Journal of Business, Finance, and Banking
E-ISSN: 3109-7103
Vol 2 No 2 July 2026
https://journal.perbanas.id/index.php/jbfb

Data Breach and Data Leak as a Threat in XYZ Bank: Risk Management Steps

Mercurius Broto Legowo [a], Rachel Desica Patricia[b], Nabilah Rahsa[c]
Nurraimi Batrisyia[d*], Siti Rosmah Julia[e]
[a,b,c] Faculty of Information Technology, Perbanas Institute, Indonesia
[d,e] Faculty of Islamic Economics and Finance, Universiti Islam Sultan Sharif Ali, Brunei Darrussalam
[*] 23b0809@unissa.bn

Abstract

The rapid digital transformation in the banking sector has significantly increased exposure to cybersecurity threats, particularly data breaches and data leak incidents. These threats may compromise the confidentiality, integrity, and availability of sensitive customer and organizational information, resulting in financial losses, reputational damage, and regulatory sanctions. This study aims to analyse the risks associated with data breaches and data leaks in Banking XYZ and propose appropriate risk management measures using the COBIT 5 framework, specifically the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains. The research employs a qualitative descriptive approach using literature review and risk analysis based on COBIT 5 processes. The findings indicate that both Data Breach and Data Leak are categorized as high-risk threats due to their high likelihood and significant business impact. The APO12 domain facilitates systematic risk identification, assessment, evaluation, and monitoring, while DSS05 supports the implementation of operational security controls. Furthermore, the study highlights that security measures such as Multi-Factor Authentication (MFA), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and continuous security monitoring are essential to mitigate cybersecurity risks. The study concludes that the COBIT 5 framework provides an effective, structured approach to strengthening information security governance and enhancing cyber resilience in the banking industry.

Keywords: *Data Breach, Data Leak, Banking Industry, Risk Management, COBIT 5, Information Security.*

Article History:
Received : 29 June 2026
Revised : 6 July 2026
Accepted : 6 July 2026
DOI : https://doi.org/10.56174/jbfb.v2i2.1345

1. Introduction

The rapid advancement of digital technology has significantly transformed the banking industry, enabling financial institutions to deliver more efficient, accessible, and customer-oriented services through digital platforms such as *mobile banking*, *internet banking*, and cloud-based services. While digital transformation offers substantial benefits, it also increases banks' exposure to cybersecurity threats, particularly data breaches and data leaks. The growing dependence on information technology, interconnected systems, and third-party services has expanded the attack surface and created new vulnerabilities that cybercriminals can exploit (Aldasoro, I. et al., 2022). Data leakage is a significant issue for an organization's reputation and finances. The alternative name for a data breach is data spill, data leakage, or Information leakage (Bargavi et al., 2022). Indonesia ranks eighth globally in the number of data breach cases, reflecting systemic vulnerabilities in national cybersecurity governance (Fadliansyah et al., 2025). The 2024 data breach incident at Indonesia's National Data Center (PDN) marked a major crisis in the governance of national cybersecurity (Bua & Idris, 2025). In response, the government enacted the Personal Data Protection (PDP) Law No. 27 of 2022, which serves as the first comprehensive legal framework in this field. However, its implementation has been hindered by delays in issuing implementing regulations, a lack of human resource capacity, and low cybersecurity awareness.

Data Breach refers to unauthorized access, disclosure, or theft of confidential information, whereas Data Leak denotes the accidental or intentional exposure of sensitive information to unauthorized parties. Both incidents may lead to severe consequences, including financial losses, reputational damage, regulatory sanctions, and erosion of customer trust (Romanosky et al., 2016). In the banking sector, where customer trust is a fundamental asset, maintaining the confidentiality, integrity, and availability of information has become a strategic necessity rather than merely a technical requirement (Kamiya et al., 2018).

In Indonesia, cybersecurity incidents have become increasingly prevalent in recent years. One of the most prominent cases was the ransomware attack on Bank Syariah Indonesia (BSI) in 2023, which disrupted banking operations and reportedly exposed customer data. Furthermore, cyberattacks targeting Indonesia's National Data Center in 2024 highlighted the country's ongoing cybersecurity challenges and demonstrated the potential impact of data breaches on critical infrastructures and financial institutions. These incidents indicate that Indonesian organizations, including banks, remain vulnerable to cyber threats and require stronger information security governance and risk management practices (Kholis, 2024).

The increasing cyber threats have encouraged the Indonesian government and regulators to strengthen cybersecurity regulations in the banking sector. The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) establishes legal obligations for organizations to protect personal data and report data breach incidents. In addition, the Financial Services Authority (OJK) issued Regulation No. 11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks, which requires banks to implement information technology governance, risk management, cybersecurity, and cyber resilience mechanisms. OJK further issued Circular Letter No. 29/SEOJK.03/2022 on Cyber Security and Resilience for Commercial Banks to provide detailed guidelines on cybersecurity implementation and resilience assessment within banking institutions.

A bank that experiences data breaches and data leaks will face serious consequences across operational, financial, legal, and reputational aspects. Bank XYZ is a leading bank in Indonesia; however, it has experienced a large-scale data breach. Bank XYZ needs stronger IT risk management practices. Risk management has consistently been a core function in banking, with a primary focus on addressing profitability challenges (Iyawa & Gamundani, 2023). COBIT 5 was selected because it offers a structured approach to IT risk management—specifically for mitigating threats of data breaches and leaks—through effective IT governance, information security controls, and continuous risk monitoring. Cybersecurity governance and risk management frameworks provide a structured approach to strengthening organizational resilience and reducing exposure to cyber threats(Mohammed et al., 2025).

Among the COBIT 5 domains, APO12 (Manage Risk) and DSS05 (Manage Security Services) are particularly relevant for addressing Data Breach and Data Leak risks. APO12 supports organizations in identifying, analyzing, evaluating, and monitoring IT-related risks, while DSS05 focuses on implementing and maintaining operational security controls to protect information assets (ISACA, 2012). Therefore, these domains provide a structured and comprehensive approach to strengthening information security governance in banking institutions.

Based on the aforementioned issues, this study aims to analyze the risks of data breaches and data leaks in Banking XYZ and propose appropriate risk management measures using the COBIT 5 framework, specifically through the APO12 and DSS05 domains. The findings are expected to contribute both theoretically and practically to improving cybersecurity governance and enhancing cyber resilience in the Indonesian banking sector.

2. Literature Review

Data Breach and Data Leaks

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 (Gowda & Gowda, 2021; Algamar et al., 2024) . 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 (Romanosky et al., 2016). 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 (Ahmad et al., 2022). Both incidents may result in the unauthorized disclosure of personal, financial, and organizational data, causing significant operational and reputational consequences for organizations (Kamiya et al., 2018).

According to Romanosky et al.(2016), 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 (2018) 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.

Data leaks involve the unintended or unauthorized dissemination of confidential or sensitive information outside the boundaries of an organization (Sachenko et al.,2025). Several studies identify human factors as one of the primary causes of data leaks and cybersecurity incidents. Parsons et al. (2017) state that employee negligence, lack of cybersecurity awareness, and improper handling of sensitive information significantly contribute to data exposure incidents within organizations. Internal threats become increasingly dangerous when organizations lack effective identity management systems, access control policies, and employee cybersecurity training. Furthermore, weak governance structures and inadequate monitoring systems may increase the probability of unauthorized data access and information leakage.

From a governance perspective, effective cybersecurity management requires integrated risk management frameworks and proactive information security strategies. COBIT 5 provides a comprehensive governance and management framework that supports organizations in aligning information technology objectives with business goals while mitigating cybersecurity risks. The APO12 (Manage Risk) domain within COBIT 5 focuses on the systematic identification, assessment, and mitigation of risk. In contrast, the DSS05 (Manage Security Services) domain emphasizes information protection, access control, incident management, and continuous security monitoring. According to ISACA, (2012) organizations implementing strong IT governance frameworks such as COBIT demonstrate improved capability in managing cybersecurity risks and maintaining information integrity.

In addition, modern cybersecurity strategies increasingly emphasize the importance of encryption technologies, multi-factor authentication, zero-trust architecture, and Data Loss Prevention (DLP) systems to minimize the risk of data breaches and data leaks (Mohammed et al., 2025). These approaches support proactive risk management by strengthening organizational resilience against cyberattacks and internal vulnerabilities. Therefore, effective cybersecurity governance in the banking sector requires not only advanced technological solutions but also organizational commitment, employee awareness, and continuous monitoring to ensure data protection and public trust in digital financial services.

IT Risk Management in Banking

Risk management has consistently been a core function in banking, with a primary focus on addressing profitability challenges (Iyawa & Gamundani, 2023). IT Risk Management is the application of risk management methods to information technology to manage risks that may arise in Information Technology (IT). Risk Management has become essential in the banking sector due to the increasing reliance on digital systems, online transactions, cloud computing, and interconnected financial technologies. Although digital transformation improves operational efficiency and service quality, it also increases cybersecurity risks such as data breaches, fraud, malware attacks, ransomware, and unauthorized access to sensitive financial information. According to ISACA (2012), IT risk management refers to the process of identifying, assessing, controlling, and monitoring risks related to the use of information technology within organizations. In the banking sector, IT risk management aims to minimize the potential impact of cyber threats and ensure that information systems align with organizational objectives and regulatory requirements. Banks must continuously evaluate vulnerabilities within their technological infrastructure to prevent disruptions that may affect financial stability and organizational reputation. Effective IT risk management also supports regulatory compliance, particularly regarding data protection, financial transparency, and information security governance.

Several studies emphasize that cybersecurity governance and risk management frameworks are essential for strengthening organizational resilience against cyber threats(Mohammed et al., 2025). ISACA (2012). explains that organizations implementing structured IT governance frameworks demonstrate better decision-making capabilities, stronger internal controls, and improved risk mitigation performance. One of the most widely adopted frameworks is COBIT 5 (Control Objectives for Information and Related Technologies), developed by ISACA, which provides comprehensive guidance for IT governance, risk management, and information security practices. COBIT 5 integrates business objectives with information technology governance to ensure effective risk optimization, resource management, and value creation.

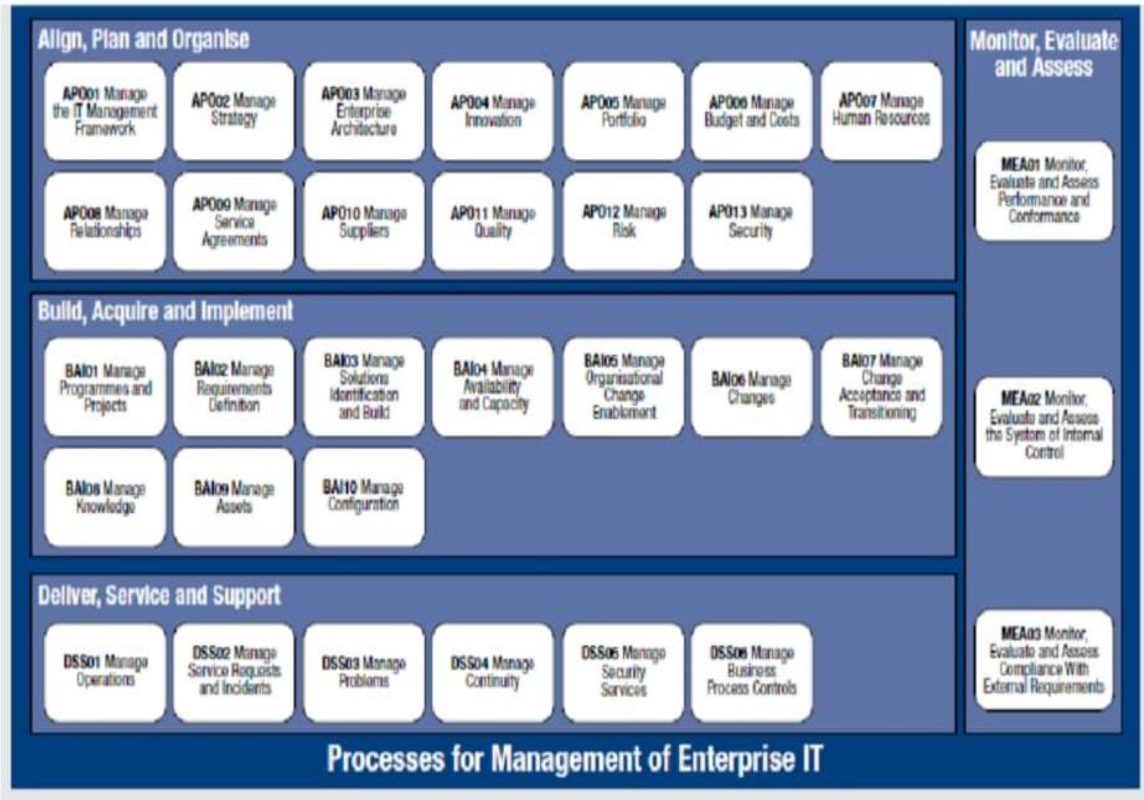
Modern IT risk management approaches in the banking industry emphasize the implementation of sophisticated cybersecurity solutions, such as encryption technologies, multi-factor authentication, AI-based monitoring systems, Data Loss Prevention (DLP), and zero-trust security frameworks (Wiiliam, 2023). In addition, employee cybersecurity awareness training and incident response planning play important roles in reducing internal vulnerabilities and human-related security risks. Effective IT risk management, therefore, requires a combination of technological capability, organizational governance, regulatory compliance, and continuous risk evaluation to maintain secure and sustainable digital banking operations.

COBIT 5 Framework

Several studies emphasize that cybersecurity governance and risk management frameworks are essential for strengthening organizational resilience against cyber threats. De Haes and Van Grembergen (2009) explain that organizations implementing structured IT governance frameworks demonstrate better decision-making capabilities, stronger internal controls, and improved risk mitigation performance. One of the most widely adopted frameworks is COBIT 5 (Control Objectives for Information and Related Technologies), developed by ISACA, which provides comprehensive guidance for IT governance, risk management, and information security practices (ISACA, 2012). COBIT 5 integrates business objectives with information technology governance to ensure effective risk optimization, resource management, and value creation.

Within the COBIT 5 framework, the APO12 (Manage Risk) domain focuses on identifying and assessing IT-related risks systematically, while the DSS05 (Manage Security Services) domain emphasizes the implementation of security controls, access management, incident response, and continuous monitoring systems. These domains are highly relevant to banking institutions because they support proactive cybersecurity management and reduce exposure to cyber threats. Research conducted by Tuttle and Vandervelde (2014) indicates that the implementation of COBIT-based governance frameworks enhances information security effectiveness and strengthens operational control when compared to organizations lacking integrated governance mechanisms.

Journal of Business, Finance, and Banking
E-ISSN: 3109-7103
Vol 2 No 2 July 2026
https://journal.perbanas.id/index.php/jbfb



Source: (ISACA, 2012)

Figure 1. COBIT 5 Framework

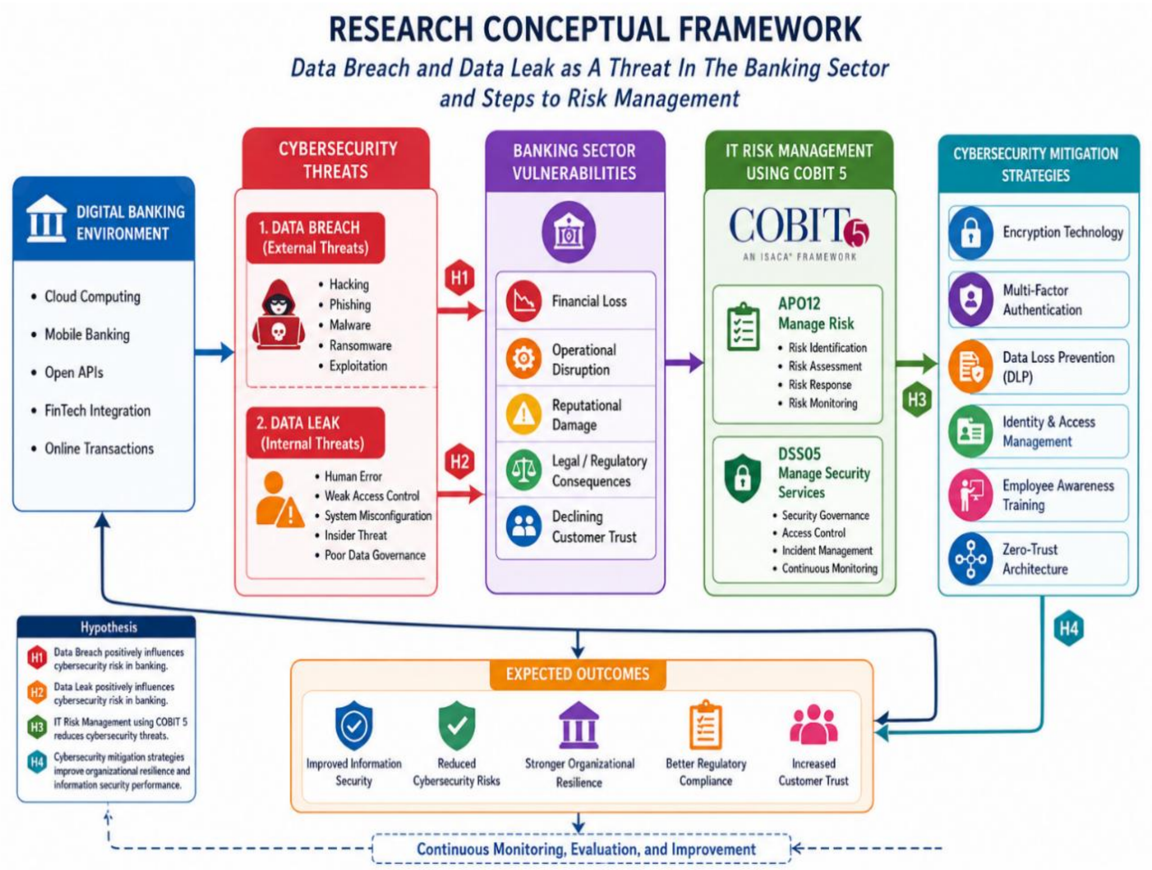
The COBIT 5 framework comprises five domains and includes 37 sub-domains (Handayani & Christioko, 2023) :

1) EDM (Evaluate, Direct, and Monitor),
2) APO (Align, Plan, and Organise),
3) BAI (Build, Acquire, and Implement),
4) DSS (Deliver, Service, and Support), and
5) MEA (Monitor, Evaluate, and Assess),

Research Conceptual Framework

Figure 1 illustrates a *Research Conceptual Framework* regarding the threats of Data Breach and Data Leak in the banking sector and the implementation of risk management strategies using the COBIT 5 framework. The framework shows that the rapid growth of digital banking environments, such as *cloud computing*, *mobile banking*, *open APIs*, and *FinTech integration*, increases cybersecurity threats. These threats are categorized into two main types: Data Breach, which involves external attacks such as hacking, phishing, malware, and ransomware, and Data Leak, which results from internal factors such as human error, weak access control, and system misconfiguration. Both threats can lead to financial losses, operational disruptions, reputational damage, legal consequences, and declining customer trust.

Journal of Business, Finance, and Banking
E-ISSN: 3109-7103
Vol 2 No 2 July 2026
https://journal.perbanas.id/index.php/jbfb



Source: Generated by ChatGPT

Figure 2. The Research Conceptual Framework

To reduce these risks, the framework positions IT Risk Management using COBIT 5 as the primary control mechanism, particularly through the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains. Furthermore, the study proposes several cybersecurity mitigation strategies, including encryption technology, multi-factor authentication, Data Loss Prevention (DLP), identity management, cybersecurity awareness training, and zero-trust architecture. The implementation of these strategies is expected to improve information security, reduce cybersecurity risks, strengthen organizational resilience, enhance regulatory compliance, and maintain customer trust in digital banking services.

3. Research Methods

This study employs a qualitative descriptive research approach to analyze data breaches and data leaks as cybersecurity threats in the banking sector and to examine risk management strategies using the COBIT 5 framework. The qualitative approach is considered appropriate because the study focuses on understanding cybersecurity phenomena, governance practices, risk management processes, and organizational responses to security incidents within banking institutions. The research emphasizes the exploration of operational case studies, cybersecurity governance practices, and information security management related to banking environments.

Journal of Business, Finance, and Banking
E-ISSN: 3109-7103
Vol 2 No 2 July 2026
https://journal.perbanas.id/index.php/jbfb

Data Collection

The data collection process in this study uses secondary data obtained from various reliable and accessible sources. These sources include academic journal articles, conference proceedings, cybersecurity reports, banking industry publications, regulatory documents, and official reports related to cybersecurity incidents in the financial sector. The study also reviews previous research discussing data breaches, data leaks, IT risk management, and COBIT 5 implementation in banking organizations.

In addition, several cybersecurity incident case studies from the banking and financial sectors are analyzed to identify common causes, impacts, and mitigation strategies related to data security incidents. The collected data focus on cybersecurity threats, governance weaknesses, risk management implementation, access control mechanisms, identity management systems, and incident response practices. Relevant COBIT 5 domains, particularly APO12 (Manage Risk) and DSS05 (Manage Security Services), are used as analytical references to evaluate organizational cybersecurity governance and risk management effectiveness

Data Analysis

The data analysis process uses a qualitative descriptive analysis technique combined with a literature review approach. The collected information is systematically categorized based on the main research themes, including data breaches, data leaks, cybersecurity threats, banking sector vulnerabilities, and IT risk management practices. The analysis aims to identify relationships between cybersecurity threats and organizational governance weaknesses in digital banking environments. Data analysis was conducted by the researcher, assisted by banking practitioners with expertise in IT risk management.

Furthermore, the study applies the COBIT 5 framework as an analytical tool to evaluate risk management and information security governance practices within banking institutions. The APO12 domain is used to analyze how organizations identify, assess, and manage cybersecurity risks, while the DSS05 domain is used to examine the implementation of security controls, access management, incident handling, and continuous monitoring systems. The findings from the analysis are then interpreted to identify critical governance gaps, organizational vulnerabilities, and effective cybersecurity mitigation strategies.

The final stage of analysis involves concluding the role of COBIT 5-based IT risk management in reducing the impact of data breaches and data leaks in the banking sector. The study also formulates recommendations for improving cybersecurity governance, strengthening information security controls, and enhancing organizational resilience against cyber threats in digital banking systems.

4. Results and Discussion

In the study titled "Data Breaches and Data Leaks as Threats at Bank XYZ: Steps to Risk Management," the findings emphasize risk management measures. The primary contribution of this research is the development of a COBIT 5-based risk management model—or a series of risk management stages—specifically focusing on the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains. These stages include:

1) **Risk Identification** – Identifying threats, vulnerabilities, and critical assets.

2) **Risk Analysis** – Analyzing the likelihood and impact of risks.
3) **Risk Evaluation** – Determining risk priorities based on risk appetite.
4) **Risk Treatment** – Determining mitigation strategies, such as the implementation of MFA, DLP, SIEM, and data encryption.
5) **Risk Monitoring** – Monitoring the effectiveness of security controls and changes in the risk profile.
6) **Risk Communication** – Communicating risk status to management and stakeholders.
.

Risk Identification Result

Data Breach Risk refers to the possibility of unauthorized access, disclosure, theft, alteration, or destruction of sensitive information stored, processed, or transmitted by banking information systems, resulting in financial losses, regulatory sanctions, reputational damage, and disruption of business operations.

Then, **Data Leaks** are risks arising from the unauthorized or accidental disclosure of sensitive banking information, including customer data, financial records, and internal organizational information, through human error, insider misuse, cyberattacks, system vulnerabilities, or inadequate data protection mechanisms. Such incidents may lead to loss of customer trust, legal consequences, and operational disruptions. Table 1 shows the identification and assessment of data breach risks.

Table 1. Risk Identification and Assessment for Data Breach

Risk ID	Risk Identification	Likelihood	Impact	Risk Score (L × I)	Risk Level
R1	**Data Breach**	4	5	20	High
R1.1	Unauthorized Access	4	5	20	High
R1.2	Credential Theft	4	4	16	High
R1.3	Malware/Ransomware Attack	4	5	20	High

Source: Research Result (2026)

Risk Identification and Assessment:

There is a high likelihood of data breaches due to the rising number of cyberattacks targeting the banking sector and organizations that handle sensitive data. The impact is severe, as it can result in financial losses, regulatory sanctions, and reputational damage to the organization. Table 2 shows the identification and assessment of data leak risks.

Table 2 Risk Identification and Assessment for Data Leaks

Risk ID	Risk Identification	Likelihood	Impact	Risk Score (L × I)	Risk Level
R2	**Data Leaks**	4	4	16	High
R2.1	Human Error	4	4	16	High
R2.2	Insider Threat	3	5	15	High
R2.3	Cloud Misconfiguration	4	4	16	High

Source: Research Result (2026)

Risk Identification and Assessment:

Data leakage risks are often caused by internal factors, such as user error, weak access rights management, and system misconfiguration. These risks can result in the loss of information confidentiality and violations of data protection regulations.

Risk Analysis Result

Table 2 presents the analysis of identified risks mapped to relevant COBIT 5 domains and sub-domains. Six COBIT 5 processes were identified as most critical for addressing malware and ransomware risks in the banking context.

Table 3. Risk Analysis Using COBIT 5 Framework

Risk	Domain COBIT 5	Likelihood	Impact	Risk Level	Priorities
Data Breach	APO12, DSS05	4	5	High	Very High
Data Leakage	APO12, DSS05	4	4	High	High

Source: Research Result (2026)

Based on an analysis using COBIT 5, both data breach and data leakage risks fall into the High Risk category. The APO12 domain plays a role in identifying, analyzing, and maintaining risk profiles, while the DSS05 domain functions to evaluate the effectiveness of operational security controls required to reduce the likelihood of information security incidents.

Risk Evaluation Result

The objective of risk evaluation is to determine risk treatment priorities and decide on appropriate risk responses. For data breach and data leakage risks, the risk evaluation process is conducted through the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains. Based on an evaluation using COBIT 5, both data breach and data leakage risks fall into the "High Risk" category and exceed the organization's risk appetite. Through the APO12 domain, the organization can evaluate its risk profile, tolerance levels, and risk response priorities.

Table 4 Risk Evaluation Result

Risiko	Inherent Risk	Existing Controls	Residual Risk	Status Evaluasi	Prioritas
Data Breach	High	Not Yet Optimal	High	Not acceptable	Very High
Data Leakage	High	Not Yet Optimal	High	Not acceptable	High

Source: Research Result (2026)

Meanwhile, the DSS05 domain is used to assess the effectiveness of existing security controls. The evaluation results indicate gaps in the implemented security controls, necessitating enhancements such as the implementation of Multi-Factor Authentication (MFA), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and real-time security monitoring to reduce residual risk levels.

Risk Treatment;

Journal of Business, Finance, and Banking
E-ISSN: 3109-7103
Vol 2 No 2 July 2026
https://journal.perbanas.id/index.php/jbfb

Within the COBIT 5 framework, risk treatment for data breaches and data leakage can be addressed through a combination of the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains. APO12 focuses on risk identification, analysis, and response, whereas DSS05 focuses on the implementation of operational security controls.

Table 5 Risk Treatment Result

COBIT 5 Domain	Process	Risk Treatment	Implementation
APO12.01	Collect Data	Identification of critical data assets and data leakage threats	Inventarisasi data nasabah, klasifikasi data sensitif
APO12.03	Maintain Risk Profile	Assessing the likelihood and impact of a data breach	Risk register dan risk matrix
APO12.05	Define Risk Action Portfolio	Determining mitigation strategies	Risk avoidance, mitigation, transfer, acceptance
DSS05.02	Manage Network and Connectivity Security	Preventing unauthorized access	Firewall, IDS/IPS, Zero Trust Architecture
DSS05.03	Manage Endpoint Security	Securing user devices	Antivirus, EDR, and patch management
DSS05.04	Manage User Identity and Logical Access	Access control	Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC)
DSS05.05	Manage Physical Access	Physical security	CCTV, biometric access, secure server room
DSS05.07	Monitor Security Events	Early detection of incidents	SIEM, Security Operations Center (SOC)
DSS05.06	Manage Sensitive Documents and Output Devices	Protection of sensitive documents	Database and File Encryption

Source: Research Result (2026)

Thus, APO12 serves as a risk governance mechanism to identify, evaluate, and determine responses to data breach and data leakage risks, while DSS05 provides the operational security controls necessary to mitigate the probability and impact of such risks. This approach enables organizations—particularly in the banking sector—to enhance information security resilience and minimize disruptions to business operations.

Risk Monitoring

Within the COBIT 5 framework, Risk Monitoring is the process of continuously monitoring risk levels, control effectiveness, and changes in the threat landscape to ensure that risks remain within the organization's risk appetite. For data breach and data leakage risks, monitoring activities are primarily conducted through the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains.

Table 6 Risk Monitoring Data Breach and Data Leaks

Risiko	Domain COBIT 5	Mekanisme Monitoring	Frekuensi
Data Breach	APO12.03	Review risk register	Quarterly
Data Breach	DSS05.07	Monitoring security log via SIEM	Real-time
Data Breach	DSS05.04	Review user access rights	Monthly
Data Leakage	DSS05.06	Monitoring DLP alerts	Real-time
Data Leakage	DSS05.04	Sensitive data access audit	Monthly
Data Leakage	APO12.06	Evaluation of mitigation effectiveness	Quarterly

Source: Research Result (2026)

Thus, within COBIT 5, APO12 plays a role in monitoring risk profiles, risk levels, and the effectiveness of risk responses, while DSS05 focuses on monitoring security operations through technical mechanisms such as SIEM, DLP, IDS/IPS, IAM, and SOC. Integrating these two domains enables organizations to detect potential data breaches and data leakage early, while ensuring that risks remain within established tolerance limits.

Risk Communication

Within the COBIT 5 framework, risk communication is the process of conveying risk-related information to all stakeholders to ensure that risks are understood, monitored, and effectively managed. Risk communication is crucial for raising information security awareness, supporting decision-making, and ensuring a rapid response to security incidents. The results of the risk communication matrix are tabulated in Table 7.

Tabel 7. Risk Communication Matrix

Risiko	Informasi yang Dikomunikasikan	Stakeholder	Frekuensi	Media Komunikasi
Data Breach	Security incident status	CISO, Direksi	Real-time	SIEM Dashboard
Data Breach	Risk Profile	Risk Committee	Monthly	Risk Report
Data Breach	Security audit results	Management	Quarterly	Audit Report
Data Leakage	DLP Violation	SOC Team	Real-time	Alert System

Journal of Business, Finance, and Banking
E-ISSN: 3109-7103
Vol 2 No 2 July 2026
https://journal.perbanas.id/index.php/jbfb

Data Leakage	Mitigation Status	Management	Monthly	Dashboard
Data Leakage	Security control evaluation	Risk Committee	Quarterly	Security Report

Source: Research Result (2026)

In COBIT 5, APO12 plays a role in communicating risk profiles, risk levels, and response strategies to management and stakeholders. Meanwhile, DSS05 focuses on operational communication regarding security events, incidents, and information security breaches. Integrating these two domains enables organizations to ensure that risks related to data breaches and data leakage are communicated in a timely, accurate, and effective manner, thereby supporting decision-making and enhancing the organization's information security resilience.

Discussion

This study demonstrates that data breaches and leaks pose a serious threat to Bank XYZ. Digital transformation in the banking sector—including the use of mobile and internet banking services and integration with third parties—has expanded the attack surface and increased vulnerability to cyber threats.(Aldasoro et al., 2022). The analysis results indicate that both risks fall into the "High Risk" category, thereby requiring ongoing attention and mitigation.

Data Breach as a Critical Threat

Research findings indicate that the risk of data breaches stems primarily from cyberattacks such as phishing, malware, ransomware, and the exploitation of system vulnerabilities. Furthermore, weak access controls and delayed system updates increase the likelihood of data breaches. The resulting impact extends beyond financial loss to include a decline in reputation and trust. (Romanosky, 2016; Kamiya et al., 2021).

Data Leak and Internal Security Challenges

Research also indicates that data breaches have increased significantly, posing substantial financial, operational, and reputational risks to the banking sector. This demonstrates that information security relies not only on technology but also on human factors and organizational processes. Therefore, raising security awareness, implementing the principle of least privilege, and periodically evaluating access rights are crucial measures. (Parsons et al., 2014).

Risk Management Using COBIT 5

The implementation of the COBIT 5 framework—specifically the APO12 and DSS05 domains—has proven capable of supporting systematic risk management. The APO12 domain assists organizations in identifying, analyzing, and evaluating risks, while DSS05 supports the implementation of operational security controls, such as MFA, SIEM, DLP, and real-time security monitoring. (ISACA, 2012). Implementing these controls can reduce the likelihood and impact of data breaches and data leak risks.

Managerial Implications

Research findings confirm that information security risk must be viewed as a strategic risk rather than merely a technical issue. Therefore, management needs to strengthen information security governance by enhancing access controls, conducting periodic security audits, and fostering an information security culture to improve the organization's cyber resilience.

5. Conclusion and Recommendation

Conclusion

This study reveals that data breaches and leaks pose a major threat to Bank XYZ in the era of digital transformation. Risk analysis results indicate that both risks fall into the "High Risk" category, given their high likelihood of occurrence and significant impact on data confidentiality, organizational reputation, regulatory compliance, and business operational continuity.

The implementation of the COBIT 5 framework—specifically the APO12 (Manage Risk) and DSS05 (Manage Security Services) domains—has proven capable of supporting the systematic management of information security risks.

The APO12 domain plays a role in the processes of risk identification, analysis, evaluation, and monitoring, while DSS05 supports the implementation of operational security controls. Implementing controls such as Multi-Factor Authentication (MFA), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and real-time security monitoring can help reduce the likelihood of data breaches and data leaks, as well as enhance the organization's cyber resilience.

Recomendatuion

Based on the research findings, Bank XYZ needs to strengthen its information security governance by implementing stricter access controls—such as Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC)—and by optimizing security technologies like Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and a Security Operations Center (SOC) to enhance real-time incident detection and response.

Furthermore, security audits and information security awareness training should be conducted periodically to ensure the effectiveness of controls and mitigate risks associated with human factors. Future research is advised to integrate COBIT 5 with other frameworks, such as ISO/IEC 27001 or the NIST Cybersecurity RMF.

References

Ahmad, A., Maynard, S. B., & Park, S. (2022). Information Security Strategies : Towards an Organizational Multi-Strategy Perspective. *Journal of Intelligent Manufacturing*, *33*(2), 1–20.

Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2022). Cyber risk, market failures, and financial stability. *Journal of Financial Stability*, *58*.

Algamar, M. D., Munir, A. B., & Hendro, H. (2024). Managing Indonesian Data Breach Notification In The Financial Services Sector: A Case For A One-Stop Notification Model. *Journal of Central Banking Law and Institution*, *3*(3), 547–584.

Bargavi, M., Senbagavalli, M., Tejashwini, K. R., & Tejashvar, K. R. (2022). Data Breach – Its Effects on Industry. *International Journal of Data Informatics and Intelligent Computing (IJDIIC)*, *1*(2), 51–57. https://doi.org/10.59461/ijdiic.v1i2.31

Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia : Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *2*(2), 100–114.

Fadliansyah, F., Mubarok, M. K., Aziz, M. D., & Elfina, A. (2025). Evaluasi pembelajaran dari kasus kebocoran data di Indonesia sebagai negara dengan data breach terbesar ke-8 di dunia. *TEKNOBIS : Teknologi, Bisnis dan Pendidikan*, *3*(2), 272–277.

Gowda, P., & Gowda, A. N. (2021). Data Breach as a Threat in the Banking Sector and Steps to Avoid It. *International Journal of Science and Research (IJSR*, *10*(4), 2019–2022.

Handayani, T., & Christioko, B. V. (2023). Audit Sistem Informasi menggunakan Framework Cobit 5 pada LPPM Universitas Semarang. *IJCIT (Indonesian Journal on Computer and Information Technology)*, *8*(1), 49–54.

ISACA. (2012). *COBIT5: A Business Framework for the Governance and Management of Enterprise IT*.

Iyawa, G., & Gamundani, A. (2023). Essential Components of an IT Risk Management Framework for the Financial Services Industry : A Review. *Proceedings of International Conference on Information Systems and Emerging Technologies, 2023*, *2018*.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What Is The Impact Of Successful Cyberattacks On Target Firms? *NATIONAL BUREAU OF ECONOMIC RESEARCH*, *02*.

Kholis, I. M. (2024). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan : Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *STAATSRECHT Jurnal Hukum Kenegaraan dan Politik Islam*, *4*(2).

Mohammed, S., Kamal, S., & Mostafa, S. (2025). Cybersecurity Governance and Risk Management Frameworks. *Computer Science and Engineering*, *5*(1). https://doi.org/DOI:10.5281/zenodo.20066402

Parsons, K., McCormack, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). ScienceDirect Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Romanosky, S., Corporation, R., & St, S. H. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity,* *2*(August), 121–135. https://doi.org/10.1093/cybsec/tyw001

William, E. (2023). Zero Trust Architecture in Banking : A New Paradigm for Cybersecurity Protection. *Computer Security and Reliability*, *2*(4), 1–4.