ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

# NIST-Based Cybersecurity Risk Management for Mitigating Customer Data Breaches and Cyber Threats in Banking

Mercurius Broto Legowo[1]; Budi Indiarto[2]; Adzrani Haura Badzlinaya Novianto[3]; Nasywa Aliyya Omar[4]

[1,2,3,4]Faculty of Information Technology, Perbanas Institute Jakarta, Indonesia

Publication Date: 2026/08/20

**Abstract: The rapid digitalization of business processes has heightened organizational vulnerability to cybersecurity threats, particularly customer data breaches, unauthorized access, malware, phishing, and cyberattacks. These threats can compromise sensitive information, disrupt operations, cause financial losses, and erode customer trust. This study aims to examine the implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) for mitigating customer data breaches and cybersecurity threats. A qualitative research approach is employed to analyze cybersecurity risks, vulnerabilities, security controls, and risk mitigation practices in accordance with the NIST RMF. The framework encompasses a systematic process for categorizing information systems, selecting and implementing security controls, assessing control effectiveness, authorizing systems, and continuously monitoring risks. The results indicate that a NIST-based approach can assist organizations in identifying and prioritizing cybersecurity risks, strengthening data protection mechanisms, enhancing incident readiness, and optimizing continuous security monitoring. The findings suggest that strengthening customer data protection requires a holistic approach integrating technological safeguards, organizational governance, employee awareness, risk assessment, and effective incident response mechanisms. This study contributes to the cybersecurity risk management literature by proposing a structured approach to strengthening organizational resilience against customer data breaches and evolving cyber threats.**

***Keywords:*** *Banking; Cyber Threats; Data Breach; NIST RMF; Risk Management.*

**How to Cite:** Mercurius Broto Legowo; Budi Indiarto; Adzrani Haura Badzlinaya Novianto; Nasywa Aliyya Omar (2026) NIST-Based Cybersecurity Risk Management for Mitigating Customer Data Breaches and Cyber Threats in Banking. *International Journal of Innovative Science and Research Technology*, 11(8), 1152-1158. https://doi.org/10.38124/ijisrt/26aug509

## I. INTRODUCTION

Banks operate in an environment characterized by significant risks, making effective responses to fundamental threats that could materially undermine institutional performance critical to their sustainability[1]. Risk management within the banking sector has drawn heightened scrutiny in recent years, particularly in the wake of turbulence that has inflicted severe damage on the credibility and viability of financial institutions[2]. Governments and regulatory bodies alike have recognized the consequences of inadequate risk governance in banking, prompting the introduction of a series of legislative and regulatory instruments aimed at curbing the risks embedded in day-to-day banking operations. Amongst the risks attracting the most serious attention are customer data breaches and the sustained threat of cyber-attacks. Customer data breach risk emerges from the exposure of sensitive personal information such as national identification numbers (NIK) and taxpayer registration numbers (NPWP).

This constitutes a form of intrusion or systemic security failure. Data leakage may equally originate from financial service providers, whether through the deliberate sale of customer data, its transfer to third parties, or the vulnerability of data protection systems to exploitation by hackers[3]. Cyber-attacks, for their part, are offensive acts carried out by one computing or telecommunications network against another, targeting websites, computer systems, and individual devices. Cyber-attack risk thus encompasses deliberate efforts by individuals or organized groups to infiltrate, damage, manipulate, or gain unauthorized access to computer systems or networks.

Indonesia's banking sector has not been immune. A striking case in point saw approximately 15 million customers of one of the country's largest Islamic banks fall victim to a data breach in May 2023, with the total volume of stolen data reaching 1.5 terabytes, encompassing customer credentials, personal information, and loan records[4]. The ransomware attack that simultaneously disrupted this

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

institution's services served as a sobering warning to the wider industry.

In a separate incident, the insurance arm of a major national bank suffered a data breach in July 2021 during which the personal records of two million policyholders were stolen and offered for sale online, with the perpetrators allegedly exfiltrating 250 Gigabytes of data for approximately USD 7,000 [5]. These incidents are part of a broader pattern, as government data indicate that Indonesia faces approximately 1.225 billion cyberattack attempts each day[5]. Such a scale of threat warrants the sustained attention of both academics and industry practitioners.

This study aims to examine the implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) for mitigating customer data breaches and cybersecurity threats. This study employs the NIST Risk Management Framework (NIST RMF) as a structured framework for managing cybersecurity risks in the banking sector. Its objectives are to identify customer data breach and cyber-attack risks, analyze these risks using the NIST RMF, and evaluate their severity to facilitate effective risk management and mitigation.

The novelty of this study resides in its application of the NIST RMF to analyze and evaluate customer data breach and cyber-attack risk management specifically within the banking industry.

## II. LITERATURE REVIEW

- *Data Breach and Cyber Attack*

Data breaches and data leaks have become major cybersecurity concerns in the digital era, particularly in industries that manage large volumes of sensitive information, such as the banking sector [6]. Although both terms are often used interchangeably, researchers distinguish them based on the nature and source of the incident. A data breach refers to intentional and unauthorized access to confidential information conducted by external attackers through cyberattacks such as hacking, phishing, malware, ransomware, or network exploitation [7]. In contrast, a data leak occurs when sensitive information is unintentionally exposed due to internal weaknesses, including human error, system misconfiguration, weak access control, or poor data governance practices [8]. Both incidents may result in the unauthorized disclosure of personal, financial, and organizational data, causing significant operational and reputational consequences for organizations

According to Romanosky et al.[7] Data breaches in the financial sector often lead to substantial economic losses, regulatory penalties, and declining customer trust because financial institutions depend heavily on information security and public confidence. Similarly, Alhassan, Sammon, and Daly [9] explain that the rapid adoption of digital banking technologies and cloud-based services has increased organizational vulnerability to cyber threats due to the expansion of interconnected digital infrastructures. These technological developments create broader attack surfaces that can be exploited by cybercriminals targeting banking systems and customer information.

- *Cybersecurity Risk Management*

Risk management remains a core banking function, particularly in mitigating risks that may adversely affect profitability[10]. Cybersecurity Risk Management is a systematic process of identifying, assessing, mitigating, monitoring, and responding to cybersecurity risks to protect an organization's information assets, systems, and digital services. In the banking sector, cybersecurity risk management aims to protect customer data, financial assets, information systems, and digital services from cyber threats while ensuring the confidentiality, integrity, and availability of critical information and services**.** According to ISACA (2012) [11] IT risk management of identifying, assessing, controlling, and monitoring risks related to the use of information technology within organizations. To manage and mitigate cybersecurity risks, particularly in the banking sector, a systematic approach involves integrating risk assessment, security controls, governance, incident response, and continuous monitoring through the NIST Risk Management Framework (NIST RMF).

- *NIST Risk Management Framework(RMF)*

The NIST RMF provides a comprehensive and systematic framework for identifying, assessing, and managing information security risks within federal information systems[12]. The framework emphasizes continuous monitoring, iterative risk management, and the integration of risk governance into the organization's overall security strategy[12].

Fig 1 NIST Risk Management Framework

Figure 1 illustrates the seven stages of the NIST RMF, which provide a structured approach to cybersecurity risk management: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Within the broader risk management paradigm, these components map onto three overarching phases that consist of risk identification, risk analysis (via the NIST RMF), and risk evaluation. Prior research by Tony Tan and Benfano Soewito in 2022, in a study titled "Cyber Attack Risk Management Using the NIST Cybersecurity Framework at ZXC University," adopted a quantitative methodology[13]. That study

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

examined the complex resource demands of higher education institutions predominantly in relation to IT infrastructure and assets in the context of supporting research-intensive and industry-oriented education. Regarding that environment, data transmission security was identified as critical to operational productivity, given the institution's susceptibility to cyber-attacks.

The ZXC University case in Batam highlighted serious challenges pertaining to the security of network infrastructure and internal web service systems. To tackle these risks, the study recommended the deployment of penetration testing alongside the NIST Cybersecurity Framework. Its findings and recommendations are applicable beyond higher education, serving as a transferable blueprint for comparable institutions.

➢ *Research Conceptual Framework*

The conceptual framework illustrated in Figure 2. Revealed how Customer Data Breaches and Cyber Attacks act as the primary cybersecurity threats that trigger the risk management process.

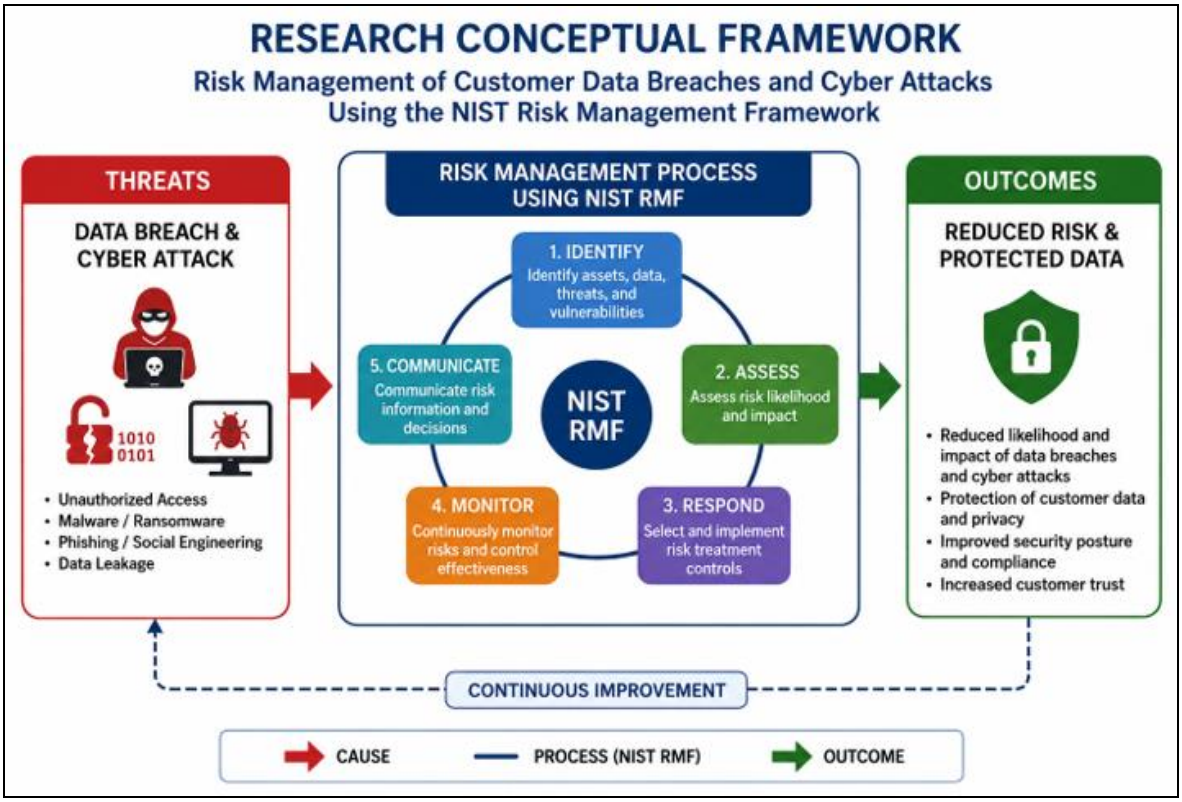


Fig 2 Research Conceptual Framework

These threats are systematically managed using the NIST Risk Management Framework (RMF), which consists of five continuous activities: Identify, Assess, Respond, Monitor, and Communicate. Through this structured process, organizations can identify vulnerabilities, evaluate risks, implement appropriate security controls, continuously monitor their effectiveness, and communicate risk-related information to stakeholders. The anticipated outcomes include reduced cybersecurity exposure, stronger customer data protection, enhanced regulatory compliance, and increased customer trust. The continuous improvement cycle ensures that the organization continuously adapts its security posture to address evolving cyber threats.

## III. METHODOLOGY

In this study, the qualitative method is used[14]. A qualitative research approach focuses on understanding phenomena by developing insights from an inductive interpretation of reality[15].

Data in qualitative research can be gathered through various techniques, such as in-depth interviews, direct observations, document reviews, and focus group discussions. The data collection technique used in this study is documentation, specifically through previously produced journals. Documentation is the process of substantiation based on any type of source—whether written, oral, pictorial, or archaeological[16].

Furthermore, the analysis technique in this study employs the NIST RMF framework. The NIST RMF framework promotes continuous security monitoring and ongoing improvement of risk management practices while aligning them with the organization's broader cybersecurity strategy[12].

## IV. RESULT AND DISCUSSION

The findings and discussion are structured around three core processes of cybersecurity risk management: risk identification, risk analysis, and risk evaluation.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

➢ *Risk Identification*

A fundamental aspect of risk management, risk identification focuses on recognizing potential threats that may prevent an organization from achieving its objectives[17]. Its purpose is to catalogue the full range of risks confronting a given organization. Risk levels and their respective descriptions are set out in Table 1.

Drawing upon the risk level taxonomy established in Table 1, the risk identification process was subsequently conducted. The results of customer data breach risk and cyber-attack risk are presented in Table 2. Overall, risk classification helps prioritize the cybersecurity risk management based on the likelihood and potential impact of the identified risks. The approach follows ISO 31000:2018 and NIST RMF principles by aligning mitigation strategies with the severity of identified risks.

Table 1 The Results of Risk Identification

| Risk Level | Level Description | Remarks |
|---|---|---|
| 1 | Low Probability Low Impact (Low Risk) | A risk with the least significant degree of influence relative to other risk categories, and under appropriate policy conditions, it may be disregarded. |
| 2 | Low Probability High Impact (Low-High Risk) | A risk of intermediate influence. Notwithstanding its lower likelihood, it warrants ongoing monitoring and sustained mitigation commensurate with its potential impact. |
| 3 | High Probability Low Impact (High-Low Risk) | A risk exerting moderate effect, albeit one that requires only routine monitoring rather than active intervention, in contrast to the Low Probability High Impact category. |
| 4 | High Probability High Impact (High Risk) | The most consequential risk tier, carrying the greatest potential for harm. It demands prompt and decisive remediation. |

Table 2 Risk Evaluation Results

| Risk Type | Risk Identification | Risk Level |
|---|---|---|
| Customer Data Breach Risk | Customer data breach risk arises from the unauthorized uploading or exposure of sensitive personal information, including national identification numbers and taxpayer numbers[18]. | 4 |
| Cyber Attack Risk | Cyber-attack risk refers to the intentional effort by individuals or organized groups to infiltrate, disrupt, manipulate, or gain unlawful access to computer systems or networks without authorization[19] | 4 |

➢ *Risk Analysis*

Once the risks had been identified, a systematic risk analysis was undertaken to examine their characteristics and develop a comprehensive understanding of their potential implications[17].

Table 3 summarizes the risk analysis findings in accordance with the NIST Risk Management Framework (NIST RMF).

Table 3 The Results of Risk Analysis Using the NIST-RMF

| NIST-RMF Component | Analysis Findings Based on NIST-RMF |
|---|---|
| **Prepare** | At this stage, it is imperative to identify emerging risks to execute the Risk Management Framework effectively. Risks that recur most frequently include:<br>1) Cyber-attacks (phishing, malware, ransomware, etc.)<br>2) Customer profiling and data misuse<br>3) Account compromise and financial fraud |
| **Categorize** | Following identification, risks are grouped into separate tiers according to the magnitude of their impact:<br>1) Level 1: (readily containable impact): profiling/data misuse<br>2) Level 2: (moderately difficult to contain): account compromise<br>3) Level 3: (most difficult to contain): cyber attacks |
| **Select** | Risk controls should be aligned with the severity of identified threats. Appropriate measures include encryption, secure backups, firewalls, and access controls for data protection, robust authentication and recovery mechanisms for account security, and continuous monitoring with regular system updates to mitigate cyber-attack risks. |
| **Implement** | At this juncture, the controls identified during categorizations are actively deployed and documented:<br>1) Profiling or data misuse:<br>• Data encryption transforms data into an unintelligible format requiring system-level decryption, effectively preventing extraction by unauthorized parties [20].<br>Implementing regular data backups in a separate repository alongside firewall protection strengthens organizational resilience by preventing data loss, mitigating the impact of data misuse, and restricting unauthorized network access through continuous traffic monitoring. |

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

| | |
|---|---|
| | 2) Account compromise:<br>• Robust security systems forestall unauthorized access to internal systems, thereby significantly raising the barrier to financial fraud [21]<br>• Crisis recovery planning ensures that in the event of a breach, residual risk is minimized and operational continuity is restored.<br>3) Cyber attacks<br>Implementing a comprehensive and continuously updated security framework reduces the risk of malware, DDoS attacks, and unauthorized access while protecting sensitive data, ensuring regulatory compliance, and enabling the early detection and timely response to cybersecurity incidents. |
| **Assess** | In the subsequent phase, the operational performance of previously implemented controls is subjected to systematic analysis to identify residual vulnerabilities across each risk category, and a comprehensive report documenting the outcomes of the implementation phase is then produced |
| **Authorize** | Subsequently, the completed report is submitted to the relevant authority or senior official who reviews findings and determines whether existing controls are to be maintained or superseded by measures anticipated to yield more satisfactory outcomes. |
| **Monitor** | The final stage involves continuous monitoring to assess control effectiveness, detect environmental changes, and strengthen the organization's resilience to emerging threats and vulnerabilities. |

➢ *Risk Evaluation*

This section states that the Risk Evaluation stage determines the significance of identified risks by assessing their potential consequences based on pre-established organizational criteria.[17]. It utilizes the insights generated during the risk analysis phase to inform decisions regarding future risk management action [12].

Accordingly, a structured risk evaluation was performed for both cyberattack and customer data breach risks expressly aimed at prioritizing the allocation of risk management resources and actions to the most consequential threats. The evaluation of cyberattack and customer data breach risks in the banking sector is presented in Table 4.

Table 4 The Results of Risk Evaluation

| Risk Priority / Category | Risk Level | Target Residual Risk Level | Risk Mitigation Decisions | Key Risk Indicators (KRI) |
|---|---|---|---|---|
| Customer Data Breach | Level 4 | Level 3 | 1) Increase employee awareness through cybersecurity training and malware education.<br>2) Implement and enforce mandatory security policies for all employees.<br>Conduct regular penetration testing to identify and fix security vulnerabilities.<br>4) Deploy endpoint protection to secure user devices against data breach threats. | ) Human error remains the single largest precipitating factor in data breaches.<br>2) Malware infiltration causes systemic damage and corporate data theft.<br>3) Insider threat from disloyal employees. |
| Cyber Attack | Level 4 | Level 3 | 1) Strengthen customer-facing protections to reduce attack vectors.<br>2) Achieve seamless integration of security systems and IT infrastructure.<br>Enhance organizational security within hybrid work settings through the deployment of endpoint security.<br>4) Bolster technical defences by collaborating with cybersecurity vendors to engineer a maximally robust security architecture.<br>) Endpoint protection secures end-user devices, such as laptops, desktops, and mobile devices, against data leakage. | Rapid digitalization increases vulnerability to cyber-attacks.<br>Cloud adoption raises the risk of confidential data breaches.<br>Remote work expands the attack surface and cyber risks. |

➢ *Discussion*

The findings suggest that customer data breaches and cyberattacks represent the most significant cybersecurity threats, as they can compromise the confidentiality, integrity, and availability of an organization's information assets. The implementation of the NIST Risk Management Framework (RMF) helps organizations to systematically identify, assess, evaluate, and prioritize cybersecurity risks based on their likelihood of occurrence and potential impact.

The findings demonstrate that risks characterized by a high likelihood of occurrence and significant potential impact require prompt mitigation through effective security measures, such as multi-factor authentication (MFA), encryption, role-based access control (RBAC), continuous

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

monitoring, and cybersecurity awareness training for employees. This structured approach supports more effective cybersecurity governance and aligns security investments with organizational risk priorities.

This study shows that the NIST RMF provides a holistic approach to cybersecurity risk management by integrating risk-based decision-making, governance, and continuous monitoring. Unlike studies on specific technologies or isolated threats, this research emphasizes an integrated framework for strengthening organizational resilience against customer data breaches and cyberattacks. The study is limited by its qualitative application within a specific organizational context. Future research should validate the framework across industries using quantitative methods such as FAIR, Bayesian networks, or machine learning. The main novelty lies in integrating customer data breach and cyberattack risks into a unified NIST RMF framework that links security controls with governance and strategic decision-making.

## V. CONCLUSION

This study concludes that customer data breaches and cyber threats represent significant information security risks for the banking sector, given the sensitivity of financial and personal information managed by banking institutions. The application of the NIST Risk Management Framework (RMF) provides a systematic approach for identifying, assessing, prioritizing, and mitigating these risks through risk-based security controls and continuous monitoring.

The findings indicate that effective mitigation requires a combination of data encryption, access control, strong authentication, secure data backups, firewall protection, regular system updates, continuous monitoring, and incident response mechanisms. The NIST-based approach enables banks to align cybersecurity controls with risk severity while strengthening data protection, operational resilience, regulatory compliance, and customer trust. This study integrates customer data breaches and cyber threats into a unified NIST-based framework, linking security controls with risk governance and strategic decision-making.

Future research should validate the proposed approach through empirical studies across multiple banking institutions and incorporate quantitative risk assessment techniques to provide more precise estimates of cybersecurity exposure and potential financial impact.

## ACKNOWLEDGMENT

The authors express their appreciation for the institutional support and academic environment provided by Perbanas Institute, which enabled the successful completion of this research. We also acknowledge the invaluable academic guidance and constructive insights provided throughout the process, which significantly enhanced the rigor and clarity of this scholarly work.

## REFERENCES

[1]. A. Kurniawan, A. Rahayu, and L. A. Wibowo, “The Effect of Digital Transformation on the Performance of Regional Development Banks in Indonesia,” J. Ilmu Keuang. dan Perbank., vol. 10, no. 2, pp. 158–181, 2021, doi: 10.34010/jika.v10i2.4426.

[2]. S. R. Vaidyula and J. Kavala, Enterprise Risk Management for Banks, no. August. 2018.

[3]. A. Soemitra and Adlina, “Consumer Protection Against Data Leakage in Financial Services in Indonesia,” J. Insitusi Politek. Ganesha Medan Juripol, vol. 5, pp. 288–303, 2022.

[4]. CNN Indonesia, “Kominfo Clarifies the Alleged BSI Data Leakage Circulating,” CNN News. 2023. [Online]. Available: https://www.cnnindonesia.com/teknologi/20230522122857-192-952382/kominfo-klarifikasi-soal-dugaan-bocoran-data-bsi-yang-beredar

[5]. F. C. Rosana, “BRI Life Customer Data Leaks Evidence of Weak Protection and Regulation,” Tempo.co.id. 2017. [Online]. Available: https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi

[6]. P. Gowda and A. N. Gowda, “Data Breach as a Threat in the Banking Sector and Steps to Avoid It,” Int. J. Sci. Res. (IJSR, vol. 10, no. 4, pp. 2019–2022, 2021.

[7]. S. Romanosky, R. Corporation, and S. H. St, “Examining the costs and causes of cyber incidents,” J. Cybersecurity, vol. 2, no. August, pp. 121–135, 2016, doi: 10.1093/cybsec/tyw001.

[8]. A. Altamimi, M. Al-Bashayreh, M. Al-Oudat, and D. Almajali, “Blockchain technology adoption for sustainable learning,” Int. J. Data Netw. Sci., vol. 6, no. 3, 2022, doi: 10.5267/j.ijdns.2022.1.013.

[9]. I. Alhassan, D. Sammon, and M. Daly, “Critical success factors for data governance : a telecommunications case study,” J. Decis. Syst., vol. 28, no. 1, pp. 41–61, 2019, doi: 10.1080/12460125.2019.1633226.

[10]. G. Iyawa and A. Gamundani, “Essential Components of an IT Risk Management Framework for the Financial Services Industry: A Review,” in Proceedings of International Conference on Information Systems and Emerging Technologies, 2023, 2023.

[11]. ISACA, COBIT5: A Business Framework for the Governance and Management of Enterprise IT. 2012.

[12]. NIST, Risk Management Framework for Information Systems and Organizations Risk Management Framework for Information Systems and Organizations. 2018.

[13]. T. Tan and B. Soewito, “Implementing the NIST Cybersecurity Framework at ZXC University,” J. Inf. Syst. Applied, Manag. Account. Res., vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

[14]. J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Sixth Edition. SAGE Publications Asia-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug509

Pacific Pte. Ltd., 2023. [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[15]. K. Dan, A. Sheren, R. Sirait, A. S. Kamalia, A. Diska, and M. B. Legowo, "Cyber Attacks Using the NIST Risk Management Framework," Pros. Sn. 2023, pp. 1–8, 2023.

[16]. N. Nilamsari, "Understanding Document Analysis in Qualitative Research," Wacana, vol. XIII, no. 2, pp. 177–181, 2014.

[17]. T. Aven, "Risk assessment and risk management : Review of recent advances on their foundation," Eur. J. Oper. Res., vol. 253, no. 1, pp. 1–13, 2016, doi: 10.1016/j.ejor.2015.12.023.

[18]. M. B. Legowo, R. Desica, N. Rahsa, N. Batrisyia, and S. R. Julia, "Data Breach and Data Leak as a Threat in XYZ Bank : Risk Management Steps," J. Business, Finance. Bank, vol. 2, no. 2, pp. 21–36, 2026.

[19]. M. Sheleme and R. R. Sharma, "Cyber-attack and Measuring its Risk," IRO J. Sustain. Wirel. Syst., vol. 3, no. 4, pp. 219–225, 2021.

[20]. O. G. Khoirunnisa, "Implementasi Algoritma AES untuk Keamanan Data Rekam Medis," PETIR J. Pengkaj. dan Penerapan Tek. Inform., vol. 15, no. 1, pp. 21–27, 2022.

[21]. B. Stojanović and J. Boži´c, "Robust Financial Fraud Alerting System Based in the Cloud Environment," Sensors-MDPI, vol. 22, no. 9461, 2022.