Journal of Emerging Information Systems and Business Intelligence
ISSN: 2774-3993
Journal homepage: https://ejournal.unesa.ac.id/index.php/JEISBI/

Enhancing Business Continuity Through Proactive Information System Risk Management in the Financial Services Sector

M. Desfreezal Zurarah Bartien[1], Aries Dwi Indriyanti[2]
[1,2]*Universitas Negeri Surabaya, Surabaya, Indonesia*
mbartien.21048@mhs.unesa.ac.id, ariesdwi@unesa.ac.id

ABSTRACT

PT XYZ, a company operating in the financial services sector, heavily relies on its colection information system to maintain smooth business operations. In line with the company's strategic plan to conduct a vendor migration for this system, a comprehensive risk analysis becomes crucial to ensure data security, regulatory compliance, and business continuity. This study aims to analyze the risks within PT XYZ's colection information system using a combined approach of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode & Effect Analysis (FMEA) methods. The OCTAVE method was systematically applied to identify relevant critical assets, threats, and vulnerabilities. Subsequently, the FMEA method was implemented to quantitatively evaluate the identified risk scenarios to determine their priority levels. The study successfully identified a range of fundamental critical assets across data, system, and brainware categories, and formulated numerous associated risk scenarios. Through the FMEA assessment, these scenarios were classified by their priority level, with a portion identified as high-risk requiring immediate attention. For these high-priority risks, this research recommends actionable mitigation strategies based on controls from the ISO 27001:2022 standard. This study produces a measurable risk profile that serves as a strategic foundation for PT XYZ to effectively manage information security.

Keyword: Risk Management, Information Security, OCTAVE, FMEA, Collection Information System.

Article Info:
Article history:
Received Ocotber 7, 2025
Revised February 5, 2026
Accepted February 20, 2026

Corresponding Author
M. Desfreezal Zurarah Bartien
Universitas Negeri Surabaya, Surabaya, Indonesia
mbartien.21048@mhs.unesa.ac.id

1. INTRODUCTION

The advancement of information technology has fundamentally reshaped various sectors, including the global business landscape. Organizations now leverage digital processes to manage operations, communication, and decision-making more effectively, leading to new opportunities in workflow automation, system integration, and in-depth data analysis. This digital transformation not only boosts productivity but also provides a significant competitive advantage [1]. However, this increased reliance on technology introduces significant challenges, particularly concerning information security and system reliability. For modern enterprises, where information systems support all operational and strategic activities, the inability to protect against internal and external threats can lead to operational disruptions, substantial financial losses, and severe reputational damage [2].

Information security is a critical component of IT governance, centered on the principles of Confidentiality, Integrity, and Availability (the CIA Triad) [3]. The urgency of upholding these principles is particularly high in the financial services sector, which is governed by strict regulations. In Indonesia, the Otoritas Jasa Keuangan (OJK) mandates that financial service businesses must secure consumer information and their information systems [4]. This context frames the central problem for PT XYZ, a financing company planning a strategic migration of its core collection information system from a third-party vendor to an in-house model. This migration presents a complex challenge, as the system is integral to the company's cash flow and consists of numerous integrated technologies. A comprehensive risk analysis is therefore imperative to perform due diligence, identify potential threats arising from the migration, and ensure continuous compliance with OJK regulations.

To address this challenge, a structured risk management approach is essential. The literature provides several frameworks, with the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method offering a structured approach to identify risks to critical assets from an organizational and technological perspective [5]. While OCTAVE excels at risk identification, the Failure Mode and Effect Analysis (FMEA) method provides a quantitative means to evaluate and prioritize these identified risks. FMEA assesses risks based on their Severity, Occurrence, and Detection, culminating in a Risk Priority Number (RPN) that guides data-driven mitigation efforts [6]. The combination of these two methods offers a comprehensive solution, enabling a thorough and prioritized risk assessment [7].

This study proposes a hybrid risk analysis framework by integrating the OCTAVE and FMEA methods to create a measurable risk profile for PT XYZ's collection information system. The novelty of this research lies in its practical application of this combined methodology to the specific, high-stakes context of a core system vendor migration within the Indonesian financial sector. The objective is to conduct an in-depth risk analysis that not only identifies critical assets and vulnerabilities but also provides a clear prioritization of risks to guide the development of effective mitigation strategies. The findings are expected to serve as a strategic reference for PT XYZ to enhance its information security posture, ensure a secure system migration, and maintain organizational continuity.

2. METHODS

This research employed a qualitative case study methodology to conduct a comprehensive information system risk analysis. Data collection was initiated through a literature review of relevant scientific journals and books, which informed the creation of an interview instrument. The primary data was gathered via semi-structured interviews with key stakeholders at three organizational levels: senior management, operational management, and staff, to ensure a multi-perspective understanding of the system [2]. The analytical process followed a structured framework combining the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode & Effect Analysis (FMEA) methods. The process began with the OCTAVE method's Organizational View to identify critical assets and their associated threat profiles based on stakeholder input. This was followed by the Technological View, where key technological components of the collection information system were identified and evaluated to uncover technical vulnerabilities. In the final Risk Analysis phase, the identified risk scenarios were quantitatively measured using FMEA. Each risk was assessed based on its Severity (S), Occurrence (O), and Detection (D) to calculate a Risk Priority Number (RPN) with the formula $RPN = \mathrm{S} \times \mathrm{O} \times \mathrm{D}$. The RPN scores were then used to categorize risks into high, medium, and low priorities [6]. For risks categorized as

'High', actionable mitigation strategies were formulated by referencing the relevant security controls from Annex A of the ISO 27001:2022 standard to produce the final recommendations.

3. RESULTS AND DISCUSSION

The analysis began by implementing the Organizational View phase of the OCTAVE method. This initial phase aimed to identify the information system's critical assets and their corresponding threat landscapes by gathering qualitative data from stakeholders at three distinct organizational tiers: senior management, operational management, and staff.

3.1 Critical Asset and Threat Profile Identification

The multi-level interview process revealed that risk perception varied significantly across the organizational hierarchy. Senior management viewed risk from a strategic perspective, focusing on fundamental threats to business continuity, such as reputational damage from data breaches, financial loss from system failure, and the strategic limitations imposed by vendor dependency. In contrast, operational management's perspective was tactical, centered on daily productivity and efficiency. Their primary concerns were system reliability, the impact of human error, and the need for better monitoring tools to ensure procedural compliance. Finally, the staff provided a practical, ground-level view, highlighting usability issues, application performance bottlenecks, and security vulnerabilities they directly encountered, such as phishing attempts. This holistic data gathering process was crucial for developing a comprehensive understanding of the risk environment.

From this analysis, a total of 18 critical assets were identified and categorized into four distinct types: Data, Software, Network, and Brainware. These assets form the core operational and strategic components of PT XYZ's collection information system. The most pivotal assets include the central Collection System (S.01), which governs all business logic; sensitive Customer and Transaction Data (D.02, D.04), which are vital for operations and regulatory compliance; and the Payment Gateway (S.06), which represents a critical single point of failure for the company's cash flow. A summary of all identified critical assets is presented in Table 1.

Following the asset identification, a total of 56 specific threats were mapped to these assets based on potential violations of their confidentiality, integrity, or availability. The identified threats encompass a wide spectrum of risks. These include technical threats, such as system unavailability and data corruption during transfer; security breaches, like unauthorized access to the collection system and leakage of sensitive customer data (PII); and human-centric threats, including human error during data input, credential theft through social engineering, and potential misuse of high-privilege access. The threat of Customer Data (D.02) leakage, for instance, directly aligns with the strategic concerns of senior management regarding regulatory compliance, while the threat of Human error by Users (B.01) reflects the primary operational concern of the management team.

Table 1. Identified Critical Assets

Asset Type	Critical Asset (Code)	Descriptions
Data	Data Warehouse (D.01)	Central repository for strategic business intelligence.
	Customer Data (PII) (D.02)	Essential for operations and subject to strict regulations.
	Contract Data (D.03)	Integrity is crucial for accurate financial calculations.
	Transaction Data (D.04)	Serves as the legal proof of payment; accuracy is absolute.
	Call Result Data (D.05)	Informs subsequent collection strategies in real-time.
	Visit Result Data (D.06)	Validates field activities and prevents agent fraud.
	Employee Data (D.07)	Confidential data essential for HR and performance management.
Software	Collection System (S.01)	The core "brain" of the entire collection operation.
	Payment Information System (S.02)	Used for monitoring and investigating payment transactions.
	Call Center System (S.03)	Endpoint application for daily desk collection activities.
	Field Collection System (S.04)	Endpoint application for agents operating in unsecured environments.
	Employee Management System (S.05)	Manages sensitive internal HR data and evaluations.
	Payment Gateway (S.06)	Critical infrastructure for processing all incoming payments.
Network	External Connectivity (N.01)	Foundation of the hybrid architecture; crucial for all data flow.
	Network Security System (N.02)	Protects the integrity and confidentiality of the network perimeter.
Brainware	User (B.01)	Primary source of operational data input; high risk of human error.
	Analyst (B.02)	Role with broad access for quality control and investigation.
	Admin (B.03)	Highest privilege level; actions can have system-wide impact.

3.2 Key Component and Vulnerability Analysis

Following the identification of critical assets, the analysis transitioned to the Technological View to examine the system's architectural design and uncover underlying vulnerabilities. This phase revealed that the collection information system operates on a Hybrid Cloud Architecture, which segregates components into two distinct environments: a vendor-controlled cloud environment hosting the core system, and an environment managed directly by PT XYZ. The logical architecture and critical data flows between these components are depicted in Figure 1.

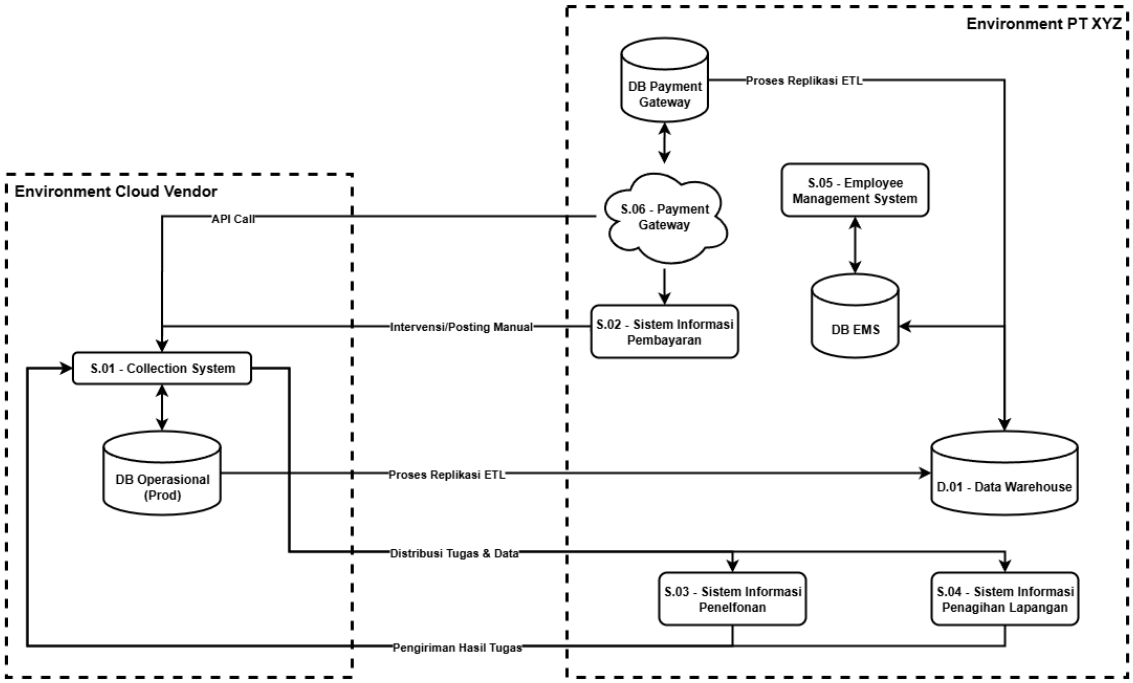

Figure 1. The Hybrid Cloud Architecture and Data Flow of the Collection Information System

The architecture highlights a significant dependency on the external vendor, who manages the core Collection System (S.01) and its operational database. Key data flows, such as the real-time payment verification via API call to the PT XYZ-managed Payment Gateway (S.06) and the daily ETL processes to the central Data Warehouse (D.01), traverse the boundaries of these two environments. This architectural separation is a foundational element in understanding the system's risk profile.

The subsequent evaluation of these key components identified a total of 93 distinct vulnerabilities. Rather than being isolated technical flaws, these vulnerabilities pointed towards systemic issues that could be categorized into several key themes:

1. **Vendor and Third-Party Dependency:** A primary source of vulnerability stemmed from a lack of control and visibility over the vendor's environment. This was evidenced by an SLA that lacked clear Recovery Time Objectives (RTOs), the absence of rights to conduct in-depth security audits of the vendor's personnel and infrastructure, and reliance on an untested Business Continuity Plan (BCP) from the provider.
2. **Weak Access Control Management:** Pervasive weaknesses in access control were identified across critical systems. Notable examples include the absence of Multi-Factor Authentication (MFA) for administrator access to the Collection System (S.01) and Payment Gateway (S.06), ineffective and non-periodic reviews of user access rights, and the granting of excessive privileges to personnel beyond their job requirements.
3. **Procedural and Policy Gaps:** A significant number of vulnerabilities were rooted in inadequate internal procedures. These included ineffective change management controls for system configurations, a lack of regular security awareness training and assessments for staff, poorly documented procedures for manual data processing, and inefficient processes for revoking access for resigned employees, which could lead to sabotage or data leakage.

4. **Technical Security Deficiencies:** The analysis also uncovered specific technical weaknesses, such as the use of outdated web browsers to access internal systems, the lack of an anti-malware mechanism for file uploads, and unencrypted data traffic channels between critical systems, creating opportunities for man-in-the-middle attacks.

These identified vulnerabilities provide the underlying causes for the threats defined previously and form the basis for the subsequent quantitative risk analysis.

3.3 Risk Prioritization and Mitigation Strategies

The culmination of the research was the comprehensive risk analysis, where the previously identified assets, threats, and vulnerabilities were integrated into the Failure Mode and Effect Analysis (FMEA) framework. A total of 93 distinct risk scenarios were quantitatively evaluated. Each scenario was scored based on its potential Severity (S), likelihood of Occurrence (O), and the effectiveness of existing controls for Detection (D). The resulting Risk Priority Number (RPN), calculated as RPN = S × O × D, provided a quantitative basis for prioritization.

The RPN scores for the 93 scenarios ranged from 80 to 648. Based on the predefined criticality criteria (RPN > 500 corresponding to 'High' priority), the analysis identified 19 high-priority risks requiring immediate attention, 45 medium-priority risks, and 29 low-priority risks. The high-priority risks were predominantly concentrated in areas related to human factors (e.g., lack of security awareness leading to credential theft), data security breaches (e.g., leakage of customer PII and transaction data), and weaknesses in core systems (e.g., lack of MFA and potential for logic manipulation). Table 2 presents the complete list of all 19 high-priority risk scenarios, ordered by risk code for consistency with the mitigation table.

Table 2. The 19 High-Priority Risk Scenarios Identified through FMEA

Risk Code	Risk	Potential Effect	Potential Cause	S	O	D	RPN
R.002	Leakage of high-value aggregate data.	Leakage of strategic business intelligence to competitors, damaging competitive advantage.	Ineffective implementation of procedures for handling and distributing confidential information.	9	7	9	567
R.006	Severe regulatory breach from leakage of customer PII.	Heavy financial penalties and severe reputational damage due to regulatory violations.	No monitoring procedures for accessing and managing customer PII.	9	7	9	567
R.010	Financial loss from insider manipulation of customer data.	Sabotage of the collection process and financial loss from data manipulation by insiders.	No monitoring or multi-level approval process for executing database queries.	9	7	9	567
R.014	Inaccurate contract data leading to mass complaints.	Incorrect billing to customers, leading to mass complaints and reputational damage.	Ineffective testing procedures for new contract calculation logic.	9	7	8	504

Risk Code	Risk	Potential Effect	Potential Cause	S	O	D	RPN
R.017	Leakage of customer payment patterns.	Significant financial loss due to leakage of customer payment patterns to external parties.	Ineffective procedures for handling and processing transaction data.	8	8	9	576
R.018	Heavy regulatory breach from transaction data corruption.	Severe regulatory penalties and reputational damage due to fraudulent financial transactions.	Weak authentication mechanism between the Payment Gateway and the Collection System.	10	6	9	540
R.022	Reputational damage from unintentional information disclosure.	Damage to company reputation and severe regulatory breaches from privacy violations.	Unconscious disclosure of information by agents in public due to lack of security training.	9	7	9	567
R.027	Data leakage from careless use of field devices.	Minor regulatory violations and widespread customer complaints from partial data leakage.	Ineffective and reactive monitoring of tablet usage procedures by Field Agents.	7	8	9	504
R.028	Data leakage from unintentional disclosure by field agents.	Minor regulatory violations and widespread customer complaints from partial data leakage.	Unconscious information disclosure by Field Agents in public due to lack of training.	7	8	9	504
R.030	Inaccurate operational reports due to manipulation of field visit results.	Inaccurate performance reports and customer complaints due to inappropriate collection treatment.	Ineffective monitoring procedures for field visit results, creating loopholes for manipulation.	7	9	9	567
R.041	Undetected large-scale financial fraud from insider manipulation of Collection System logic.	Massive, undetected financial losses due to manipulated system logic by insiders.	No system exists to detect anomalies in logic or configuration, audits are only reactive.	10	6	10	600
R.042	Operational paralysis from malware infection.	Paralysis of collection operations caused by malware attacking the Collection System.	No anti-malware mechanism to inspect configuration files uploaded by admins.	10	7	8	560
R.046	Internal fraud from misuse of access rights.	Internal fraud or financial data corruption due to misuse of access rights by insiders.	Granting of excessive access rights to unauthorized personnel.	8	7	9	504
R.047	Unauthorized access to customer payment history.	Unauthorized access to the complete payment history of customers.	No Multi-Factor Authentication (MFA) for accessing the Payment Information System.	9	7	9	567
R.052	Potential data leakage from compromised call center credentials.	Potential leakage of customer data displayed on the Call Center System.	Lack of security awareness refreshment training on digital credentials for call center operators.	7	9	9	567

Risk Code	Risk	Potential Effect	Potential Cause	S	O	D	RPN
R.059	Unauthorized access to field collection app.	Potential leakage of customer information from unauthorized access to the field collection app.	Weak password policy (PIN only) without a mandatory secondary password.	8	8	9	576
R.072	Financial loss from payment gateway takeover.	Massive financial loss and heavy regulatory sanctions from a takeover of the company's payment flow.	No MFA mechanism for accessing the Payment Gateway.	10	6	9	540
R.083	Credential theft of regular users.	Unauthorized access to the collection system, leading to data theft or operational disruption.	Lack of recurring security awareness training and assessment, making users vulnerable to phishing.	8	9	9	648
R.087	Data privacy violation from misuse of excessive access rights by analysts.	Undetected data manipulation or privacy violations by analysts with excessive access rights.	Granting of excessive access rights not aligned with job duties by administrators.	9	7	9	567

For all 19 risks categorized as 'High' priority, a protection strategy was developed by mapping each risk to relevant security controls from Annex A of the **ISO 27001:2022** standard. This approach ensures that the proposed mitigation actions are aligned with internationally recognized best practices. The recommended strategies aim to address the root causes of the vulnerabilities, providing PT XYZ with a clear and actionable roadmap for strengthening its information security posture, as detailed in Table 3.

Table 3. Recommended Mitigation Strategies for High-Priority Risks

Risk Code	ISO 27001:2022 Control	Recommended Action	Person in Charge (PIC)
R.002	A.8.3 - Information access restriction	Review all DWH report distribution lists and strictly enforce the need-to-know principle.	Risk Management, Collection Support
R.006	A.5.34 - Privacy and protection of PII	Develop and enforce a strict SOP for PII handling to ensure compliance with privacy regulations.	Legal & Compliance, Risk Management
R.010	A.8.16 - Monitoring activities	Implement User Activity Monitoring (UAM) to detect and generate real-time alerts for anomalous data modifications.	IT Security, Risk Management
R.014	A.8.26 - Application security requirements	Establish detailed functional and integrity requirements (e.g., calculation logic) as a formal blueprint before vendor development.	Risk Technology Business Analyst
R.017	A.5.10 - Acceptable use of assets	Define and socialize an Acceptable Use Policy (AUP) for transaction data, prohibiting sharing outside of official purposes.	Risk Management, Collection QA

Risk Code	ISO 27001:2022 Control	Recommended Action	Person in Charge (PIC)
R.018	A.8.21 - Security of network services	Implement mutual TLS (mTLS) to ensure both critical systems (S.01 & S.06) authenticate each other.	IT Department, IT Security
R.022	A.6.3 - Information security awareness	Implement a recurring security awareness program for call center staff with modules on protecting customer confidentiality.	HR, Risk Management
R.027	A.7.7 - Clear desk and clear screen	Enforce a "clear screen" policy via MDM (auto-lock) and mandate the use of privacy screen protectors on field devices.	IT Department, IT Security
R.028	A.6.3 - Information security awareness	Create a dedicated training module for field agents on information security risks when working in public spaces.	HR, Risk Management
R.030	A.8.16 - Monitoring activities	Implement unannounced, random field audits and develop an anomaly dashboard to detect unusual patterns.	Collection QA, Collection Support
R.041	A.5.36 - Compliance with policies	Mandate periodic internal audits of the Collection System to verify that all system changes comply with established policies.	Internal Audit, Risk Management
R.042	A.8.7 - Protection against malware	Ensure the vendor contract mandates the implementation and continuous updating of an advanced anti-malware solution.	IT Department, IT Security
R.046	A.8.2 - Privileged access rights	Manage privileged access by requiring a second approval (four-eyes principle) before executing functions like manual posting.	Risk Technology, Collection QA
R.047	A.8.5 - Secure authentication	Mandate and enforce the use of Two-Factor Authentication (2FA) for all access to the Payment Information System.	IT Department, IT Security
R.052	A.6.3 - Information security awareness	Integrate a cybersecurity module into the onboarding program for all new employees and conduct regular awareness campaigns.	HR, Risk Management
R.059	A.5.17 - Authentication information	Implement a strong password policy via MDM, enforcing complexity, minimum length, and periodic updates.	IT Department
R.072	A.8.5 - Secure authentication	Require 2FA for administrative access to the Payment Gateway and implement a periodic API key rotation schedule.	IT Department, IT Security
R.083	A.6.3 - Information security awareness	Make participation in security training a mandatory annual performance metric for all staff to ensure engagement.	HR, Risk Management, All Management
R.087	A.8.16 - Monitoring activities	Implement UAM on critical systems to log and analyze activities of privileged users, especially data exports or configuration changes.	IT Security, Risk Management, Internal Audit

CONCLUSION

This study successfully conducted a comprehensive information system risk analysis at PT XYZ by integrating the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode & Effect Analysis (FMEA) methods. The research

systematically identified 18 fundamental critical assets across data, software, network, and brainware categories, against which 56 contextual threats were mapped. The subsequent architectural analysis uncovered 93 underlying vulnerabilities, primarily related to procedural oversight, third-party vendor management, and personnel security awareness. The core contribution of this research is the quantification and prioritization of 93 risk scenarios. Through the FMEA assessment, the system's risk profile was clearly defined, classifying 19 risks as high-priority (RPN > 500) that require immediate intervention.

The findings provide significant practical contributions for PT XYZ. The resulting prioritized risk register and the proposed mitigation strategies, which are mapped to the ISO 27001:2022 standard, serve as an actionable roadmap for enhancing the organization's information security posture. Furthermore, this "as-is" risk analysis provides a crucial baseline that can be used as a primary input for defining robust security requirements for the company's strategic project of migrating the collection system to an in-house model. From a theoretical standpoint, this study demonstrates the effective application of a hybrid OCTAVE-FMEA framework in the financial services sector, offering a replicable case study for both academics and practitioners.

While this research achieved its objectives, it is subject to limitations, primarily its focus on a single information system within one organization. Future research could expand upon this work by applying the framework to different types of systems or industries. Further studies could also incorporate a longitudinal approach to assess the effectiveness of the implemented mitigation strategies over time or integrate quantitative threat modeling to enhance the accuracy of the 'Occurrence' scoring in the FMEA analysis.

REFERENCES

[1] Norliani, M. N. Sari, M. S. Safarudin, R. Jaya, Baharuddin, and A. R. Nugraha, “TRANSFORMASI DIGITAL DAN DAMPAKNYA PADA ORGANISASI: TINJAUAN TERHADAP IMPLEMENTASI TEKNOLOGI INFORMATIKA,” *JRPP: Jurnal Review Pendidikan dan Pengajaran*, vol. 7, no. 3, pp. 10779–10787, 2024.

[2] B. Harto *et al.*, *Transformasi Bisnis di Era Digital: Teknologi Informasi dalam Mendukung Transformasi dalam Mendukung Transformasi Bisnis di Era Digital*, 1st ed. Jambi: PT. Sonpedia Publishing Indonesia, 2023.

[3] B. Raharjo, *KEAMANAN SISTEM INFORMASI*. Semarang: Yayasan Prima Agus Teknik, 2021.

[4] Otoritas Jasa Keuangan, *PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA NOMOR 22 TAHUN 2023TENTANG PELINDUNGAN KONSUMEN DAN MASYARAKAT DI SEKTOR JASA KEUANGAN*. 2023.

[5] K. Thaung, *Advances in Intelligent and Soft Computing*. 2012. doi: 10.1007/978-3-642-25908-1.

[6] A. Alijoyo, B. Wijaya, and I. Jacob, *Failure Mode Effect Analysis*. Bandung: Center for Risk Management & Sustainability Indonesia, 2020. [Online]. Available: www.lspmks.co.id

[7] M. S. A. Setiawan, E. M. Safitri, M. A. T. Taufiqurahman, and M. A. Pratama, “Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic.id menggunakan Metode OCTAVE dan FMEA,” *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 11, no. 3, pp. 504–514, Jul. 2023, doi: 10.26418/justin.v11i3.66628.