Perbanas International Conference on Economics, Business, Management, Accounting and IT (PROFICIENT) 2026
"Integrity-Driven Innovation: Reimagining Business, Finance, and Digital Transformation for Sustainable Impact"

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

Information Technology Risk Management For Malware And Ransomware Attacks In Banking Using Cobit 5 Framework

Nur Akhmad Van Jouvi[1,a)], Fathur Rahman[2,b)], Mercurius Broto Legowo[3,c)]

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

[a)]Corresponding author: nur.akhmad24@perbanas.id
[b)]fathur.rahman27@perbanas.id
[c)]mercurius@perbanas.id

Abstract. *The rise of malware and ransomware attacks targeting the banking sector has emerged as a critical threat to financial data integrity and service continuity. Indonesian banking institutions, including Bank Rakyat Indonesia (BRI) and Bank Syariah Indonesia (BSI), have experienced significant cyber incidents in recent years, highlighting the urgent need for a structured IT risk management approach. This study aims to analyze malware and ransomware risks in the Indonesian banking sector using the COBIT 5 framework as the primary governance reference. A qualitative case study method was employed, examining real-world incidents and mapping identified risks against relevant COBIT 5 domains, including EDM03, APO12, APO13, BAI06, DSS05, and DSS04. The analysis identifies four key risk categories: malware infection, ransomware attacks, malware-induced data breaches, and insider threats. Each risk is assessed based on probability and impact levels, followed by mitigation strategies and Key Risk Indicators (KRIs) with measurable thresholds. The findings demonstrate that COBIT 5 provides a comprehensive and structured governance approach to address escalating cyber threats in the banking sector. This study contributes practical risk management guidance aligned with Indonesian financial regulatory requirements under OJK supervision.*

Keywords: *malware, IT risk management, COBIT 5, Indonesian banking, cybersecurity governance*

INTRODUCTION

The increasing sophistication of cyber threats poses unprecedented challenges to the global banking sector. Among the most destructive threat categories are malware and ransomware, which are malicious software designed to infiltrate, disrupt, and extort financial institutions. The International Monetary Fund (IMF, 2024) reported that financial institutions account for nearly 20% of all ransomware victims globally, with the banking subsector as the primary target. In Indonesia, the threat has materialized into significant real-world incidents. Bank Rakyat Indonesia (BRI) suffered a ransomware attack in December 2024 attributed to the Bashe group, resulting in data exfiltration and operational disruption. Bank Syariah Indonesia (BSI) experienced a ransomware attack in May 2023 that rendered ATM networks and mobile banking inaccessible for several days, affecting millions of customers (Pratama & Rahayu, 2023).Despite the severity of these incidents, systematic IT risk management frameworks specifically addressing malware and ransomware in the Indonesian banking context remain underdeveloped. Existing studies have largely

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

focused on general cybersecurity frameworks without providing operationally actionable guidance tailored to the banking sector's regulatory environment (Rhoades, 2020; Susanto & Almunawar, 2018).

The Control Objectives for Information and Related Technologies (COBIT 5), developed by ISACA (2012), provides a comprehensive governance and management framework for enterprise IT widely adopted in the financial sector. Its process-oriented domains , namely EDM, APO, BAI, and DSS, offer a structured basis for identifying, analysing, and mitigating cyber risks including malware and ransomware (De Haes et al., 2020).

This study addresses the gap by applying COBIT 5 to systematically manage malware and ransomware risks in Indonesian banking, using the BRI and BSI incidents as primary case studies. The research aims to: (1) identify and assess malware and ransomware risk categories; (2) analyse risks using relevant COBIT 5 domains; and (3) evaluate and propose mitigation strategies with measurable Key Risk Indicators (KRIs) aligned with OJK regulatory requirements.

LITERATURE REVIEW

Malware and Ransomware in the Banking Sector

Malware encompasses any software intentionally designed to cause disruption, damage, or unauthorized access to computer systems (Stamp, 2022). In the banking context, malware manifests as Trojans targeting financial credentials, spyware monitoring transaction activities, and memory-scraping tools extracting payment card data (Rieck et al., 2011).

Ransomware is a destructive malware subset that encrypts victim data and demands payment for decryption keys (Richardson & North, 2017). Modern ransomware groups employ double-extortion tactics ,where attackers simultaneously encrypt data and threaten public disclosure, significantly amplifying reputational damage (Connolly et al., 2020). Chainalysis (2024) reported that ransomware payments exceeded $1 billion globally in 2023, with financial services among the top three targeted sectors.

COBIT 5 Framework

COBIT 5, published by ISACA (2012), is a globally recognised framework for IT governance and management covering 37 processes across five domains: EDM, APO, BAI, DSS, and MEA. It integrates with ISO/IEC 27001, ITIL v3, and NIST CSF, making it versatile for banking environments subject to multiple regulatory requirements (De Haes et al., 2020).

Several studies have validated COBIT 5's effectiveness in managing IT risks in financial institutions. Oktarina and Hakim (2022) demonstrated its applicability in assessing IT governance maturity at Indonesian banks. Setiawan et al. (2023) applied COBIT 5 domains to identify cybersecurity control gaps in regional development banks. However, no study has specifically mapped COBIT 5 to malware and ransomware risks with operationally measurable KRIs in Indonesian banking , which is the gap this research addresses.

IT Risk Management Framework

IT risk management involves the systematic identification, assessment, and mitigation of risks affecting information systems and business operations. The ISO 31000:2018 standard defines risk as the 'effect of uncertainty on objectives,' providing a universal risk management process applicable to IT governance frameworks (International Organization for Standardization, 2018). The National Institute of Standards and Technology (NIST, 2012) further provides detailed guidance for conducting risk assessments through SP 800-30.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

In Indonesia, the OJK has issued POJK No. 11/POJK.03/2022 requiring banks to implement comprehensive IT risk management, conduct regular security assessments, and report cyber incidents within 14 business days (Otoritas Jasa Keuangan, 2022). This regulatory context makes COBIT 5 not merely advisable but operationally necessary for Indonesian banks.

METHODS

This study employs a qualitative case study research design, appropriate for examining complex sociotechnical phenomena within real-world contexts (Yin, 2018; Creswell & Creswell, 2018). The primary cases are: (1) the BRI ransomware attack (December 2024) by the Bashe group; and (2) the BSI ransomware incident (May 2023). These cases were selected for their recency, severity, and public documentation.

Data collection involved a systematic review of: (a) publicly available incident reports and cybersecurity advisories; (b) OJK and Bank Indonesia regulatory documents; (c) peer-reviewed journal articles and conference proceedings (2015–2025); and (d) ISACA's COBIT 5 framework documentation. A total of 24 primary and secondary sources were synthesised.

The risk assessment follows a 5×5 probability-impact matrix consistent with ISO 31000:2018 and NIST SP 800-30 guidelines. Risk Level = Probability (P) × Impact (I), producing scores from 1–25, categorised as: Low (1–5), Moderate (6–10), High (11–15), Very High (16–20), and Extreme (21–25). COBIT 5 domain mapping aligned each identified risk to the most relevant process domains based on their control objectives, after which mitigation strategies and KRIs with measurable thresholds were formulated.

RESULTS AND DISCUSSION

Result of IT Risk Identification and Assessment

Based on systematic analysis of the BRI and BSI incidents alongside a review of global malware and ransomware threat patterns, four primary IT risk categories were identified. Table 1 presents the complete risk identification matrix.

TABLE 1. IT Risk Identification and Risk Level Assessment

Code	Risk Type	Risk Description	Prob. (P)	Impact (I)	Risk Level
R-01	**Malware Infection Risk**	Malicious software infection on banking IT infrastructure: - Trojans & spyware stealing customer credentials - Viruses & worms corrupting operational data integrity - Keyloggers recording employee & customer login activities - Rootkits concealing malware from detection systems	**4** (Likely)	**4** (Major)	**16** Very High
R-02	**Ransomware Attack Risk**	Encryption of critical banking data demanding ransom: - Encryption of core banking systems & customer databases - Lateral movement via SMB/RDP network exploitation - Double extortion: encryption combined with data publication threat	**4** (Likely)	**5** (Catastrophic)	**20** Very High ★ Priority 1

		- Real cases: BRI (Dec 2024); BSI (May 2023)			
R-03	**Data Breach via Malware**	Exfiltration of sensitive banking data via malware: - Mass theft of KYC customer data - Exfiltration of card data via memory scrapers - Sale of customer data on dark web - Violation of OJK POJK No. 11/2022	**3** (Possible)	**5** (Catastrophic)	**15** High
R-04	**Insider Threat via Malware**	Internal access misuse facilitating malware spread: - Employees clicking phishing links unknowingly - Malicious insiders installing malware on workstations - IT vendors/contractors abusing privileged access - Weak access controls on sensitive data systems	**3** (Possible)	**4** (Major)	**12** High
Scale: 1–5 Low | 6–10 Moderate | 11–15 High | 16–20 Very High | 21–25 Extreme (Risk Level = P × I)					

Two risks, R-01 (Malware Infection) and R-02 (Ransomware Attack), attain Very High risk levels (scores 16 and 20 respectively). R-03 (Data Breach via Malware) and R-04 (Insider Threat) register at High levels (scores 15 and 12). R-02 receives Priority 1 designation given its Catastrophic impact rating and direct empirical validation through the BRI and BSI incidents.

The probability rating of 4 (Likely) for both R-01 and R-02 is supported by empirical evidence: two major ransomware incidents occurred in Indonesian banking within 18 months (BSI: May 2023; BRI: December 2024). Sophos (2024) reports a 64% increase in ransomware frequency in the financial sector between 2022 and 2024. The Catastrophic impact rating for R-02 reflects the operational reality that ransomware can simultaneously encrypt core banking systems, disrupt customer services, and trigger regulatory sanctions under OJK's cyber incident reporting requirements (Otoritas Jasa Keuangan, 2022).

Result of COBIT 5-Based Risk Analysis

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.

TABLE 2. Risk Analysis Using COBIT 5 Framework

COBIT 5 Domain	Sub-Domain	Related Risk	Risk Analysis
EDM	**EDM03** Ensure Risk Optimisation	R-01 R-02	Senior management has not established explicit cyber risk tolerance policies for malware and ransomware threats. Without a measurable risk appetite statement, IT security investment decisions remain reactive. Periodic monitoring of cybersecurity control effectiveness is absent, allowing incidents such as those at BRI (2024) and BSI (2023) to escalate undetected (ISACA, 2012; Pratama & Rahayu, 2023).
APO	**APO12** Manage Risk	R-01 R-02 R-03 R-04	Banks lack systematic malware/ransomware risk registers updated in real time. Threat intelligence on emerging malware variants is not collected structurally, causing Business Impact Analysis (BIA) to misrepresent actual threat exposure. This results in misaligned risk prioritisation and suboptimal allocation of IT security resources (De Haes et al., 2020; Setiawan et al., 2023).

APO	**APO13** Manage Security	R-01 R-02 R-04	Information Security Management Systems (ISMS) have not been consistently implemented across all business units. Endpoint security policies, patch management, and privileged access controls are unevenly enforced. The absence of structured Security Awareness Training elevates vulnerability to phishing as the primary malware delivery vector (Susanto & Almunawar, 2018; Proofpoint, 2024).
BAI	**BAI06** Manage IT Changes	R-01 R-02	The IT change management process does not mandate security evaluations. Critical patches for banking systems are delayed by bureaucratic approval cycles. Vulnerabilities exploited by ransomware (e.g., EternalBlue/MS17-010) were vendor-patched but not applied institutionally, directly enabling the BSI incident (Verizon, 2024; Pratama & Rahayu, 2023).
DSS	**DSS05** Manage Security Services	R-01 R-02 R-03 R-04	The absence of a 24/7 Security Operations Center (SOC) results in high Mean Time to Detect (MTTD) for malware incidents. Outdated antivirus/EDR solutions cannot detect fileless or polymorphic malware. Backup data is not regularly tested, extending recovery time post-ransomware attack significantly (Sophos, 2024; Rhoades, 2020).
DSS	**DSS04** Manage Continuity	R-02 R-03	Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) do not include ransomware-specific scenarios. Network isolation procedures during active ransomware infection are undefined, slowing first-response coordination. The BSI incident confirmed that the absence of tabletop exercises left teams unable to contain service disruption within acceptable timeframes (Yin, 2018; OJK, 2017).

The COBIT 5 analysis reveals systemic governance gaps across all framework domains. At the strategic level, the absence of explicit cyber risk appetite statements (EDM03) creates a fundamental disconnect between board-level risk tolerance and operational security investments , a pattern consistent with findings by Kouns and Minoli (2010) on IT risk governance maturity in financial institutions.

At the operational level, the most critical gap lies within DSS05 (Manage Security Services), where inadequate endpoint protection, absence of a 24/7 SOC, and unverified backup procedures directly contributed to extended service disruption during the BSI ransomware incident (Pratama & Rahayu, 2023). The BAI06 gap , specifically the failure to apply available patches, represents a recurring pattern globally; Verizon (2024) reports that 85% of successful ransomware attacks exploit known, patchable vulnerabilities.

C. Risk Evaluation, Mitigation, and Key Risk Indicators

Table 3 presents the complete risk evaluation including treatment decisions, specific mitigation strategies, and KRIs with measurable threshold targets for continuous monitoring.

TABLE 3. Risk Evaluation, Mitigation Strategies, and Key Risk Indicators (KRI)

Code	Current Level	TargetResidual	Mitigation Strategy	Key Risk Indicators (KRI)
R-01	**16** Very High	**6** Moderate	1. Deploy next-gen EDR across all endpoints 2. Network Segmentation & Zero Trust Architecture 3. Patch Management: critical patches ≤72hrs, major ≤30 days 4. Email Security Gateway with sandboxing 5. Application Whitelisting on sensitive workstations	KRI-1: Infected endpoints/month → Target: 0 KRI-2: Critical patches applied on time → Target: ≥95% KRI-3: Mean Time to Detect (MTTD) → Target: ≤4 hours KRI-4: Unhandled EDR alerts >24hrs → Target: 0 KRI-5: Endpoints with active EDR → Target: 100%

R-02	**20** Very High ★P1	**4** Low	1. 3-2-1 Backup: 3 copies, 2 media, 1 immutable cloud offsite 2. Strict network segmentation isolating core banking systems 3. Ransomware Response Plan with tabletop every 6 months 4. Disable SMBv1; enforce MFA on all remote access 5. Establish 24/7 SOC with ransomware incident playbook	KRI-1: Ransomware incidents detected/year → Target: 0 KRI-2: Recovery Time Objective (RTO) → Target: ≤4 hours KRI-3: Recovery Point Objective (RPO) → Target: ≤1 hour KRI-4: Systems with verified immutable backup → Target: 100% KRI-5: Network isolation on anomaly detection → Target: ≤15 min
R-03	**15** High	**6** Moderate	1. Data Loss Prevention (DLP) for transfer monitoring 2. Encrypt data-at-rest (AES-256) & in-transit (TLS 1.3) 3. Need-to-Know & Least Privilege policy enforcement 4. Cyber insurance for financial risk transfer 5. Breach Notification procedure per OJK within 14 days	KRI-1: Customer data breach incidents/quarter → Target: 0 KRI-2: Sensitive data encrypted (at-rest & in-transit) → Target: 100% KRI-3: Unauthorized data access violations/month → Target: 0 KRI-4: OJK incident reporting time → Target: ≤14 business days KRI-5: POJK No.11/2022 compliance score → Target: ≥90%
R-04	**12** High	**4** Low	1. Mandatory Security Awareness Training + phishing simulation monthly 2. Privileged Access Management (PAM) for admin accounts 3. User Behavior Analytics (UBA) automated anomaly monitoring 4. Third-party security assessment & NDA for all IT vendors 5. USB/removable media policy: whitelist authorised devices only	KRI-1: Staff passing Security Awareness Training/quarter → Target: ≥95% KRI-2: Staff failing phishing simulation → Target: <5% KRI-3: Privileged access misuse incidents/month → Target: 0 KRI-4: Vendors with current security assessment → Target: 100% KRI-5: Unhandled UBA alerts >8hrs → Target: 0
Decision: REDUCE for all risks. REDUCE and TRANSFER (cyber insurance) for R-03. Priority: R-02 (score 20) → R-01 (score 16) → R-03 (score 15) → R-04 (score 12).				

The evaluation adopts a REDUCE strategy for all four risks, supplemented by a TRANSFER component (cyber insurance) for R-03. This treatment selection reflects severity levels identified in the assessment phase and aligns with the ISO 31000:2018 risk treatment hierarchy (International Organization for Standardization, 2018).

The KRI thresholds for R-02 , specifically Recovery Time Objective (RTO) of ≤4 hours and Recovery Point Objective (RPO) of ≤1 hour, are benchmarked against OJK's business continuity guidelines for systemically important banks (Otoritas Jasa Keuangan, 2017). The BSI incident demonstrated that without pre-tested recovery plans, actual recovery time can exceed 72 hours , representing an 18-fold deviation from the target KRI (Pratama & Rahayu, 2023).

The Security Awareness Training KRI target of <5% phishing simulation failure rate aligns with Proofpoint (2024), which identifies human error as the entry point for 74% of malware incidents in the financial sector. Combined with PAM and UBA controls, this creates a comprehensive defence-in-depth approach addressing both technical and human attack vectors.

Proceedings of the Perbanas International Seminar on Economics, Business, Management, Accounting and IT
[June 2026] [ISSN 3047-0951]

CONCLUSIONS

This study demonstrated the applicability of COBIT 5 in systematically managing malware and ransomware risks in the Indonesian banking sector. Through a qualitative case study examining the BRI (2024) and BSI (2023) incidents, four primary IT risk categories were identified: Malware Infection Risk (Very High, score 16), Ransomware Attack Risk (Very High, score 20), Data Breach via Malware (High, score 15), and Insider Threat via Malware (High, score 12).

The COBIT 5 domain analysis across EDM03, APO12, APO13, BAI06, DSS05, and DSS04 revealed systemic governance gaps including absent cyber risk appetite statements, delayed patch management, lack of 24/7 SOC capabilities, and insufficient ransomware-specific continuity planning. These gaps directly contributed to the severity of recent banking cyber incidents in Indonesia.

The proposed mitigation framework, incorporating EDR deployment, immutable backup strategies, ransomware response plans, Security Awareness Training, and Privileged Access Management, is supported by 20 quantitative KRIs with measurable thresholds aligned to OJK regulatory requirements. Future research should extend this framework through empirical validation via survey-based COBIT 5 maturity assessment across multiple Indonesian banking institutions.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Faculty of Information Technology, Perbanas Institute, Jakarta, for providing academic support and a conducive research environment throughout this study. Special appreciation is extended to the supervisors and lecturers who provided valuable guidance, constructive feedback, and insights during the research process.

The authors also acknowledge the contributions of various institutions and publicly available sources whose reports, regulations, and cybersecurity incident documentation were utilized in the development of this research, particularly those related to malware and ransomware incidents in the Indonesian banking sector. Finally, the authors are grateful to the organizing committee of the Perbanas International Conference on Economics, Business, Management, Accounting and IT (PROFICIENT) 2026 for providing a platform to disseminate and discuss this research with the academic and professional community.

References

Basel Committee on Banking Supervision. (2021). Principles for the sound management of operational risk. Bank for International Settlements.

Chainalysis. (2024). Crypto crime report 2024: Ransomware payments exceed $1 billion. Chainalysis Inc.

Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa023

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). Enterprise governance of information technology: Achieving alignment and value. Springer.

International Monetary Fund. (2024). Global financial stability report: The last mile, Financial vulnerabilities and risks. IMF Press.

International Organization for Standardization. (2018). ISO 31000:2018, Risk management: Guidelines.ISO.

ISACA. (2012). COBIT 5: A business framework for the governance and management of enterprise IT.ISACA.

Kouns, J., & Minoli, D. (2010). Information technology risk management in enterprise environments. JohnWiley & Sons.

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (SP 800-30Rev. 1). NIST.

Oktarina, D., & Hakim, L. (2022). IT governance assessment using COBIT 5 at a state-owned bank in Indonesia. *Journal of Information Systems and Informatics*, *4*(3), 621–635.

Otoritas Jasa Keuangan. (2017). POJK No. 14/POJK.03/2017 tentang rencana aksi bagi bank sistemik.OJK.

Otoritas Jasa Keuangan. (2022). POJK No. 11/POJK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum. OJK.

Pratama, A., & Rahayu, S. (2023). Analisis dampak serangan ransomware terhadap layanan perbankan: Studi kasus Bank Syariah Indonesia. *Jurnal Keamanan Siber Indonesia*, *4*(2), 88–101.

Proofpoint. (2024). State of the phish 2024: An in-depth look at user awareness, vulnerability, and resilience. Proofpoint Inc.

Rhoades, J. L. (2020). Cybersecurity risk management in the banking sector. *Journal of Financial Regulation*, *6*(1), 45–72. https://doi.org/10.1093/jfr/fjaa003

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10–21.

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of Computer Security*, *19*(4), 639–668.

Setiawan, B., Kusuma, A., & Wibowo, H. (2023). Cybersecurity control gap analysis using COBIT 5: Evidence from regional development banks. *Indonesian Journal of Computing and Cybernetics Systems*, *17*(1), 45–58.

Sophos. (2024). The state of ransomware 2024. Sophos Ltd.

Stamp, M. (2022). Information security: Principles and practice (3rd ed.). John Wiley & Sons.

Susanto, H., & Almunawar, M. N. (2018). Information security management systems: A novel framework and software as a tool for compliance with information security standard. CRC Press.

Verizon. (2024). Data breach investigations report 2024. Verizon Business.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.