust policies to meet current threats." (KPN, 2025)

In the Cyber Supply Chain Risk Management aspect, the Bank conducts vendor assessments for all partners and service providers with access to its data, systems, and networks. This process includes filling out security questionnaires, verifying security certifications such as ISO 27001, and performing due diligence on the vendor's track record in managing cybersecurity incidents. The Bank also conducts performance monitoring and audits of vendors on a regular basis. The Bank requires annual cybersecurity posture reports from vendors, including penetration test results or vulnerability assessments if available. Other monitoring methods used include automatic SLA-based monitoring and alarm triggers to detect anomalies in third-party system activities.

"We have a continuous monitoring mechanism for vendors, especially those with access to core systems or sensitive data. Evaluations are done annually or after major changes such as system upgrades. If a vendor fails to meet security commitments, we take mitigation steps, including contract termination." (MRO, 2025)

b) Identify

The analysis of the "Identify" component includes aspects such as Asset Management, Risk Assessment, and Improvement. Below is the analysis of these aspects in the "Identify" component at Bank Pembangunan Daerah XYZ. From the Asset Management aspect, Bank Pembangunan Daerah XYZ conducts hardware inventory through an integrated IT Asset Management (ITAM) system. Additionally, the Bank manages IT assets with a full lifecycle asset management approach, which consists of initial inventory, labeling and tagging, classification, monitoring, annual physical audits, and software inventory. The Bank registers each IT asset through the IT Asset Management System, marked with a unique label for tracking the asset. Assets are then classified based on category, criticality, and data sensitivity. The asset status is periodically monitored using the Configuration Management Database (CMDB). Additionally, in relation to cybersecurity risks, the Bank ensures the security of internal and external network communications by implementing various technical controls such as the use of next-generation firewalls, data encryption (TLS/SSL), VPN for remote access, and network segmentation. Data communication operations are monitored periodically through vulnerability assessments and penetration testing in accordance with regulatory standards.

"To ensure the security of internal and external network communications, we implement layered firewalls, data encryption, VPN for remote access, and network segmentation. All these efforts are aligned with regulatory standards such as OJK and IT security principles based on ISO 27001 and NIST CSF." (TIF, 2025)

In the Risk Management aspect, Bank Pembangunan Daerah XYZ applies a vulnerability management process using both tools and manual testing, conducted periodically, and collaborates with the IT division to validate cybersecurity threats and classify their severity. Additionally, the Bank actively receives information regarding cybersecurity threats from external parties such as regulators (OJK & BI) about developments in cybersecurity threats through circulars, notices, and third-party vendors that typically provide analysis on current threats and global cyberattack trends, along with real-time information from online platforms.

Internal and external threats are identified through monitoring by the Security Operations Center (SOC), security log analysis, alerts from SIEM (Security Information and Event Management), and incident reports from employees through the incident reporting system.

"We identify internal and external threats to our systems through 24/7 SOC monitoring, SIEM alerts, and incident reports from employees. All detected threats are documented in the Bank's Cyber Threat Register." (TIF, 2025)

Once identified, the potential for exploitation of system vulnerabilities is assessed using a risk scoring approach, taking into account the impact on core services, the type of data, and the likelihood of exploitation based on the Vulnerability Scoring System (CVSS). The Bank also requires prospective strategic partners to undergo Third-Party Risk Assessments, which include evaluating security certifications, the results of the latest IT security audits, and the vendor's security governance structure.

In the Improvement aspect, the Bank identifies opportunities for improvement in its cybersecurity management processes by conducting continuous improvement based on data from internal audits, OJK supervisory findings, and feedback from operational units. Each quarterly evaluation results in a list of lessons learned and corrective actions, which are discussed in the Risk Management Committee. Risk evaluations based on security testing results or simulated cyberattacks are conducted through a comprehensive analysis of findings from vulnerability assessments, penetration testing, and simulated cyberattacks. Each finding is analyzed to assess the risk level using a combination of likelihood (probability of occurrence) and impact (its effect on operations and data).

"We evaluate risks by analyzing the results of security tests and simulated attacks, then classify findings based on risk levels. High-risk findings are prioritized for mitigation, and

the evaluation results are reported to the Risk Management Committee and the Board of Directors." (MRO, 2025)

Improvements are developed from the gap analysis between SOPs and actual implementation. Bank Pembangunan Daerah XYZ also conducts incident handling simulations to assess procedure readiness. If discrepancies or ineffective controls are identified, the cybersecurity procedures will be revised or integrated with relevant tools, such as the Security Information and Event Management System (SIEM).

c) Protect

In the analysis of the "Protect" component, the analysis covers aspects such as Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Platform Security, and Technology Infrastructure Resilience in the cybersecurity risk management of Bank Pembangunan Daerah XYZ. Bank Pembangunan Daerah XYZ manages user identities and credentials by implementing a centralized Identity and Access Management (IAM) system. Each user is assigned a unique identity and authentication credentials, such as usernames and passwords that comply with complexity standards. For hardware, access is managed based on roles (role-based access) and controlled via endpoint management devices that verify device IDs.

"We manage user identities and credentials through a centralized Identity and Access Management system. Each user has a unique identity with credentials that meet security standards, and for hardware, access is controlled based on roles through endpoint management." (TIF, 2025)

The Bank undertakes several protection stages, starting with identity verification using multi-factor authentication (MFA), combining something the user knows (password) and something the user has (OTP token or biometric), in addition to verification, user and hardware authentication processes use the Zero Trust Security principle, where every access request must go through user identity verification and device authentication, both in the internal and external environments of the bank. Endpoint devices are continuously monitored to ensure that only verified devices can connect to the bank's network.

In the Awareness and Training aspect, the Bank has conducted training with a three-layered educational approach tailored to the level of risk and job functions of employees. The first is general training that includes basic understanding of cybersecurity threats, email and internet usage rules, simulated cyberattacks, and tips for securing personal accounts and devices. Second, the Bank conducts ongoing internal campaigns related to secure technology use and provides specific warnings during incident escalations or new attacks. Third, the Bank monitors effectiveness by conducting pre-tests and post-tests after training.

"Every new employee must undergo basic cybersecurity training, and we ensure they sign an integrity pact and understand their obligations to maintain data confidentiality before they are granted access to the system." (HR, 2025)

The Bank also implements more advanced and technical training such as role-specific specialization training, certified workshops, external benchmarking, and incident response simulations. Role-specific training is conducted for the IT team, focusing on server hardening, API security, and the ISO 27001 framework; for the audit team, training on forensic investigations, red flag digital fraud, and log monitoring; and for frontliners, training on customer data protection, and secure use of EDC & CRM.

In the Data Security aspect, the Bank ensures the confidentiality, integrity, and availability of data at rest through the implementation of several key technical controls. Data stored on servers, databases, and external storage devices is encrypted using industry-standard algorithms. To maintain integrity, the Bank applies checksums, hash verification, and role-based access controls to ensure that only authorized users can access specific data. Additionally, data storage servers are protected in high-standard data center facilities, with layered physical controls and redundancy systems to ensure data availability under all conditions.

"We ensure the confidentiality, integrity, and availability of data at rest by applying encryption using the AES-256 standard for all stored data. Additionally, we apply role-based access control, verify data integrity using checksums, and ensure availability with redundancy systems at high-standard data center facilities." (TIF, 2025)

Data is protected through a combination of technical and procedural controls. During processing, data is encrypted using memory encryption or secure enclave technology to prevent unauthorized access. Strict access control is implemented at the application level, secure sessions are used, and real-time monitoring of critical data activities is also applied.

In the Platform Security aspect, the Bank configures both software and hardware using a centralized Configuration Management Database (CMDB) approach. Configuration changes are made through a formal change management process, including risk analysis and approval from the IT steering committee. Standard configurations (baseline configurations) are applied to all critical devices, and these standard configurations are protected from unauthorized changes. Configuration audits are conducted periodically to ensure that all software and hardware comply with the established security standards.

"We manage configurations using a centralized Configuration Management Database (CMDB). Every configuration change must go through a formal Change Management process, and the baseline configuration of critical devices is audited periodically to ensure compliance with security standards." (TIF, 2020)

The Bank performs maintenance, replacement, and removal of software and hardware following the IT asset lifecycle based on risk management principles. Hardware that has reached the end of its useful life or software that is no longer supported by the vendor is evaluated based on its impact on security and operations. Regarding hardware removal, the secure wipe method or physical destruction is used, while for software, secure deinstallation procedures are followed to prevent residual data leakage.

In the Technology Infrastructure Resilience aspect, the Bank uses next-generation firewalls, intrusion detection/prevention systems (IDPS), and network segmentation technology to limit and control access to critical parts of the network. Multi-factor authentication (MFA) is also applied to access critical systems. Additionally, the Bank applies security monitoring to detect suspicious activities and ensures that any unauthorized access attempts are promptly detected and responded to.

"We ensure the network is protected using next-generation firewalls, intrusion detection/prevention systems (IDPS), and network segmentation. In addition, multi-factor authentication (MFA) is applied to access critical systems, and monitoring is conducted 24/7 to detect suspicious activities." (ITGRC, 2025)

Furthermore, protection for the Bank's technology assets against natural disasters or technical disruptions is implemented through comprehensive Disaster Recovery (DR) and Business Continuity Planning (BCP). The Bank’s data is replicated to disaster recovery centers located away from the main operational site to mitigate the risk of natural disasters. Redundancy systems for critical hardware and daily automatic data backups are implemented. Regarding technical disruptions, the Bank has a Computer Security Incident Response Team (CSIRT) ready to handle and mitigate issues by conducting real-time monitoring with the aid of specific tools to detect disruptions in networks or applications.

d) Detect

The analysis of the Detect component includes the analysis of cybersecurity risk management in aspects such as Continuous Monitoring and Adverse Event Analysis at Bank Pembangunan Daerah XYZ. In the Continuous Monitoring aspect, the Bank implements a Security Information and Event Management (SIEM) system integrated with firewall devices, intrusion detection systems (IDS), and endpoint protection to conduct real-time monitoring of network activities. This system is designed to detect anomalies, attack patterns, and suspicious traffic that may indicate a cybersecurity incident. Every activity log from servers, core banking systems, and network devices is consolidated and analyzed. The Bank sets certain thresholds that can trigger automatic notifications to the internal CSIRT (Computer Security Incident Response Team) when irregular activity is detected. The Bank also conducts periodic vulnerability scanning and penetration testing to assess the reliability of the security controls in place. Monitoring results are generally analyzed monthly and reported to the Risk Management Division and Board of Directors as part of integrated controls.

"The Bank has implemented a SIEM and IDS system that enables early detection of anomalies and suspicious activities in real-time. Our CSIRT team is tasked with monitoring and following up on all incident notifications 24/7." (ITGRC, 2025)

In its operations, cybersecurity threat monitoring is supported by the Bank's Human Resources Division through steps such as risk mapping based on job roles, monitoring digital activities, implementing a reporting and whistleblowing system, and conducting performance and cybersecurity ethics evaluations.

In the Adverse Event Analysis aspect, the Bank identifies and analyzes anomalies and cybersecurity incidents through the implementation of a Security Monitoring Framework based on risk-based detection and continuous security intelligence. Each identified event is classified based on its potential impact on the confidentiality, integrity, and availability of the Bank's services.

"Every anomaly detected through monitoring systems such as the Fraud Detection System (FDS) and SIEM will be technically and operationally reviewed. We classify the events based on their urgency concerning services, and escalate them to the Cyber Incident Response Team (CIRT) for validation and mitigation. This approach allows us to maintain the continuity of bank operations in real-time." (ITGRC, 2025)

The Bank implements a threat intelligence integration process to correlate information from various sources related to cybersecurity threats to understand the impact of these threats. From internal sources, the Bank obtains information on SIEM logs, internal incidents, and security audits, while external sources provide threat feeds from OJK and BI. The information gathered is then automatically correlated using SIEM and analyzed to assess potential impact, exposed targets, and exploitable vulnerabilities. The analysis results are used to update the Bank's cybersecurity threat model and strengthen cybersecurity defense controls. This approach helps the Bank understand risks from multiple perspectives and proactively enhance resilience.

e) Response

The analysis of the Response component at Bank Pembangunan Daerah XYZ is conducted through the analysis of cybersecurity risk management in several aspects such as Incident Management, Incident Analysis, Incident Response Reporting and Communication, and Incident Mitigation. In the Incident Management aspect, the Bank executes its incident response plan based on the Incident Response Plan (IRP). The IRP is implemented immediately after an incident is verified. When an incident is verified, the Cyber Incident Response Team (CIRT) coordinates the response steps. The incident is classified according to its impact, and escalation is made to management with formal notifications sent to the Compliance and Risk Management Divisions. If the incident impacts external systems, third-party data, or vendor infrastructure, the Bank activates the SOP for coordination with third parties, such as contacting vendors and strategic partners and also coordinating with the relevant regulators. All response activities are recorded in the system for further investigation purposes. The Bank prepares an incident report and conducts a post-incident evaluation for policy improvements, enhanced control systems, and strengthened collaboration with third parties.

"Whenever a cybersecurity incident is verified, we immediately activate the pre-established incident response plan. The Cyber Incident Response Team coordinates across functions to ensure that mitigation steps are directed and proportionate to the impact scale. If the incident involves third parties, such as IT vendors or network partners, we immediately coordinate through communication channels agreed upon in the cooperation agreements. All processes are documented and aligned with reporting protocols to the regulators." (ITGRC, 2025)

The Bank conducts triage and incident validation through steps such as initial reporting by users, system monitoring, or third-party vendors, performing initial triage to categorize the incidents based on priority levels (low, medium, high, and critical), validating the incident using digital forensics, log analysis, and manual investigation. Once validated, the incident is classified based on the type of threat and its priority level for handling.

In the Incident Analysis aspect, the Bank analyzes each cybersecurity incident through a structured and documented Root Cause Analysis (RCA). This process is conducted by the CIRT in collaboration with the IT Governance, Risk & Compliance Division. The steps taken include gathering logs and detailed chronologies, analyzing the techniques, tactics, and procedures used, assessing weaknesses and control gaps exploited either technically or procedurally, determining the technical and organizational root causes of the incident, and preparing a remediation and strengthening plan to prevent similar incidents from recurring. The RCA is performed formally, and its results are documented in a post-incident evaluation report, which is discussed at the management level and presented to the Board of Directors. All activities during the incident investigation process are systematically documented using an incident tracking & forensic logging system.

In the Incident Response Reporting and Communication aspect, the Bank has clear, structured procedures for cybersecurity incident communication that align with internal policies and regulations from OJK and BI. These procedures include the Bank's CSIRT, which is responsible for internal and external coordination during incidents, with assistance from the Compliance Division to ensure communication procedures are consistently followed according to applicable standards. Once an incident is identified, the Bank notifies the Board of Directors and all relevant internal parties via internal communication channels. The Bank also ensures that incident reports are sent to regulators in a timely manner, with proactive and transparent communication. The Compliance Division communicates with the Public Relations and CSR Division to manage information for customers and the public to ensure clarity, accuracy, and accountability. After the incident is resolved, the Bank evaluates the effectiveness of the communication efforts to improve communication quality and responsiveness in the future.

"During the incident recovery process, we provide regular updates to regulators, management, and relevant external parties. Every development, mitigation step, or challenges encountered are communicated openly, both through official reports and special coordination meetings." (KPN, 2025)

In the Incident Mitigation aspect, the Bank implements mitigation steps to prevent the spread of a cybersecurity incident quickly and in a structured manner through the isolation of affected systems, blocking harmful access, and applying additional controls such as reducing access rights and terminating active sessions. If the incident originates from a technical vulnerability, the CIRT immediately performs emergency patching or applies a recommended temporary solution. All mitigation steps are coordinated with third parties if external vendors are involved, and real-time monitoring is applied. These actions are fully recorded in the incident tracking system to ensure accountability and effectiveness in limiting the impact of the cybersecurity incident before entering the recovery phase.

"Once an incident is detected, we immediately isolate the affected systems and apply technical controls such as blocking access or patching. All actions are coordinated and monitored in real-time to prevent further spread." (ITGRC, 2025)

f) Recover

The analysis of the Recover component includes aspects such as Incident Recovery Plan Execution and Incident Recovery Communication. In the Incident Recovery Plan Execution aspect, the Bank recovers from a cybersecurity incident based on scenarios prepared in the Business Continuity Plan (BCP) and Incident Recovery Plan (IRP). The decision will then be made on whether recovery will be done fully, gradually, or through a backup system. Priority is given to financial transaction services and operations involving the public. The execution is overseen directly by the CSIRT and Risk Management Division.

"Recovery is done gradually, starting with ensuring that financial transaction services are restored first, even if it has to be run from backup systems. That's the key principle in our BCP." (MRO, 2025)

In the Incident Recovery Communication aspect, the Bank uses systematic communication, beginning with the Compliance Division and IT Division providing periodic internal reports on recovery progress through regular coordination meetings, daily or weekly situation reports, and informal communication to ensure all internal parties are kept updated on recovery status. The Bank communicates with regulators on a scheduled basis with progress reports covering the current recovery status, additional mitigation steps, and any further risk evaluations required by regulators. Simultaneously, the Bank communicates with business partners and external parties to ensure everyone understands the current situation and the actions being taken by the Bank. Transparently, the Bank also informs customers about service recovery progress through various official channels. Communication efforts are evaluated based on feedback from stakeholders to ensure the effectiveness, clarity, and transparency of the information conveyed.

"During the recovery process, we routinely provide updates to regulators, management, and relevant external parties. Every development, mitigation step, and challenges faced are

communicated openly, both through official reports and special coordination meetings." (KPN, 2025)

Evaluation of Cybersecurity Risk Management Compliance with NIST Cybersecurity Framework

Based on the analysis of the compliance of cybersecurity risk management implementation at Bank Pembangunan Daerah XYZ according to the components of the NIST Cybersecurity Framework, there are both strengths and weaknesses in the implementation of cybersecurity risk management that need to be addressed to improve the quality of the services provided. The findings are as follows:

In the Govern component, the Bank has built a fairly systematic cybersecurity governance framework. This is reflected in the establishment of the CSIRT team, the integration of cybersecurity risk management strategies into the Bank's Business Plan (RBB), and the implementation of information security policies that follow ISO 27001 standards. However, there are gaps in the governance process that can be improved. There is no document explicitly mapping the expectations of stakeholders such as regulators, business partners, and customers regarding cybersecurity. Furthermore, specific Key Performance Indicators (KPIs) for cybersecurity success have not been formulated in a measurable and documented manner. The socialization of the information security policy has also not reached all levels of the organization evenly. This is evident from the lack of formal evidence of policy dissemination or reporting on the staff's understanding of the policy. Therefore, cybersecurity governance would be more effective if complemented with a stakeholder communication mechanism and measurable performance reporting to ensure decision-making is based on comprehensive input and objective data.

In the Identify component, the Bank has demonstrated a commitment to IT risk management by performing digital asset inventory through the ITAM system and establishing Key Risk Indicators (KRIs). This identification forms an important foundation for detecting potential threats to information systems. However, further evaluation reveals that the system does not cover the recording of non-physical assets such as software licenses and APIs, which also carry significant risks. The current cybersecurity risk assessment is still descriptive and does not yet utilize a quantitative approach to calculate the financial impact of potential incidents. Furthermore, there is no documented mechanism regarding the use of lessons learned from previous incidents to update SOPs or IT policies. This indicates a need for strengthening the risk identification process through the integration of historical data and quantitative analysis, enabling risk management to play a strategic role in long-term security planning.

In the Protect component, the Bank has implemented adequate technical protections such as tiered employee training, role-based access controls, and regular data backup procedures. These efforts support operational stability and minimize internal vulnerabilities. However, there are several key aspects that have not been optimally implemented. Some internal applications are not yet connected to a centralized access management system, and protection of data in transit, such as on email communications and banking applications, has not been technically documented in the policy. Additionally, there is no evidence of the implementation of active protection systems like Endpoint Detection and Response (EDR) or proactive anti-malware technologies. To ensure comprehensive cybersecurity protection, the company needs to develop a layered security architecture and ensure that every system layer is actively protected, including endpoint devices and data in transit.

In the Detection component, the Bank has established a monitoring and alert system for anomalous activities on ATM and e-channel services. The active role of CSIRT in monitoring potential incidents adds value to the organization's responsiveness. However, the use of advanced detection technologies is still limited. The Bank has not yet implemented a SIEM (Security Information and Event Management) system to automatically integrate and correlate logs from various systems. Incident analysis is still done manually, without support from big data or machine learning-based tools. Given the increasing complexity of threats, detection capabilities need to be enhanced to be not only reactive but also predictive and responsive on a larger scale.

In the Response component, the Bank has formalized incident response procedures through SOPs and cross-unit training involving the CSIRT team. Incident reporting to regulators and internal communication has been structured. However, the organizational response could still be strengthened. There is no emergency communication channel or dashboard that allows for quick decision-making during real-time incidents. Additionally, the SOPs have not explicitly linked updates with reflections and lessons learned from previous incidents. Strengthening the response will greatly depend on the organization's ability to manage crises in a coordinated manner, supported by information systems and continuous evaluations of every cybersecurity event that has occurred.

In the Recovery component, the Bank has a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) that are routinely tested for ATM systems and other main services. This shows the company's preparedness in anticipating service disruptions due to IT incidents. However, the scope of testing does not yet include digital services such as mobile banking or recovery scenarios involving third parties like cloud vendors. Evaluations of recovery communication are also not systematically documented, despite being important for maintaining public and stakeholder trust. Therefore, the company needs to expand testing scenarios and design post-crisis communication evaluations to make the entire recovery process more adaptive and responsive to the dynamics of digital threats.

CONCLUSION

Based on the discussion presented, Bank Pembangunan Daerah XYZ has systematically implemented a cybersecurity risk management approach. However, through a review using the NIST Cybersecurity Framework as an evaluation effort, several optimization opportunities have been identified in six key components of the NIST framework as follows:

1. Governance Component: Optimization in governance can be achieved by explicitly providing documentation for mapping stakeholder expectations, as well as enhancing strategic success through the creation of specific KPIs for cybersecurity.
2. Identify Component: The current condition indicates the need for strengthening the risk identification process through the integration of historical data and quantitative analysis, enabling risk management to play a more strategic role.
3. Protect Component: To ensure comprehensive cybersecurity protection, the bank needs to develop a layered security architecture and ensure that each system layer is actively protected, including endpoint devices and data in transit.
4. Detection Component: Given the increasing complexity of threats, the detection capability needs to be enhanced to be not only reactive but also predictive and responsive on a larger scale.
5. Response Component: SOP updates have not been explicitly linked to the results of reflections and lessons learned from previous incidents. Therefore, support from

information systems and continuous evaluation of every cybersecurity event that has occurred is needed.

6. Recovery Component: The company needs to expand testing scenarios and design post-crisis communication evaluations to ensure the recovery process is more adaptive and responsive to the dynamics of digital threats.

REFERENCES

Badan Siber dan Sandi Negara (BSSN). (2021). Laporan Tahunan Keamanan Siber Indonesia 2021. https://bssn.go.id/laporan-tahunan-keamanan-siber-indonesia-2021/

Badan Siber dan Sandi Negara (BSSN). (2023). Industri Keuangan Rentan Terhadap Serangan Siber. Diakses dari https://finansial.bisnis.com/read/20240729/90/1786201/bank-digital-dan-industri-keuangan-indonesia-yang-rentan-terhadap-serangan-siber

Bougie, R., & Sekaran, U. (2020). Research Methods for Business: A Skill Building Approach. Wiley.

CNBC Indonesia. (2023, 15 November). BPD Bali kebobolan Rp21,59 M, dana nasabah raib. Diakses dari https://www.cnbcindonesia.com/market/20231115063713-17-489065/bpd-bali-kebobolan-rp2159-m-dana-nasabah-raib

CNBC Indonesia. (2023, 15 November). BPD Bali kebobolan, Rp21,59 M dana nasabah raib. Diakses dari https://www.cnbcindonesia.com/market/20231115063713-17-489065/bpd-bali-kebobolan-rp2159-m-dana-nasabah-raib

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management—Integrating with Strategy and Performance. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Halim, A., & Mais, E. (2020). Evaluasi Penerapan Manajemen Risiko dalam Audit Kepabeanan. Jurnal Akuntansi dan Keuangan, 15(2), 123-135.

IBM Security X-Force. (2023). Threat Intelligence Index 2023. https://www.ibm.com/downloads/cas/ADLMYLAZ

IBM Security. (2023). Jenis Ancaman Siber dan Strategi Mengatasinya. Diakses dari https://www.ibm.com/id-id/think/topics/cyberthreats-types

Illahi, A. S., Rahman, F., & Putra, A. (2023). Strategi Manajemen Risiko Operasional Selama Pandemi COVID-19. Jurnal Manajemen Risiko, 10(1), 45-58.

Kenyon, B. (2019). ISO 27001 controls: A guide to implementing and auditing. IT Governance Publishing.

Liputan6.com. (2023, 15 Mei). Phishing hingga ransomware jadi ancaman nyata buat keamanan perbankan. Diakses dari https://www.liputan6.com/tekno/read/5583386/phishing-hingga-ransomware-jadi-ancaman-nyata-buat-keamanan-perbankan

National Institute of Standards and Technology. (2024). Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. National Institute of Standards and Technology (NIST).

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

Otoritas Jasa Keuangan (OJK). (2016). Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum.

https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Pages/POJK-Nomor-18.POJK.03.2016.aspx

Otoritas Jasa Keuangan (OJK). (2021). Consultative Paper - Manajemen Risiko Keamanan Siber Bank Umum. Otoritas Jasa Keuangan. Diakses dari https://www.ojk.go.id/id/kanal/perbankan/implementasi-basel/Documents/Pages/Consultative-Papers/Consultative%20Paper%20Manajemen%20Risiko%20Keamanan%20Siber%20Bank%20Umum.pdf

Otoritas Jasa Keuangan (OJK). (2022). Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. https://www.ojk.go.id/id/regulasi/Pages/Penyelenggaraan-Teknologi-Informasi-Oleh-Bank-Umum.aspx

Otoritas Jasa Keuangan (OJK). (2022). Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum. https://www.ojk.go.id/id/regulasi/Pages/Ketahanan-dan-Keamanan-Siber-Bagi-Bank-Umum.aspx

Radar Bali. (2023, 12 Januari). Bobol Rp 21 miliar, tabungan nasabah BPD Bali tiba-tiba lenyap berpindah rekening, Polda Bali selidiki. Diakses dari https://radarbali.jawapos.com/perbankan/703269543/bobol-rp-21-miliar-tabungan-nasabah-bpd-bali-tetiba-lenyap-berpindah-rekening-polda-bali-selidiki

Solihin, I., & Kurniawan, A. (2022). Penguatan Manajemen Risiko dalam Menghadapi Ancaman Siber pada Lembaga Keuangan Syariah. Jurnal Keuangan Islam, 8(3), 210-225.

Sudarmanto, E., Astuti, K., Kato, I., Basmar, E., Simarmata, H. M. P., Yuniningsih, I., Wisnujati, N. S., & Siagian, V. (2021). Manajemen risiko perbankan. Yayasan Kita Menulis. ISBN 978-623-342-051-8.

Sugiyono. (2018). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.

Suryanto. (2019). Manajemen Risiko dan Asuransi.

The NIST Cybersecurity Framework (CSF) 2.0. (2024). https://doi.org/10.6028/NIST.CSWP.29

Tirto.id. (2023, 15 Mei). Serangan ransomware & upaya perbankan minimalisasi ancaman siber. Diakses dari https://tirto.id/serangan-ransomware-upaya-perbankan-minimalisasi-ancaman-siber-gSg3

Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. Computers and Security, 139. https://doi.org/10.1016/j.cose.2024.103708

World Economic Forum. (2023). The Global Risks Report 2023 (18th ed.). World Economic Forum. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2023

Yin, R. (2014). Case Study Research: Design and Methods (5th ed.). Sage.