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

Information Technology Asset Risk Management for XYZ Digital Wallet Application with ISO 3100:2018 and FMEA

Meidiana Hana Putri[1], Ghea Sekar Palupi[2]

[1]*State University of Surabaya, Surabaya, Indonesia*

meidianahana.21015@mhs.unesa.ac.id, gheapalupi@unesa.ac.id

ABSTRACT

A digital wallet application is a type of information technology service in the financial sector. This digital service relies on IT assets to support its business processes. Therefore, service providers must ensure the security and availability of these assets by analyzing potential risks. This study conducts a risk management analysis of the XYZ digital wallet application using an integrated approach based on the ISO 31000:2018 framework and the FMEA method. The process includes stages of communication and determination of analysis needs, risk assessment, risk evaluation, and risk treatment. Based on the identification of critical assets, which include hardware, software, data, and human resources, a total of 18 assets were found to support the business processes of the XYZ digital wallet application. From the risk evaluation results, five risks were identified as priorities: illegal access to personal computers and laptops, physical damage to computer components due to water spills, data leaks related to application performance, loss of user information during backup processes, and physical damage to the local cable network. As a result, risk treatment recommendations were provided to mitigate these prioritized risks.

Keyword: Risk Management, Digital Wallet, ISO 31000: 2018, FMEA, Information Technology

Article Info:
Article history:
Received June 30, 2025
Revised July 08, 2025
Accepted July 21, 2025

Corresponding Author
Meidiana Hana Putri
State University of Surabaya, Surabaya, Indonesia
meidianahana.21015@mhs.unesa.ac.id

1. INTRODUCTION

Technological advancements have driven the growth of digital services across various sectors, including the financial sector. This is evident in the continuous development of digital financial service products, particularly with the emergence of digital wallet applications that simplify financial transactions through users' mobile phones. As the demand for these digital services increases, service providers must optimize their business processes by implementing various innovations to fulfil their functions effectively, enhance profitability, and minimize potential losses. This is especially important considering that the more complex the products and activities of digital wallet services become, the higher the risks they face. Risks in digital wallet services are primarily associated with information technology. If an IT system failure occurs, the organization may be paralyzed due to the inability to access critical information or may be forced to rely on inaccurate information caused by processing errors. (Amani & Vidiyastutik, 2017). To minimize potential information technology risks, management processes must operate in accordance with the company's established standard procedures and methods. Information Technology Risk Management is the process of identifying and addressing technological threats that may impact a company or organization in achieving its

objectives. Implementing IT risk management is essential, as it enables the company to identify the risks or threats associated with the use of technology within its information systems, thereby helping to reduce the level of operational risk. (Rajjani, Hanggara, & Musityo, 2021)

Therefore, service providers need to regularly conduct information technology risk management analysis for digital wallet services. The risk management process, including systems and applications, should also be reviewed periodically to optimize its effectiveness. In this study, a risk management analysis will be carried out for the XYZ digital wallet application using the ISO 31000:2018 framework integrated with the FMEA method. ISO 31000:2018 is widely applicable across various industries. It provides a comprehensive risk management framework that offers guidance on risk identification, risk analysis, and risk evaluation. (Santosa & Palupi, 2024). In a study conducted by [1], ISO 31000:2018 was applied to analyze information technology risks following incidents of manipulation and hacking in a mobile banking application system. The analysis identified residual risks, which refer to risks that may reoccur, and these can be used as a reference for developing appropriate mitigation strategies. Meanwhile, FMEA is a methodology used to evaluate failures within a system, design, process, or service [2]. The FMEA method is employed to generate a Risk Priority Number (RPN), which translates the results of risk identification into a risk assessment matrix based on three factors: occurrence, severity, and detection. In a study by [3] on risk assessment in the development of a General Affairs Service application at service company PT XYZ, 28 risks were identified and evaluated using FMEA parameters, resulting in 3 extreme risks, 9 high risks, 5 medium risks, and 11 very low risks. The integration of ISO 31000:2018 with the FMEA method is considered an optimal approach for conducting risk management processes within an organization. According to the Risk Management document based on the Indonesian National Standard (SNI) ISO 31000, FMEA is a flexible technique that can be implemented without requiring extensive resources, while still producing accurate and reliable quantitative outputs [4].

2. METHODS

This study is qualitative research, in which data collection was conducted through interviews and observations of the research object. The framework used as a reference for the implementation of this research is ISO 31000:2018 on risk management, which is combined with the FMEA method to translate the collected data into a risk assessment matrix. ISO 31000 provides general guidelines to support risk management processes in both organizations and corporations [5]. Failure Mode and Effect Analysis, or FMEA, is a method used to identify and analyze potential failures along with their consequences [6]. This method includes an assessment component in the form of scorecards, which translate qualitative evaluations into a quantitative matrix. The steps for integrating ISO 31000:2018 with the FMEA method in conducting risk management analysis are presented in Figure 1 below:

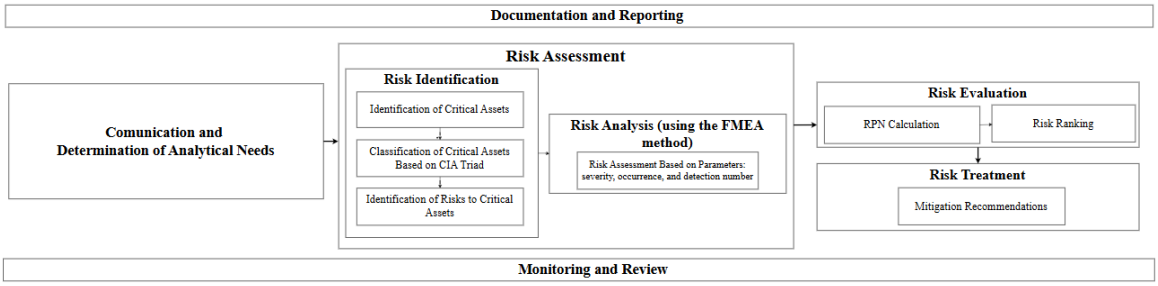

Figure 1. Flow of Research Methodology Using ISO 31000:2018 Integrated with FMEA source: Researcher

2.1. Communication and Determination of Analytical Needs

In this phase, communication will be carried out with relevant stakeholders regarding the implementation of risk management to be conducted by the researcher. This stage is defined in a RACI matrix, which serves as an output to indicate the responsibilities of each stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed. [7].

2.2. Risk Assessment Process

The risk assessment process involves several stages to obtain results for risk identification, analysis, and evaluation. The following describes the stages within the risk assessment process:

2.2.1 Risk Identification

This stage aims to produce a list of risks along with their causes and potential impacts on the organization in a qualitative format. The results of this risk identification will be used as input for the subsequent stages [4]. The risk identification process consists of the following steps:

2.2.1.1 Critical Asset Identification

In this context, the identification of critical assets focuses on understanding and assessing the information assets that are essential to the organization. This step involves examining the computing infrastructure that constitutes the organization's assets to uncover vulnerabilities in IT asset components. [8].

2.2.1.2 Classification of Critical Assets Based on the CIA Triad

Referring to the study by [9] critical assets are classified according to the CIA triad: confidentiality, integrity, and availability. The classification results will be used as input in the FMEA assessment process to consider the potential impact on the company if a risk occurs on a critical asset [9].

2.2.1.3 Risk Identification of Critical Assets

This stage involves identifying possible failure modes that may occur throughout the processes, based on an examination of each process step or procedure related to the company's product or service delivery [10].

2.2.2 Risk Analysis

Risk analysis provides input for risk evaluation, decisions on how risks should be treated, and the most appropriate risk treatment strategies and methods. At this stage, risk assessment will be carried out using the parameters provided in the FMEA method.

2.2.2.1 Risk Assessment Based on Parameters

This step measures the potential for failure using three components: severity, occurrence, and detection, each rated on a scale from 1 to 10.

2.3. Risk Evaluation

3.3.1 RPN Calculation

The next step, after determining the values for severity, occurrence, and detection, is to calculate the Risk Priority Number (RPN) by multiplying the scores of each criterion: Severity

(S) × Occurrence (O) × Detection (D). Risks with high RPN values will be prioritized for mitigation.

2.4. Risk Treatment

2.5.1 Mitigation Recommendations

This stage aims to find solution approaches to reduce the likelihood and impact of risks on the organization [11].

3. RESULTS AND DISCUSSION

This study analyses information technology asset risk management in the XYZ digital wallet application by integrating the ISO 31000:2018 framework with the FMEA method. Risk identification is conducted on the information technology assets used to support the business processes of the digital wallet application.

3.1 Communication and Determination of Analysis Requirements

As outlined in the methodology section, communication and consultation are conducted to clarify the roles and responsibilities of each stakeholder in the risk management process (Zulvikri & Mukaram, 2024). The RACI matrix is used to assign different types of tasks to the team members involved. After successfully identifying the roles and responsibilities of each stakeholder, mapping can be used to determine which parties should be the target for data collection and observation in the next phase. Based on the mapping results and the RACI analysis, it was found that the digital wallet service provider company XYZ collaborates with an IT service provider to support the application's business processes.

The involvement of the vendor in the risk management process of the XYZ digital wallet application is not limited to technical implementation but also includes active participation in the implementation and monitoring of risks. This indicates that the vendor is categorized as part of the company’s assets, particularly in the form of human resources directly involved in the risk cycle. Therefore, even though parts of the business process are delegated, the responsibility for risk management remains under the internal supervision of the company, and the vendor must be integrated into the risk management system in accordance with the established agreement. After successfully identifying the roles and responsibilities of each stakeholder, the mapping can be used to determine which parties should be the focus of data collection and observation for the next stage.

3.2 Risk Assessment

Several identification stages are required for risk assessment in order to develop the necessary risk register. The results of the identification process are obtained through data collection and observation, based on RACI-based responsibility mapping of each stakeholder.

3.2.1 Critical Asset Identification

The technology components that support business processes are categorized based on their type, including hardware components, software components, data and information, and human resources who serve as stakeholders. This classification is intended to help the organization identify potential risks that may impact those assets [12] [13]. According to [14], Companies may outsource some of their business processes to third parties to improve efficiency and effectiveness while transferring certain risks. However, they must still manage the risks that arise as a result of such transfers. Third parties or vendors are therefore

categorised as human resource assets, as the services they provide are bound by contractual agreements. The results of the critical asset identification for the XYZ digital wallet application are presented in Table 1.

Table 1 Critical Asset Identification Source: Researcher

Code Asset	Asset Name	Category Asset	Code Asset	Asset Name	Category Asset
A1	Server	Hardware	**A10**	Website Helpdesk	Software
A2	Personal Computer	Hardware	**A11**	System Linux Operations	Software
A3	Mobile Phone	Hardware	**A12**	Information user	Data
A4	CCTV	Hardware	**A13**	Merchant and Partner Data	Data
A5	Laptop	Hardware	**A14**	Application Performance Information	Data
A6	Hard disk External	Hardware	**A15**	Internet Network	Network
A7	Switch	Hardware	**A16**	Cable Network	Network
A8	Router	Hardware	**A17**	IT Staff	Human Resources
A9	Website Monitoring	Software	**A18**	Vendor	Human Resources

Based on the critical asset identification process, the asset inventory includes 8 hardware components, 2 software components, 3 types of data, 2 types of networks, and 2 crucial human resources that support the business processes of the XYZ application. Each of these assets will be classified according to its level of urgency using the CIA triad parameters, which assess the importance of confidentiality, integrity, and availability.

3.2.2 Classification of Critical Assets Based on the CIA Triad

According to the study conducted by [9] on FMEA assessment, critical assets should be classified based on the CIA triad, with asset categories defined as follows:

1) Class A: Failure of the information asset is highly critical and will result in complete service disruption.
2) Class B : Failure of the information asset will cause minor service disruptions.
3) Class C : Failure of the information asset will lead to inconvenience for staff or customers.

Based on these parameters, the classification results of critical assets for each asset involved in the business processes of the XYZ digital wallet application are presented in Table 2 below:

Table 2 Critical Asset Classification Source: Researcher

Asset Name	Class	Total
Server, Website Monitoring, User Information, Merchant and Partner Data, Application Performance Information, Internet Network	A	6
PC, CCTV, Laptop, Hard Disk, Switch, Wifi Router, Helpdesk Website.	B	7
Mobile Phone, Linux Operating System, LAN Network	C	3

Classification of critical assets based on the CIA triad supports the impact assessment process in the event of a risk occurring. The higher the classification level, the greater the assigned impact score.

3.2.3 Risk Identification

Once the critical assets have been identified, the next step is to assess the potential risks. This is done by outlining possible failure modes and their potential impact on business processes. The results of the risk identification exercise for the XYZ digital wallet application are presented in Table 3 below:

Table 3 Risk Register XYZ Digital Wallet Application Source: Researcher

Asset Code	Asset Name	Class	Risk	Risk Code
A1	Server	A	Physical damage to the server	**R1**
			Overheat	**R2**
			Overload	**R3**
			Misconfiguration of root user access	**R4**
			Vulnerability of nature and location	**R5**
A2	Personal Computer	B	Missing Data	**R6**
			Illegal access	**R7**
			Physical components are damaged	**R8**
A3	CCTV	B	Unable to detect activity	**R9**
			Device malfunction	**R10**
A4	Mobile Phone	C	Device Malfunction	**R11**
			Lost device	**R12**
A5	Laptop	B	Physical components are damaged	**R13**
			Illegal access	**R14**
A6	Hard disk External	A	Missing Data	**R15**
A7	Switch	B	Overheat	**R16**
			Physical damage	**R17**
A8	Wifi Router	B	Overheat	**R18**
			Physical damage	**R19**
A9	Website Monitoring	A	Downtime	**R20**
A10	Website Helpdesk	B	Downtime	**R21**
			Overload	**R22**
A11	Linux Operating System	C	Malware attack	**R23**
A12	User information	A	Data input error	**R24**
			Data missing	**R25**
A13	Merchant and Partner Data	A	Data input error	**R26**
A1 4	Application performance information	A	Data leakage	**R27**
A15	Internet Network	A	Network Disruption	**R28**
A16	LAN and WAN networks	C	Device malfunction	**R29**
A17	IT Staff		Human error	**R30**
A18	Vendor		Vendors locking	**R31**

3.4 Risk Analysis

3.4.1 Risk Assessment Based on Parameters

Risk assessment is based on the impact, potential causes, and detectability, which together produce the Risk Priority Number (RPN) for the XYZ digital wallet application. The assessment results are presented in Table 4 below:

Table 4 Risk Assessment using FMEA method Source: Researcher

Risk Code	Risk	Impact	S	Causes of Failure	O	Current detection	D	RPN
R1	Physical damage to the server	Server not working	8	Devices exposed to water vapor from split AC	7	Regular AC checks every month	2	**112**
R2	Overheat on the server	Server gets hot	7	AC malfunction in data center	4	Regular AC checks each month	2	**56**
R3	Server overload	Server downtime	7	Server capacity was full	2	There is a notification performance on telegram	2	**28**
R4	Error configuring root server user access	Changes configuration illegal	8	Brute force login	4	Firewall installation and monitoring	2	**64**
R5	Natural vulnerability and location of data center	Asset damage	9	Natural disaster-prone location	4	Disaster related alarms	2	**72**
R6	PC data lost	Data not saved	6	Storage was full	2	Using external storage	5	**60**
R7	Illegal access to PC	The existence of fraud	9	Password leaked	7	Updating the password	7	**441**
R8	Damaged PC components	Device cannot be used	6	Dust and age device	2	Maintenance device periodically	2	**24**
R9	CCTV cannot detect activity	Activity not recorded in blind spots	9	Presence of dangerous blind spots	1	Regular monitoring and security guards	3	**27**
R10	CCTV malfunction	Device cannot be used	7	Inadequate maintenance	2	Device replacement or repair	4	**56**
R11	Damage Mobile phone devices	Device cannot operate	7	Inadequate maintenance	3	Device replacement or repair	4	**84**
R12	Mobile Phone Lost	Business process are constrained	9	Assets are not in place	2	Storage in a safe place	3	**54**
R13	The physical Component of the laptop are damaged	Device inoperable	6	Exposed to water spills	8	Do not bring liquids into the working space	7	**336**
R14	Illegal access to laptop	Data loss	9	Password leak	7	Updating password	7	**441**
R15	Hard disk data Lost	Data cannot be used	7	Storage was full	2	Data storage management in partitions	4	**56**
R16	Overheat Switch	Device inoperable	6	Damage to the AC	2	Checking AC condition	2	**24**
R17	Physical damage to switch	Device inoperable	6	Inadequate maintenance	2	Cleaning and maintenance device	2	**24**
R18	Router Overheat	Device inoperable	6	Poor air circulation	2	Controlling room temperature	4	**48**

Risk Code	Risk	Impact	S	Causes of Failure	O	Current detection	D	RPN
R19	Router is broken	Device inoperable	6	Dust and age device	2	Replacement or maintenance the device	2	**24**
R20	Downtime on Website Monitoring	Business process will be disturbed	8	DDoS Attack	2	Using a load balancer	3	**48**
R21	Downtime on Website helpdesk	Business process will be disturbed	8	Problems with the internet network	2	Waiting for the network to recover	5	**80**
R22	Overload on website helpdesk	Business process will be disturbed	8	Surge in activity traffic	2	Using a load balancer	3	**48**
R23	Malware attacks on linux operating systems	Business processes bottlenecks	8	Security system is not updated	2	There is a built - in firewall that has been installed	3	**48**
R24	User data input error	Transaction process cannot be carried out	8	Human error	4	Rechecking the data that has been entered	3	**96**
R25	User data lost	Data cannot be used	9	Data corrupted during backup process	2	Checking back	7	**126**
R26	Leaked app performance data	Business and reputation loss	9	Malware	4	Using antivirus and firewall	5	**180**
R27	Internet Network Disruption	Business process are hampered	7	Provider network disruption	2	Waiting for the network to be recover	5	**70**
R28	Cable device malfunction	Business process hampered	7	Lack of cable maintenance	5	Arranging the cable network for safety	5	**175**
R29	Human error of IT staff	Business losses	8	Intentional or unintentional human error	4	Implementing SOP and policy	2	**64**
R30	Vendor Locking	Over budgeting	5	Business process transfer excessive	2	Re-evaluating the business needs	5	**50**

3.5 Risk Evaluation

By using the RPN, the organization can determine the priority order for addressing the identified risks. A higher RPN value indicates a more critical risk that should be addressed first. Table 5 presents the ranking of risks that were previously analysed.

Table 5 Risk Evaluation Source: Reascher

Risk Code	Risk	RPN	Risk Code	Risk	RPN
R7	Illegal access to PC	**441**	**R2**	Overheat on the server	**56**
R14	Illegal access to laptop	**441**	**R10**	CCTV malfunction	**56**
R13	The physical Component of the laptop are damaged	**336**	**R15**	Hard disk data Lost	**56**
R26	Leaked app performance data	**180**	**R12**	Mobile Phone Lost	**54**
R28	Cable device malfunction	**175**	**R30**	Vendor Locking	**50**
R25	User data lost	**126**	**R18**	Router Overheat	**48**

Risk Code	Risk	RPN	Risk Code	Risk	RPN
R1	Physical damage to the server	**112**	**R20**	Downtime on Website Monitoring	**48**
R24	User data input error	**96**	**R22**	Overload on website helpdesk	**48**
R11	Damage Mobile phone devices	**84**	**R23**	Malware attacks on linux operating systems	**48**
R21	Downtime on Website helpdesk	**80**	**R3**	Server overload	**28**
R5	Natural vulnerability and location of data center	**72**	**R9**	CCTV cannot detect activity	**27**
R27	Internet Network Disruption	**70**	**R8**	Damaged PC components	**24**
R4	Error configuring root server user access	**64**	**R16**	Overheat Switch	**24**
R29	Human error of IT staff	**64**	**R17**	Physical damage to switch	**24**
R6	PC data lost	**60**	**R19**	Router is broken	**24**

At the risk evaluation stage, the results of the risk ranking were obtained and mapped, as shown in Figure 2 below.

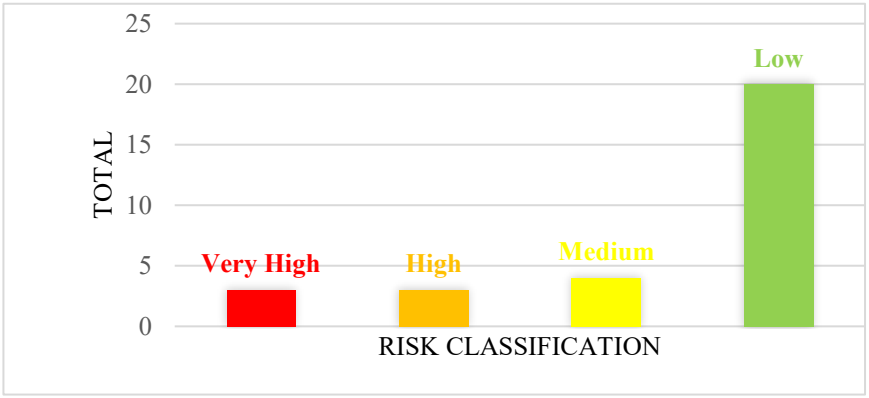

Figure 2 Risk Classification Diagram source: researcher

As can be seen from the risk mapping results, most of the risks have relatively low scores due to the sufficient detection and prevention measures in place. However, several risks still have very high or high scores and must be prioritised for treatment.

3.6 Risk Treatment

Risk treatment may involve mitigation actions. The mitigation strategies in this study are based on IT risks categorized as very high (RPN ≥ 200) and high (RPN: 120–199), assuming that if these risks were to materialize, they would significantly disrupt critical business processes within the XYZ digital financial application. Risk mitigation strategies are classified into four standard options: risk avoidance, risk limitation, risk transference, and risk acceptance [14]. There are five IT risks identified for mitigation, as they fall into the very high or high categories and have the potential to disrupt critical business processes in the XYZ digital wallet application. These risks are:

1. Illegal access to PCs and laptops
2. Physical damage to PC and laptop components due to water spills
3. Data leakage related to application performance
4. Loss of user information (data corruption) during backup processes
5. Physical damage to LAN cable network

The mitigation recommendations for these risks are presented in Table 6 below:

Table 6 Risk Mitigation Recommendation Source: Researcher

Risk Code	Mitigation Steps	References
R7, R14	Password Management includes: 1. Users are required to change their passwords after initial registration. 2. Passwords must be unique and difficult to guess. They should not be based on personal information or common word patterns, and should include alphanumeric or special characters. 3. Users must keep their passwords confidential and change them immediately if they become compromised. 4. Previously used passwords cannot be reused. 5. Passwords must not be displayed on the screen during registration.	[15] 5.7 Authentication Information [16] Control 5.15 Access Control, 5.17 Authentication Information, 5.18 Access Rights
R13	Guidelines for Bringing Liquids into the Work Area includes: 1. Prohibiting the bringing of liquids in open containers into the work area. 2. Only allowing beverages in tightly closed bottles. 3. Prohibiting any form of liquid in sensitive work areas (such as server rooms and important archive storage rooms). 4. Providing written warnings and advisories against placing or bringing liquids in open containers arbitrarily within the work area.	[17] 6.1.12 Hazard Identification and Risk Assessment [16] A.1.7 Physical Security of IT Assets [15] 7.8 Equipment Siting and Protection
R26	Data Leakage Protection and Prevention Measures: 1. Restricting application access rights for unauthorized users. 2. Configuring firewalls to protect against malicious websites. 3. Regularly updating malware detection and repair software. 4. Scanning data before used it 5. Limiting the number of users with administrator-level privileges. 6. Removing inactive or unused user accounts. 7. Restricting access to high-utility programs. 8. Setting application time-out intervals. 9. Implementing additional security authentication, such as two-factor authentication. 10. Applying encryption and access control during the data backup process.	[15] 8 Control 8.7 Protection Against Malware, 8.9 Configuration Management, 8.12 Data Leakage Prevention
R28	Preventing Data Corruption During Backup Includes: 1. Performing regular data backups [18] 2. Using differential or incremental backup techniques [18] 3. Implementing automated backup protocols using heartbeat mechanisms and the rsync (Remote Sync) application for automated data mirroring between systems. [19] 4. Scheduling automatic backups using cronjob to perform routine backups at predefined times. [19] 5. Performing offsite data replication using available storage utilities to create more secure copies of critical data, ensuring recovery is possible in the event of damage to the main system. [20]	[18] [19] [20]
R25	1. Placing power and telecommunication cables related to information transmission infrastructure underground or within protective enclosures.	[15] 7.12 Cabling Security

Risk Code	Mitigation Steps	References
	2. Using armored pipes as an additional protective layer for cables. 3. Providing cable location markers to minimize unintentional damage due to lack of awareness. 4. Installing locked boxes and alarms at inspection and termination points. 5. Using electromagnetic shielding to protect the cables. 6. Utilizing fiber optics and alternative routing. 7. Conducting regular and controlled access inspections for patch panels.	

CONCLUSION

This study successfully identified risks to the information technology assets of the XYZ e-money application using the ISO 31000:2018 framework and the FMEA method. Two risks were found at a very high level and three at a high level, including device damage due to liquid spills, password leakage, malware attacks, data corruption during the backup process, and physical network damage. The recommended mitigation strategies include risk mitigation steps, a backup plan, and a recovery plan to ensure the continuity of application operations.

The result focused on analysing risks related to information technology assets, which are a key component in supporting the application's performance. To complement this research, future studies are recommended to analyse the risks arising from business processes, considering that these processes play a crucial role in determining service effectiveness, operational efficiency, and compliance with policies and regulations. By combining both aspects, risk management can be carried out more comprehensively and holistically.

REFERENCES

[1] P. Pratama and M. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *Jurnal Telematika,* 2020.

[2] H. Pribadi and Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," *Jurnal Sistem Informasi Bisnis Universitas Diponegoro,* 2020.

[3] A. Sofianingtias and M. Prasetya, "Analisis Penilaian Risiko Pengembangan Aplikasi GA Service Menggunakan Failure Mode and Effect Analysis(FMEA) (Studi Kasus Perusahaan Jasa PT XYZ)," *Owner: Riset & Jurnal Akuntansi,* pp. 2116-2126, 2024.

[4] ISO, BSI ISO 31000:2018 Second Edition, 2018.

[5] F. D. Y. Hardiyanto, "MANAJEMEN RISIKO TI ISO 31000 DENGAN COBIT 5 DAN FMEA (PT. XYZ)," *Jurnal Sistem Informasi dan Tenologi SITECH,* 2021.

[6] N. Najwa, "ANALISIS KONSISTENSI HASIL RISIKO TEKNOLOGI INFORMASI FAILURE MODE AND EFFECT ANALYSIS (FMEA).," *Repository ITS,* 2018.

[7] M. Zulvikri and M. Mukaram, "Optimalisasi Pengawasan Kinerja Karyawan Business Consultant PT XYZ : Implementasi Sistem RACI Melalui Project Google Spreadsheet," *Jurnal Riset Manajemen,* pp. 197-207, 2024.

[8] G. Juniati, Ilhamsyah and F. Ferdy, "ANALISIS, EVALUASI, DAN MITIGASI RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE DAN FMEA (STUDI KASUS: UNIT PENGELOLA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI UNIVERSITAS XYZ)," *URNAL KHATULISTIWA INFORMATIKA,* 2021.

[9] L. Lai and K. Chin, "Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security," *ndustrial Engineering & Management Systems City University of Hong Kong,* 2014.

[10] A. Alijoyo, B. Wijaya and I. Jacob, "content: lspmks," 2020. [Online]. Available: https://lspmks.co.id/wp-content/uploads/2020/06/Failure-Modes-and-Effects-Analysis.pdf.

[11] I. GRC, "Artikel, Risk: GRC Indonesia," 2023. [Online]. Available: https://grc-indonesia.com/mengenal-mitigasi-risiko-pengertian-tujuan-jenis-contoh-dan-perencanaannya/.

[12] M. Fachrezi, "Manajemen risiko keamanan aset teknologi informasi menggunakan iso 31000:2018 diskominfo kota salatiga.," *Jatisi (Jurnal Teknik Informatika Dan Sistem Informasi),* pp. 764-773, 2021.

[13] H. Mamuaja and A. Cahyono, "Siolga information technology risk management analysis using iso 31000," *Journal of Information Systems and Informatics,* pp. 57-67, 2024.

[14] S. Snedaker and C. Rima, Business Continuity and Disaster Recovery Planning for IT Professionals, Waltham, United States of America: Elsevier, 2014.

[15] ISO27002, Information security, cybersecurity and privacy protection — Information security control, 2022.

[16] ISO27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, 2022.

[17] ISO45001, Occupational health and safety management systems, 2018.

[18] y. Raharjo and A. Girsang, "Performance Tuning for Optimal Backup Process on Database Server," *International Journal of Advanced Trends in Computer Science and Engineering,* 2020.

[19] W. Yuliono and A. Prihanto, "Sinergi Replikasi Server dan Sistem Failover pada Database Serveruntuk Mereduksi Downtime Disaster Recovery Planing (DRP)," *Journal of Informatics and Computer Science Universitas Negeri Suravaya,* 2021.

[20] U. Shoaib, "Fast Data Access through Nearest Location-BasedReplica Placement," *Hindawi, Science programming,* 2022.

[21] D. S. Santosa and G. Palupi, "ANALYSIS OF RISK MANAGEMENT IN THE IMPLEMENTATION OF ENTERPRISE RESOURCE PLANNING (ERP) USING THE

FMEA METHOD AT PT XYZ," *Journal of Emerging Information System and Business Intelligence (JEISBI),* 2024.

[22] A. Folorunso, V. Mohammed, I. U. Wada and B. J. & Samuel, "The impact of iso security standards on enhancing cybersecurity posture in organizations.," *World Journal of Advanced Research and Reviews,* 2024.

[23] M. Čička, R. Turisová and D. Čičková, "Risk assessment using the pfda-fmea integrated method. Quality Innovation Prosperity," *Quality Innovation Prosperity,* 2022.

[24] M. Cho, M. Son, C. Muller and P. Fernandez, "A New Framework for Defining Realistic SLAs:An Evidence-Based Approach," in *Conference Paper in Lecture Notes in Business Information Processing* , 2017.