Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 3, 882-895
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i3.353

Scenario-Based Risk and Control Formulation for Electronic Banking Channels ATM and EDC in Indonesian Commercial Banks

Navya Kirana Safitri* Telkom University, Indonesia
Sinung Suakanto Telkom University, Indonesia
Basuki Rahmad Telkom University, Indonesia

***Corresponding author:**
Navya Kirana Safitri, Telkom University, Indonesia, Indonesia.
✉navyakiranas@student.telkomuniversity.ac.id

Article Info:
Article history:
Received: May 18, 2026
Revised: June 29, 2026
Accepted: July 09, 2026

Keywords:
ATM; EDC; Risk Scenario; Risk Control; Risk Management; Banking.

Abstract

Background: ATMs and EDCs remain critical infrastructure components within Indonesia's national payment system. However, their extensive utilization exposes commercial banks to various technological, operational, human, physical, and third-party risks. Despite recurring incidents comprehensive studies that formulate ATM and EDC risk scenarios and corresponding control measures within the Indonesian banking context remain limited.
Objective: This study formulates risk scenarios and corresponding control measures for ATM and EDC electronic banking channels in Indonesian commercial banks.
Methods: A structured literature review was conducted using six academic databases: Google Scholar, ScienceDirect, ResearchGate, Scopus, Wiley Online Library, and MDPI. The identified risks were analyzed using the ISACA *Risk IT Framework* and mapped to the NIST *Cybersecurity Framework (CSF) 2.0* and ISO/IEC 27001:2022 standards. The proposed model was validated by six Subject Matter Experts (SMEs) with expertise in banking operations, IT risk management, information security, and payment systems using a 1–5 Likert scale.
Results: The study identified 25 risk scenarios across six categories and formulated 25 consolidated control measures. Each scenario links risk sources or threat actors, risk events, potential impacts, and corresponding controls. The controls were classified as preventive, detective, and corrective measures and mapped across the people, process, and technology dimensions. Expert validation produced an average score of 4.13/5.00 (83%), indicating a high level of acceptance.
Conclusion: As a proposed model derived from a systematic literature review and expert validation, this study provides a structured reference framework for risk management practitioners and policymakers in Indonesian commercial banking institutions.

To cite this article: Safitri, N. K., Suakanto, S., & Rahmad, B. (2026). Scenario-Based Risk and Control Formulation for Electronic Banking Channels ATM and EDC in Indonesian Commercial Banks. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(3), 882-895. https://doi.org/10.59261/jequi.v8i3.353

INTRODUCTION

The rapid advancement of information technology has enabled organizations to strengthen their ability to develop and maintain competitive advantage, while simultaneously reshaping prevailing trends, global market dynamics, and consumer behavior (Diener, 2021; Ulrich-Diener et al., 2025). In the banking sector, the widespread adoption of the internet has fundamentally altered the landscape of banking services, intensifying competition in the digital domain. Consequently, banks are compelled to adapt by introducing innovative digital-based services to replace obsolete technologies (Broby, 2021; Kraus et al., 2021; Ulrich-Diener et al., 2025).

Technological advancements have driven innovation in the banking industry by transforming business models through digital applications that improve access to financial services (Aspan et al., 2022). To enhance customer convenience and remain competitive amid the rapid growth of financial technology companies in Indonesia, banks have increased their investment in technology and strengthened digital banking services in line with the Banking 4.0 era and OJK Regulation POJK 12/POJK.03/2018. In this context, digital banking activities are supported by the key channels regulated by the Financial Services Authority (OJK) and Bank Indonesia, including ATMs, EDCs, internet banking, mobile banking, card-based payment instruments, QRIS, and corporate banking systems, which plays initial role not only in regulatory compliance but also in expanding market reach and competitiveness (Hidayat & Kassim, 2023; Maulidya & Afifah, 2021; Nuryana, 2024).

Although the use of mobile banking, internet banking, and e-wallets continues to grow, ATMs and EDCs remain essential components of Indonesia's financial transaction ecosystem. Data from Bank Indonesia indicate a consistent increase in the number of EDC machines, while ATM usage remains substantial, with transaction values reaching approximately IDR 7.2 quadrillion in 2024. This demonstrates that ATMs and EDCs continue to serve as critical infrastructure within the national payment system (Bank Indonesia, 2025a, 2025b).

However, the extensive utilization of these electronic channels also exposes banks to a wide range of security risks, including jackpotting, skimming, card data theft, and misuse of customer data by internal staff or merchants. The National Cyber and Crypto Agency (BSSN) reported that Indonesia experienced over 700 million cyber-attacks throughout 2022, with ransomware and malware-based attacks being the most prevalent threat category. According to BSSN's data, a total of 714,170,967 traffic anomalies and cyber intrusions were recorded during that year (CNN Indonesia, 2022). Furthermore, several Indonesian banks have experiences technology disruption that resulted in security vulnerabilities and service unavailability. Notable incidents include unauthorized access to customer account at Bank BCA resulting in losses of IDR 70 billion (Tempo, 2025), a week-long ATM service outage at bank DKI that prevented customers from making cash withdrawals (CNBC, 2025), and customer data theft through EDC machines in Surakarta (Espos, 2023). Such incidents lead to both financial and reputational losses and highlight the complex risk landscape of ATM and EDC channels, which encompasses technological, operational, human, and regulatory dimensions.

In response, banks have implemented various risk mitigation measures, including penetration testing, Fraud Detection Systems, operational certifications, and compliance with regulatory requirements issued by OJK and Bank Indonesia (Moon et al., 2022; Tandra, 2024). Nevertheless, the implementation and effectiveness of these controls vary considerably across institutions, indicating the need for more comprehensive and forward-looking risk management approaches.

According to the ISACA Risk IT Framework, effective risk management requires a mutual understanding between business and IT stakeholders regarding the risks to be managed. A key challenge in this process lies in the identification and analysis phase, specifically in recognizing risks that are relevant to a given context and that could adversely affect IT operations, either directly or indirectly (Sarker, 2025). To address this challenge, ISACA recommend the development of risk scenarios that provide a structural representation of the probability, frequency, and potential implications of risk events for the organization. In line with this, risk controls should be established to reduce both the likelihood and the impact of risks that may materialize.

Previous studies have examined ATM and EDC security from several perspectives. Studies on ATM security commonly focus on individual attack types, such as skimming, jackpotting, card fraud, or malware attacks (Eka & Umar, 2025). Other studies discuss cybersecurity risk management in banking through general frameworks, regulatory compliance, or information security controls (Chandra sekhar & Kumar, 2023). While these studies provide useful insights, they generally address risks, incidents, and controls separately. They do not provide an integrated and channel-specific representation that systematically connects risk sources or threat actors, risk events, potential impacts, and corresponding controls for ATM and EDC channels in

Indonesian commercial banks (Gerald et al., 2024; Harasheh & Provasi, 2023).

This limitation creates three research gaps. First, there is a scope gap, as existing studies tend to focus on individual ATM or EDC threats rather than a multidimensional risk landscape covering technological, operational, human, physical, and third-party risks. Second, there is a structural gap, as the reviewed literature presents risks, incidents, impacts, and controls in different formats and levels of detail. This variation makes it difficult to obtain a consolidated scenario-based reference that systematically represents the relationship between risk sources or threat actors, risk events, potential impacts, and corresponding controls for ATM and EDC channels in Indonesian commercial banks. Third, there is a control integration gap, as existing studies generally discuss controls independently and do not systematically link them to specific risk scenarios, classify them as preventive, detective, and corrective, or map their applicability across people, process, and technology.

Accordingly, this study formulates ATM and EDC risk scenarios and corresponding controls for Indonesian commercial banks. The novelty of this study does not lie in the use of the ISACA Risk IT Framework, NIST CSF 2.0, or ISO/IEC 27001:2022 as standalone frameworks. Rather, it lies in the integration of these established references to formulate an ATM and EDC-specific risk scenario and control reference model. The model systematically links risk sources or threat actors, risk events, potential impacts, and corresponding controls. Each control is classified as preventive, detective, or corrective; mapped across people, process, and technology; and aligned with NIST CSF 2.0 and ISO/IEC 27001:2022.

Based on the identified gaps, this study aims to (1) identify and categorize risks affecting ATM and EDC channels, (2) formulate risk scenarios that link risk sources or threat actors, risk events, and potential impacts, (3) formulate corresponding controls and classify them as preventive, detective, and corrective, and (4) map the controls across people, process, and technology and align them with NIST CSF 2.0 and ISO/IEC 27001:2022. The resulting model is subsequently evaluated through expert judgement.

Accordingly, this study addresses the following research questions: (1) What type of risks can occur in ATM and EDC electronic channels in banking institutions? (2) What risk scenarios and corresponding risk controls can be formulated to address the identified risks affecting ATM and EDC channels? (3) To what extent are the proposed risk scenarios and corresponding risk controls applicable to Indonesian commercial banks?

METHOD

This study employed a qualitative research design consisting of three sequential phases: (1) a Structured Literature Review (SLR) to identify and synthesize risks affecting ATM and EDC channels, (2) risk scenario and risk control formulation using internationally recognized IT risk management frameworks, and (3) expert validation to evaluate the relevance and applicability of the proposed model. The overall research process is illustrated in Figure 1.

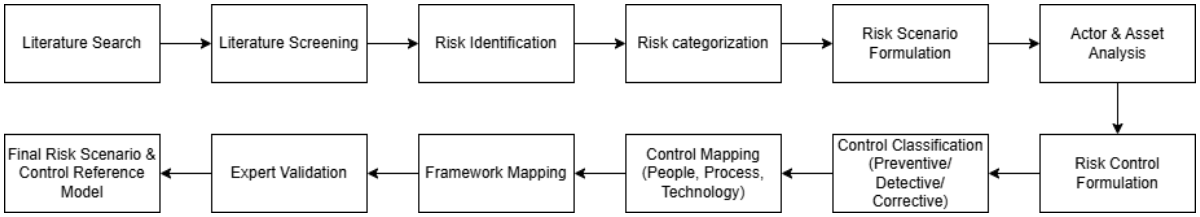

Figure 1. Research process

The first phase involved a systematic search and synthesizing existing literature relevant to a defined research topic (Machado et al., 2022). A systematic search was conducted across six academic databases: Google Scholar, ScienceDirect, ResearchGate, Scopus, Wiley Online Library, and MDPI. The search was performed using a combination of the following keywords: "scenario-based risk management", "ATM", "EDC", "cybersecurity", "Indonesian banking", "IT governance", "internal controls", "banking fraud", "electronic banking channels", and "ISACA IT Risk". The search was limited to publication between 2020 and 2026. In addition to academic literature,

relevant regulatory documents issued by Indonesian financial authorities were also incorporated as supplementary sources, including regulations and circulars issued by Bank Indonesia (BI) and the Financial Service Authority (OJK), such as Bank Indonesia Regulations (PBI), OJK Regulations (POJK), and OJK Circulars (SEOJK) were incorporated as supplementary sources to ensure alignment with the Indonesian regulatory framework. In addition to academic publications, publicly reported cybersecurity incidents involving ATM and EDC channels were reviewed to provide contextual evidence of emerging threats. However, these reports were not treated as primary evidence for risk identification and were used only to complement findings obtained from academic literature and regulatory documents.

Studies were included if they were published between 2020 and 2026, written in English or Indonesian, and published in peer-reviewed journals or conference proceedings. In terms of subject matter, included studies were required to address topics related to IT risk management, cybersecurity, banking fraud, ATM/EDC operations, IT governance, or internal controls in financial institutions. Studies published before 2020, irrelevant to information technology risk or banking operations, and duplicate publications identified across multiple databases were excluded. The literature selection process followed four sequential stages: (1) Identification an initial database search yielded 312 candidate records across all six databases; (2) Screening titles and abstracts were reviewed against the inclusion and exclusion criteria, resulting in 87 potentially relevant studies; (3) Eligibility assessment full-text review was conducted on the 87 screened studies, of which 43 were excluded due to insufficient relevance to ATM/EDC operations, lack of empirical grounding, or unavailability of full text; (4) Inclusion the remaining 44 studies, together with 12 regulatory documents and 5 publicly reported banking incidents, formed the final corpus used for risk scenario and control formulation. Studies were screened based on the predefined inclusion and exclusion criteria to ensure their relevance to the research objectives. The final corpus comprised literature that was considered relevant for developing the proposed risk scenarios and corresponding controls.

The second phase involved a deep analytical process to structure categorize and map the risk scenarios and risk controls identified through the literature review. This phase was guided by two complementary frameworks. The ISACA Risk IT Framework was employed to structure the risk scenarios, providing the analytical lens through which each risk event was examined in terms of its initiating actor, affected asset, and potential business impact. Risk identified from the literature were first categorized according to their characteristics and underlying causes. Each identified risk was subsequently formulated into a structured risk scenario consisting of a risk source or threat actor, risk event and potential impact following the ISACA Risk IT framework. This process resulted in six risk categories namely technological risk, operational risk, legal and regulatory risk, natural disaster risk, ATM/EDC vendor risk, switching vendor risk and shared network risk.

NIST CSF 2.0 and ISO/IEC 27001:2022 were then used as the primary reference frameworks for developing and mapping corresponding risk controls. Each control was classified into preventive, detective or corrective controls according to its functional role in the risk management lifecycle. Furthermore, each control was mapped to the People-Process-Technology domains and aligned with the corresponding NIST CSF 2.0 functions and ISO/IEC 27001:2022 Annex A controls to ensure consistency with internationally recognized cybersecurity and information security practices.

To assess the comprehensiveness and relevance of the proposed model, expert validation was conducted involving six Subject Matter Experts (SMEs) selected through purposive sampling. The minimum threshold of six validators was adopted to ensure sufficient diversity of expert perspectives while remaining feasible within the scope of this study. Validators were required to possess a minimum of 5 years of professional experience in IT risk management, banking operations, auditing, or IT governance, and familiarity with at least one internationally recognized IT risk management framework. Validators were drawn from diverse institutional backgrounds, including commercial banking institutions, IT consulting firms, and an independent audit practice, to ensure a broad and representative assessment. Each validator completed a validation instrument consisting of eight assessment statements evaluated using five-point Likert scales (1

= Strongly Disagree, 5 = Strongly Agree), covering relevance, completeness, clarity, consistency, applicability, and practical usefulness of the proposed model.

The validation result was analyzed using descriptive statistics by calculating the average score for each assessment statement and the overall mean score across all validators. The mean score for each statement was interpreted using the following scale: 1.00–1.79 = Strongly Disagree, 1.80–2.59 = Disagree, 2.60–3.39 = Neutral, 3.40–4.19 = Agree, 4.20–5.00 = Strongly Agree. To mitigate potential validator bias, validators were not informed of each other's responses, and the validation instrument was administered independently without interaction among validators. The instrument was pre-tested for clarity with two independent reviewers prior to distribution, and minor ambiguities in wording were resolved before the formal validation round. Qualitative comments provided by the SMEs were analyzed descriptively and incorporated to refine the proposed risk scenarios and corresponding risk controls.

RESULTS AND DISCUSSION

Result

Electronic Channels Architecture Overview

To provide foundational context for the risk scenarios developed in this study, Figure 1 presents a general overview of the ATM and EDC electronic channel architecture referencing on Bank Indonesia's *Blueprint Sistem Pembayaran Indonesia* (BSPI) 2025. As illustrated in Figure 1, ATM and EDC channels operate within a broader digital baking ecosystem that also includes internet banking and mobile banking. All these channels connect to a central Switching component, which serves as the primary transaction routing engine responsible for directing transaction requests to the appropriate destination, whether internal banking systems or external networks. This central role makes the switching infrastructure a critical single point of dependency, where any disruption can simultaneously affect multiple banking channels (Pangestu & Baskoro, 2022).

For transactions directed to the bank's own systems, the switching component communicates with Middleware (MCI), which acts as an integration layer between the switching engine and the core banking system. The core banking system is the authoritative source of customer account data and balance records and serves as the final arbiter of transaction authorization and settlement. Upon completion of core banking processing, responses are routed back through Middleware (EXT) which handles outbound communication to external parties and ensures that transaction results are properly relayed to the originating channels (Kumar, 2025; Saputra, 2025).

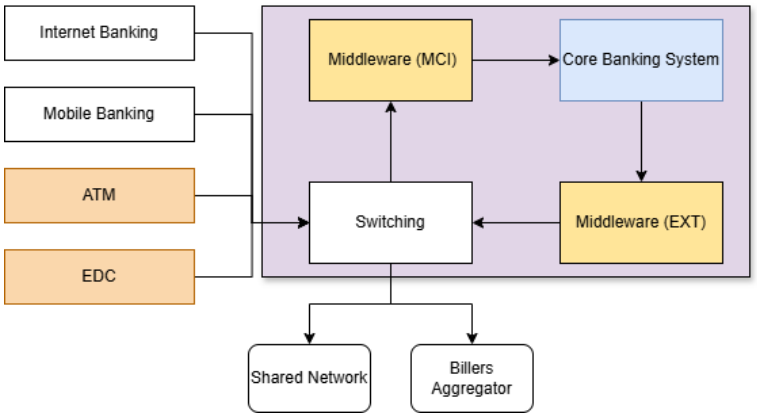

Figure 2. Electronic channel architecture overview

For transactions involving external parties, the switching component connects to two additional external networks, the Shared Networks, which facilities interbank transactions and card payment processing through network such as ATM Bersama, Prima or international card schemes, and the Biller Aggregator which handles bill payment and top-up transactions directed to third party billers (Putra & Kosasih, 2021; Andri & Lastiati, 2024).

This multi-layered architecture creates a complex web interdependencies between internal and external components, each of which represents a potential point of failure or exploitation. The ATM and EDC channels, as the physical endpoints of this infrastructure, are exposed to risks originating not only from their own hardware and software, but also from vulnerabilities and disruptions propagating through any of the upstream components including the switching system, middleware layers, core banking, shared network, and third-party aggregators (Mithun et al., 2022). This architecture serves as the basis for identifying potential risk sources and formulating ATM and EDC risk scenarios.

Risk Scenario

The synthesis of reviewed literature, regulatory documents, and documented banking incidents in Indonesia yielded a total of 25 risk scenarios threatening ATM and EDC electronic channels. These scenarios were structured using the ISACA Risk IT Framework, which prescribed that each risk scenario should define the initiating actor, the affected asset, and the potential business impact (ISACA, 2020; Nisa' et al., 2023). The identified risks were categorized into six categories, there are technological risk, operational risk, legal and regulatory risk, natural disaster risk, ATM/EDC vendor risk, switching vendor risk, and shared network risk. To establish traceability between risk scenarios and their corresponding mitigating controls, each scenario is mapped to the relevant risk controls developed in this study, as denoted in the "Mitigated By" column referencing Table 2. The complete of risk scenarios is presented in Table 1.

Table 1. Risk scenarios development

No.	Risk Category	Risk Scenario Title	Actor	Asset	Mitigated by
1.	Technological Risk	Ransomware attack on ATM and EDC management servers	People	Technology	C-7, C-8, C-9, C-14, C-22, C-23
2.	Technological Risk	Zero-day vulnerability exploitation in EDC software	Technology	Technology	C-7, C-14, C-15, C-17
3.	Technological Risk	Skimming	People	Technology	C-4, C-5, C-6, C-16, C-19
4.	Technological Risk	Phishing targeting bank employees or customers	People	Technology	C-1, C-2, C-4, C-16, C-21, C-25
5.	Technological Risk	ATM and EDC infrastructure misconfiguration with core banking integration	People	Technology	C-7, C-9, C-10, C-17, C-19, C-24
6.	Technological Risk	Network misconfiguration between ATM and switching or shared network	People	Technology	C-6, C-7, C-9, C-17, C-21
7.	Operational Risk	Incorrect ATM and EDC transaction fee configuration	People	Process	C-3, C-5, C-11, C-18, C-20, C-24
8.	Operational Risk	Transaction failure threshold misaligned with bank's business strategy	People	Process	C-11, C-18, C-20, C-24
9.	Operational Risk	ATM cash account configuration misaligned with the back records	People	Process	C-3, C-11, C-13, C-20, C-24
10.	Operational Risk	Failure during ATM and EDC reconciliation process	People	Process	C-13, C-18, C-20, C-21, C-24
11.	Legal and Regulatory Risk	Non-compliance with PCI DSS national security standard	People, Process	Process, Technology	C-4, C-6, C-7, C-9, C-11, C-17, C-19
12.	Legal and	Violation of personal data	Process	Process	C-4, C-9,

No.	Risk Category	Risk Scenario Title	Actor	Asset	Mitigated by
	regulatory Risk	protection regulations			C-11, C-12, C-21
13.	Natural Disaster Risk	Bank data center affected by natural disaster	Process	Technology	C-8, C-22, C-23
14.	Natural Disaster Risk	Regional power supply disruption	Technology	Technology	C-8, C-22, C-23
15.	Natural Disaster Risk	ATM kiosk or merchant EDC affected by natural disaster or civil unrest	Process	Technology	C-8, C-22, C-23
16.	ATM/EDC Vendor Risk	ATM vendor performing improper cash replenishment	People	Technology	C-3, C-9, C-12, C-18, C-21
17.	ATM/EDC Vendor Risk	ATM and EDC OS configuration misaligned with bank network post-upgrade	People	Technology	C-7, C-9, C-10, C-17, C-21
18.	ATM/EDC Vendor Risk	ATM cash imbalance during cash-in and cash-out processes	Process	Process	C-13, C-18, C-20, C-21, C-24
19.	ATM/EDC Vendor Risk	Hardware malfunction during cash-in or cash-out	Technology	Process	C-5, C-14, C-19, C-22
20.	Switching Vendor Risk	Switching database replication failure with bank database	Technology	Technology	C-13, C-14, C-17, C-21, C-22
21.	Switching Vendor Risk	System failure during migration process	Process, Technology	Technology	C-9, C-10, C-17, C-21, C-22
22.	Switching Vendor Risk	System malfunction due to unidentified as-is to to-be configuration changes	Process, People	Technology	C-9, C-10, C-17, C-19, C-21
23.	Shared Network Risk	Disruption of connectivity between shared network and bank	Technology	Technology	C-6, C-8, C-14, C-22, C-23
24.	Shared Network Risk	Mandatory compliance updates imposed by shared network operator	Process	Process, Technology	C-9, C-11, C-12, C-17, C-24
25.	Shared Network Risk	Undetected transaction anomalies bypassing shared network fraud detection	Technology, People	Technology	C-14, C-15, C-16, C-19, C-21

As presented in Table 1, the identified risk scenarios demonstrate that ATM and EDC electronic channels are exposed to multidimensional risks originating from technological, operational, regulatory, environmental, and third-party domains. Furthermore, the structured formulation of each scenario establishes explicit relationships between the threat source, affected asset, potential impact, and corresponding controls. This traceability provides the foundation for developing the proposed risk control model presented in the following section.

To facilitate traceability between the identified risk scenarios and the proposed mitigation measures, each scenario is linked to one or more risk controls through the "Mitigated By" column. The corresponding control identifiers (RC) refer to the proposed controls presented in Table 2. Multiple control references indicate that a single risk scenario may require a combination of preventive, detective, and corrective controls to achieve effective risk mitigation.

Risk Control

The analysis resulted in a consolidated set of 25 risk controls designed to mitigate the identified ATM and EDC risk scenarios. To facilitate implementation, the proposed controls were classified into three categories based on their functional role in the risk management lifecycle, namely preventive, detective, and corrective controls. Each control was developed by synthesizing recommendations from the reviewed literature and subsequently mapped to the corresponding functions of NIST CSF 2.0 and controls in ISO/IEC 27001:2022 Annex A. In addition, each control was mapped to the people, process, and technology dimensions to ensure alignment between the identified risk scenarios and the applicable mitigation measures. The complete set of proposed risk controls is presented in Table 2.

Table 2. Risk control

No.	Control	Type	Applicable To	NIST CSF 2.0	ISO 27001:2022
C-1.	Code of conduct, whistleblowing channel, and integrity screening	Preventive	People	GV.OC-01, GV.PO-01, GV.RR-02	A.5.1, A.6.1, A.62
C-2.	Security awareness and ethics training	Preventive	People	PR.AT-01, PR.AT-02	A.6.3 A.5.1
C-3.	Role definition, RACI matrix, and segregation of duties	Preventive	People, Process	GV.RR-01, GV.RR-02, PR.AA-05	A.5.2, A.5.3, A.8.18
C-4.	Role-based access control and least-privilege enforcement	Preventive	People, Technology	PR.AA-01, PR.AA-05	A.5.15, A.5.18, A.8.2
C-5.	Physical and logical device security	Preventive	Technology	PR.AA-03, PR.PS-01	A.7.1, A.7.8, A.8.1
C-6.	Network segmentation, encryption, and endpoint hardening	Preventive	Technology	PR.DS-02, PR.IR-01, PR.PS-01, PR.PS-02	A.8.20, A.8.21, A.8.22,
C-7.	Patch, vulnerability, and configuration management	Preventive	Technology	ID.RA-01, PR.PS-02, GV.PO-01	A.8.8, A.8.9, A.8.19, A.8.32
C-8.	Backup and redundancy infrastructure	Preventive	Technology	PR.DS-04, PR.DS-11	A.8.13, A.8.14 A.5.30
C-9.	Change management and change approval governance	Preventive	Process, Technology	GV.PO-02, GV.RR-03, ID.IM-02, PR.PS-04	A.8..32, A.5.2, A.5.3
C-10.	UAT, piloting test and pre-production release validation	Preventive	Process, Technology	PR.PS-04, ID.IM-02	A.8.29, A.8.32
C-11.	SOP, workflow standardization, and compliance-based KPI	Preventive	Process	GV.PO-01, GV.PO-02, PR.PS-04	A.5.36, A.5.37
C-12.	Policy governance, escalation line, and accountability matrix	Preventive	People, Process	GV.PO-01, GV.RR-01, GV.RR-03	A.5.1, A.5.2, A.5.3
C-13.	Inter-system reconciliation and process automation	Preventive	Process, Technology	PR.DS-01, PR.PS-04, GV.PO-01	A.8.17, A.8.25, A.8.26

No.	Control	Type	Applicable To	NIST CSF 2.0	ISO 27001:2022
	validation				
C-14.	Continuous monitoring through SIEM, EDS/IPS, and log management	Detective	Technology	DE.CM-01, DE.CM-03, DE.CM-07, DE.AE-02	A.8.15, A.8.16, A.5.25
C-15.	Threat intelligence correlation and anomaly detection	Detective	Technology	ID.RA-02, DE.AE-06 DE.CM-08	A.5.7, A.8.16, A.8.8
C-16.	Access anomaly alerting and privilege monitoring	Detective	People, Technology	DE.CM-03, DE.AE-06 PR.AA-05	A.8.2, A.8.16 A.5.18
C-17.	Configuration drift and vulnerability scanning	Detective	Process, Technology	DE.CM-01, DE.CM-09, ID.RA-01	A.8.9, A.8.16, A.8.29
C-18.	Real-time process monitoring, SLA tracking, and exception alerting	Detective	Process	DE.CM-09, DE.AE-03, DE.AE-06, GV.OV-01	A.8.15, A.8.16, A.5.36
C-19.	Internal audit, policy compliance review, and fraud analytics	Detective	People, Process	ID.IM-02, GV.OV-02, GV.OV-03, DE.CM-06	A.5.35, A.5.36, A.8.16
C-20.	Periodic reconciliation and performance dashboard	Detective	Process	DE.AE-02, ID.IM-02, GV.OV-01	A.5.36, A.8.16
C-21.	Incident response, root cause analysis, and corrective action	Corrective	People, Process, Technology	RS.AN-03, RS.AN-04, RS.AN-05, RS.MI-01	A.5.26, A.5.27, A.5.28, A.10.2
C-22.	Rollback, data restore and system recovery	Corrective	Technology	RC.RP-01, RC.RP-02, RC.RP-03, RS.MI-02	A.8.13, A.5.30, A.8.32
C-23.	Disaster recovery planning and DR drills	Corrective	Technology	RC.RP-01, RC.RP-05	A.5.29, A.5.30, A.8.14
C-24.	Process re-engineering, policy synchronization, and continuous improvement	Corrective	Process	ID.IM-01, ID.IM-04, GV.OV-03, GV.PO-02	A.5.27, A.5.37, A.10.1, A.10.2
C-25.	Retraining, role, redesign, and incident communication	Corrective	People	RS.CO-01, RS.CO-03, RC.CO-03, PR.AT-01	A.5.26, A.5.27, A.6.3, A.6.4, A.6.8

Table 2 presents the proposed risk controls demonstrate that effective ATM and EDC risk management requires a balanced combination of preventive, detective, and corrective measures across people, process, and technology dimensions. The mapping also shows that several controls mitigate multiple risk scenarios simultaneously, indicating that the proposed model adopts a layered defense approach rather than relying on isolated security measures. Furthermore, the alignment with NIST CSF 2.0 and ISO/IEC 27001:2022 provides traceability between the proposed controls and internationally recognized cybersecurity and information security practices, supporting their applicability within Indonesian commercial banking institutions.

Expert Validation

To evaluate the applicability and comprehensiveness of the proposed model, expert validation was conducted involving six practitioners from Indonesian commercial banking institutions with professional backgrounds in IT risk management, IT governance, banking operations, and information security. Each validator assessed the proposed model using eight evaluation statements measured on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). The complete validation results are presented in Table 3.

The validation results indicate an overall mean score of 4.13 out of 5.00, indicating that the proposed model is generally considered comprehensive and applicable for ATM and EDC risk management in Indonesian commercial banking institutions. Most evaluation criteria received mean scores above 4.00, particularly those related to the completeness of the identified risk scenarios, the relevance of the proposed risk controls, and the overall applicability of the model. The relatively lower score for corrective controls (3.80) suggests that additional recovery mechanisms or implementation guidance may further strengthen the proposed model. Overall, the validation findings provide empirical support for the practical applicability of the proposed model and serve as the basis for the discussion presented in the table 3.

Table 3. Expert validation

No.	Statement	Mean Score
1.	The identified risk categories adequately represent the types of risks occurring in ATM and EDC operations	4.20
2.	The developed risk scenarios are relevant and representative of actual threats	4.20
3.	The proposed preventive controls are sufficient to reduce the likelihood of identified risks	4.20
4.	The proposed detective controls are sufficient to enable timely identification of risk events	4.20
5.	The proposed corrective controls are sufficient to facilitate recovery following a risk event	3.80
6.	The mapping of controls to NIST CSF 2.0 and ISO/IEC 27001:2022 is appropriate and accurate	4.00
7.	The overall model comprehensively covers the risk landscape of ATM and EDC channels	4.20
8.	The proposed model can serve as a practical reference for risk management practitioners	4.20
	Overall Mean	**4.13**

Although the validation demonstrates positive practitioner acceptance of the proposed model, the results should be interpreted within the context of qualitative expert judgement and are therefore discussed further in terms of practical implications and study limitations in the following section.

Discussion

The findings indicate that the risk landscape of ATM and EDC electronic channels extends beyond conventional cybersecurity threats. Although technological risks constitute the largest category, a substantial number of identified scenarios originate from operational processes, regulatory compliance, physical infrastructure, and dependencies on third-party providers (Ciaccio & Onat, 2025; Degadwala & Bharatbhai, 2024; Mahardinata & Imaroh, 2025). This finding suggests that effective ATM and EDC risk management requires a multidimensional approach that integrates people, process, technology, and external governance rather than relying solely on technical safeguards.

Another notable finding is the explicit relationship established between risk scenarios and corresponding risk controls. Each identified scenario was formulated by linking the threat source, affected asset, potential impact, and appropriate preventive, detective, and corrective controls.

This traceability enables banking institutions to better understand not only what risks may occur but also which controls are most relevant for mitigating those risks, thereby supporting more systematic and consistent risk management practices (Ilmiha & Shah, 2024; Joseph et al., 2024).

Previous studies have primarily focused on specific issues related to ATM and EDC operations, such as fraud detection, cybersecurity incidents, information security compliance, or the implementation of individual risk management frameworks (Amsaroka et al., 2024; Hakki et al., 2026). While these studies provide valuable recommendations, they generally identify risks independently without explicitly establishing relationships between risk sources, risk events, potential impacts, and corresponding controls.

In contrast, this study proposes a structured model that integrates the ISACA Risk IT Framework for scenario formulation with NIST CSF 2.0 and ISO/IEC 27001:2022 for risk control mapping. Rather than directly adopting controls from international standards, the proposed controls were first formulated based on the identified ATM and EDC risk scenarios and subsequently mapped to both models. This approach strengthens traceability between identified risks and mitigation strategies while maintaining alignment with internationally recognized cybersecurity and information security practices.

From a practical perspective, the proposed model may serve as a reference for Indonesian commercial banks in identifying ATM and EDC risks and selecting appropriate controls based on the characteristics of each risk scenario. The structured relationship between risk scenarios and controls may also support more consistent implementation of IT risk management practices across banking institutions.

Nevertheless, implementing the proposed model may present several practical challenges. Advanced security controls, such as continuous monitoring platforms, disaster recovery infrastructure, and security analytics, require considerable financial investment (Joseph et al., 2024; Widjajarto et al., 2024). Furthermore, successful implementation depends on the availability of qualified personnel with expertise in IT risk management and cybersecurity (Plachkinova & Knapp, 2023). The complexity of integrating controls across legacy core banking systems, middleware, switching platforms, shared networks, and third-party vendors may also affect implementation effectiveness.

This study is subject to several limitations. The proposed model was developed through structured literature review, framework analysis, and expert judgement without empirical implementation within an operational banking environment. In addition, expert validation involved six practitioners and therefore reflects qualitative professional judgement that may be influenced by individual experience and interpretation. Future research may involve broader expert participation and empirical implementation to further evaluate the effectiveness of the proposed model in banking operations. Accordingly, the primary contribution of this study lies not in introducing new cybersecurity controls, but in providing a structured and traceable model that systematically links ATM and EDC risk scenarios with corresponding risk controls and internationally recognized security standards.

CONCLUSION

This study proposed a scenario-based risk scenario and risk control model for ATM and EDC electronic channels in Indonesian commercial banking institutions. Through a structured literature review, framework analysis, and expert validation, the study identified 25 risk scenarios across six risk categories and formulated 25 consolidated risk controls classified into preventive, detective, and corrective controls. The proposed controls were subsequently mapped to NIST CSF 2.0 and ISO/IEC 27001:2022 to ensure alignment with internationally recognized cybersecurity and information security practices. Expert validation produced an overall mean score of 4.13 out of 5.00, indicating positive practitioner acceptance of the proposed model.

The findings suggest that ATM and EDC risk management requires a holistic approach that integrates governance, process standardization, vendor management, and regulatory compliance across people, process, and technology dimensions. Rather than introducing new security controls, this study contributes by systematically linking risk scenarios with corresponding controls and internationally recognized frameworks, thereby providing a structured reference for

future risk management initiatives in Indonesian commercial banking institutions.

This study has several limitations. The proposed model was developed through literature synthesis and expert judgement without empirical implementation in an operational banking environment. In addition, expert validation involved only six practitioners, which may not fully represent the diversity of perspectives across Indonesian commercial banks. Furthermore, the model focuses on qualitative risk formulation and does not incorporate quantitative risk assessment or prioritization methods. Future research should evaluate the model through implementation in commercial banking institutions, involve a broader panel of experts, and investigate quantitative approaches to support risk prioritization and decision-making.

ACKNOWLEDGEMENT

The authors would like to thank Mr. Sinung Suakanto and Mr. Basuki Rahmad for the guidance and support throughout this research, and Telkom University for the academic resources provided.

AUTHOR CONTRIBUTION STATEMENT

Navya Kirana Safitri contributed to the conceptualization, research design, data collection, risk analysis, and preparation of the original manuscript. Sinung Suakanto contributed to methodology development, supervision, validation, and critical review of the research framework. Basuki Rahmad contributed to methodology development, technical evaluation, interpretation of findings, manuscript refinement, and final review.

REFERENCES

Ali, S. M., Hoq, S. N., Bari, A. M., Kabir, G., & Paul, S. K. (2022). Evaluating factors contributing to the failure of information system in the banking industry. *Plos one*, *17*(3), 1–21. https://doi.org/10.1371/journal.pone.0265674

Amsaroka, M. H., Yadiati, W., & Winarningsih, S. (2024). Literature Review: the Relationship Between Internal Control System of the Government (SPIP), Good Government Governance (GGG), And Fraud Prevention. *JASa (Jurnal Akuntansi, Audit Dan Sistem Informasi Akuntansi)*, *8*(1), 122–136. https://doi.org/10.36555/jasa.v8i1.2440

Andri, A., & Lastiati, A. (2024). The Influence Of Brand Awareness, Transaction Fees On Consumer Intention In Transacting Using ATM Off Network/Off Us With Consumer Trust As A Moderating Variable. *Accruals (Accounting Research Journal of Sutaatmadja)*, *8*(02). 86–97.

Aspan, H., Nasution, A. P., & Malikhah, I. (2022). *Digital Banking in Indonesia : The Development of Cashless Culture and Regulations*. *9*(January), 534–543.

Bank Indonesia. (2025a). *Tabel 5a. ATM dan ATM + Debet*. 8.

Bank Indonesia. (2025b). *Tabel 5b. Infrastruktur Alat Pembayaran Menggunakan Kartu (APMK) dan Uang Elektronik (UE) Table 5g . Card-Based Payment Instruments (APMK) and Electronic Money (UE) Infrastructures Jumlah Merchant Juta Transaksi / Millions of Transaction Juta Tra*.

Broby, D. (2021). Financial technology and the future of banking. *Financial Innovation*, *7*(1). https://doi.org/10.1186/s40854-021-00264-y

Chandra, S., & Kumar, M. (2023). An Overview of Cyber Security in Digital Banking Sector. *East Asian Journal of Multidisciplinary Research*, *2*(1), 43–52. https://doi.org/10.55927/eajmr.v2i1.1671

Ciaccio, J., & Onat, I. (2025). An Analysis of ATM and Point-of-Sale Skimming. In *Orion Policy Institute*. Orion Policy Institute. https://doi.org/10.13140/RG.2.2.24913.03680

CNBC. (2025). *Kronologi Bank DKI Error Seminggu Lebih hingga Direktur IT Dipecat*. https://www.cnbcindonesia.com/market/20250409151436-17-624624/kronologi-bank-dki-error-seminggu-lebih-hingga-direktur-it-dipecat

CNN Indonesia. (2022). *RI Dihantam 700 Juta Serangan Siber di 2022, Modus Pemerasan Dominan*. https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan

Diener, F. (2021). *Digital Transformation in Banking : A Managerial Perspective on Barriers to Change*.

Degadwala, S., & Bharatbhai, P. T. (2024). Advancements in ATM Security for Movement and Tampering Detection: A Review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(5), 79–89. https://doi.org/10.32628/cseit2410587

Eka, K. W. D., & Umar Gazali, I. M. (2025). Law Enforcement of Skimming as a Cyber Crime: Digital Forensic Challenges and Evidence in Court. In *Pena Justisia* (Vol. 24, Number 1).

Espos. (2023). *Penipuan lewat Mesin EDC, Mantan Karyawan Bank Ternama di Semarang Ditangkap*. https://regional.espos.id/penipuan-lewat-mesin-edc-mantan-karyawan-bank-ternama-di-semarang-ditangkap-1781400

Gerald, N., Oluwapelumi, O., & Eli, K. A. (2024). Quality control in financial operations: Best practices for risk mitigation and compliance. *World Journal of Advanced Research and Reviews*, *24*(1), 735–749. https://doi.org/10.30574/wjarr.2024.24.1.3100

Hakki, T. W., Sofianty, D., Simanungkalit, J., & Alvionita, D. (2026). Pencegahan Fraud Melalui Internal Control dan Governance Risk Management Compliance. *JEMSI*, *7*(5). https://doi.org/10.38035/jemsi.v7i5

Harasheh, M., & Provasi, R. (2023). A need for assurance: Do internal control systems integrate environmental, social, and governance factors? *Corporate Social Responsibility and Environmental Management*, *30*(1), 384–401. https://doi.org/10.1002/csr.2361

Hidayat, A., & Kassim, S. (2023). *The Digital Banking Services: A Selection Model From Islamic*. *8*(1), 41–58.

Ilmiha, J., & Shah Suboh, A. (2024). The Effectiveness of Internal Control in Preventing Accounting Fraud in Financial Companies. *East Asian Journal of Multidisciplinary Research (EAJMR)*, *3*(6), 2181–2192. https://doi.org/10.55927/eajmr.v3i6.9952

ISACA. (2020). *Personal Copy of Basuki Rahmad (ISACA ID: 206164) RISK IT PRACTITIONER GUIDE, 2nd Edition 2 About ISACA Reservation of Rights*. www.isaca.org

Joseph, E. K. Z., Frederick, O. A., Nicholas, N., & Bernard, O. A. (2024). Effectiveness of internal controls mechanisms in preventing and detecting fraud. *Finance & Accounting Research Journal*, *6*(7), 1259–1274. https://doi.org/10.51594/farj.v6i7.1322

Kraus, S., Jones, P., Kailer, N., Weinmann, A., & Chaparro-banegas, N. (2021). *Digital Transformation: An Overview of the Current State of the Art of Research*. https://doi.org/10.1177/21582440211047576

Kumar, L. M. S. (2025). Developing Protocol Translation Mechanisms for Legacy Banking Systems. *International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)*, *14*(5). https://doi.org/10.15680/IJIRSET.2025.1405004

Machado, A. D. B., Secinaro, S., Calandra, D., Secinaro, S., & Calandra, D. (2022). Knowledge management and digital transformation for Industry 4.0: a structured literature review. *Knowledge Management Research & Practice*, *20*(2), 320–338. https://doi.org/10.1080/14778238.2021.2015261

Mahardinata, P., & Imaroh, T. S. (2025). Risk Management Analysis to Minimize the Occurrence of Fraud in ATM Machine Activities (A Study at XY Company in the Jakarta Area). *Jurnal Doktor Manajemen (JDM)*, *8*(1), 112. https://doi.org/10.22441/jdm.v8i1.33125

Maulidya, G. P., & Afifah, N. (2021). Perbankan Dalam Era Baru Digital: Menuju Bank 4 . 0. *Jurnal Proceeding Seminar Bisnis Seri V*, 278–288.

Moon, I. T., Shamsuzzaman, M., Musfiqur, M., Mridha, R., Sayed, A., & Rahaman, M. (2022). *Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems*. 103–129. https://doi.org/10.4236/jcc.2022.107007

Nisa, F. Z., Febrianti, G. D., & Ajrina, N. N. (2023). Systematic Literature Review: Analisis Implementasi Manajemen Risiko TI Menggunakan Framework COBIT di Sektor Industri Jasa. *Bulletin of Computer Science Research*, *4*(1), 66–74. https://doi.org/10.47065/bulletincsr.v4i1.313

Nuryana, I. (2024). Perkembangan Industri Perbankan di Era Digital. *Jurnal Manajemen Dan Keuangan*, *13*(2), 162–179.

Pangestu, A., & Baskoro, R. A. (2022). *Analysis of the Development of the National Payment Gateway (GPN) as a Symbol of Domestic Retail Transaction Sovereignty in Indonesia*. (December 2020).

https://doi.org/10.4108/eai.27-7-2021.2316817

Plachkinova, M., & Knapp, K. (2023). Least Privilege across People, Process, and Technology: Endpoint Security Framework. *Journal of Computer Information Systems*, *63*(5), 1153–1165. https://doi.org/10.1080/08874417.2022.2128937

Putra, I. M. A. M., & Kosasih, J. I. (2021, December). Modes of Bank Fund Transfer Crime in Digital Transactions. In *2nd International Conference on Business Law and Local Wisdom in Tourism (ICBLT 2021)* (pp. 167-171). Atlantis Press.

Saputra, S. (2025). Analisis Perbandingan Format Pesan ISO 8583 dan JSON pada Sistem Transaksi Keuangan. *Bulletin of Computer Science Research*, *6*(1), 548-557. https://doi.org/10.47065/bulletincsr.v6i1.839

Sarker, S. K. (2025). Bridging IT Risk Governance in Bangladesh: A Comparative Gap Analysis of Bangladesh Bank's Guideline on ICT Security v4.0 and ISACA's Risk IT Framework. *International Journal of Innovative Science and Research Technology*, 626–630. https://doi.org/10.38124/ijisrt/25oct257

Tandra, R. (2024). *The Best Machine Learning for Fraud Detection in Banking Sector : A Systematic Literature Review*. *7*(2). https://doi.org/10.32877/eb.v7i2.1474

Tempo. (2025). *BCA Investigasi Kasus Pembobolan Rekening Nasabah*. https://www.tempo.co/ekonomi/bca-investigasi-kasus-pembobolan-rekening-nasabah-2069111

Ulrich-Diener, F., Dvouletý, O., & Špaček, M. (2025). The future of banking: What are the actual barriers to bank digitalization? *BRQ Business Research Quarterly*, *28*(2), 491–513. https://doi.org/10.1177/23409444231211597

Wang, R., & Ziegel, J. F. (2021). Scenario-based risk evaluation. *Finance and Stochastics*, *25*(4), 725–756. https://doi.org/10.1007/s00780-021-00460-9

Widjajarto, A., Lubis, M., & Lubis, A. R. (2024). Service Level Agreement (SLAs) Model for Disaster Recovery Center (DRC) Based on Computational Resource Model of Virtual Machine. *Procedia Computer Science*, *234*, 1476–1483. https://doi.org/10.1016/j.procs.2024.03.148