DOI: https://doi.org/10.33197/justinfo.vol1.iss2.2023.1745 ISSN: 3031-3449

Payment and Transaction Risk Management at Coffeeshop X Using NIST 800-30 Framework

[1]Noven Wirlando Marbun, [2]Faris Asasul Iz, [3]Muhammad Ramadhan, [4]Lorrida Jein Herlina Kogoya, [5]Lazuardi Fahreza Nugraha, [6]Ucu Nugraha

[1]Sistem Informasi, FakultasTeknik, Universitas Widyatama, Bandung, Indonesia, noven.marbun@widyatama.ac.id
[2]Sistem Informasi, FakultasTeknik, Universitas Widyatama, Bandung, Indonesia, asasul.iz@widyatama.ac.id
[3]Sistem Informasi, FakultasTeknik, Universitas Widyatama, Bandung, Indonesia, ramadhan.2983@widyatama.ac.id
[4]Sistem Informasi, FakultasTeknik, Universitas Widyatama, Bandung, Indonesia, lorrida.kogoya@widyatama.ac.id
[5]Sistem Informasi, FakultasTeknik, Universitas Widyatama, Bandung, Indonesia, lazuardi.fahreza@widyatama.ac.id
[6]Sistem Informasi, Fakultas Teknik, Universitas Widyatama, Bandung, Indonesia, ucu.nugraha@widyatama.ac.id

ABSTRACT

Information technology enables efficient and effective completion of activities, saving both time and energy. However, this convenience comes with inherent risks that need to be managed to prevent severe consequences such as information leaks, financial losses, and disruptions to business processes. This research focuses on implementing the NIST 800-30 framework as a risk management framework for Coffeeshop X. The objective is to provide concrete steps and recommendations for mitigating potential risks. The analysis identifies several risks that could threaten the business continuity of Coffeeshop X, including natural disasters, operating system vulnerabilities, physical security breaches, and damage to software and hardware. By applying the NIST 800-30 framework, the research highlights specific control measures necessary for Coffeeshop X to mitigate these risks. These measures aim to reduce the likelihood and impact of such events, ensuring that business activities can proceed smoothly and securely. The study's findings underscore the importance of a robust risk management strategy to safeguard the operations of Coffeeshop X and maintain its business continuity.

Keywords: Technology Information, Risk Management, NIST 800-30 Framework, Operating System Security, Coffeshop.

Corresponding Author:

Ucu Nugraha
Sistem Informasi, Fakultas Teknik, Universitas Widyatama
Bandung, Indonesia
ucu.nugraha@widyatama.ac.id

INTRODUCTION

Currently, almost all information is conveyed and stored in information system technology, such as menu information, discount information, and transaction data. This technology makes various activities easier so that they can be carried out efficiently and effectively, without requiring a lot of energy and time[1]. However, behind this convenience, there is a serious threat. Information technology stores various transactions, information, and personal data that can be misused by irresponsible parties. Many people are still unaware of this threat, so they often ignore risk management analysis from the start[2].

Ignoring risk management analysis not only affects the security of information systems, but can also cause fatal losses such as information leaks, financial losses, and disruption to business processes. Companies that do not implement information technology risk management analysis will face difficulties and the potential for large losses. Therefore, risk management analysis is very important in the use of information technology[3].

This research aims to analyze the security and information system architecture at Coffeeshop X using the NIST 800-30 framework. The aim is to mitigate information system risks and provide recommendations for Coffeeshop X. This study explores the application of the NIST 800-30 Method in the context of Coffeeshop Coffeeshop X, with active transactions, faces information security risks such as cyber threats, data leaks, and system instability[4].

This research aims to investigate concrete steps to use the NIST 800-30 Method as a risk management recommendation for Coffeeshop X to reduce the risks associated with their payment systems. Payment and transaction risks not only affect the operational reliability of a business but can also have a serious impact on customer reputation and trust. Therefore, understanding how Coffeeshop This research is expected to contribute to the theoretical understanding of risk management in the context of payments and transactions, as well as practical guidance for improving the security and reliability of payment systems in similar businesses.

LITERATURE REVIEW

Risk

Risk is an essential concept in management, finance, technology, and various other fields. This term refers to the potential for loss or negative impact due to an undesirable event. Risk assessment, which involves identifying, evaluating, and managing existing risks, has become important in making effective decisions in various aspects of life and business. In management literature, risks are often classified by source or type. Financial risks relate to the possibility of financial loss due to changes in asset values, market fluctuations, or economic uncertainty. Meanwhile, operational risk relates to risks from the organization's internal processes, such as human error, system failure, or lack of operational procedures[5].

Risk management

Risk management has become a very important aspect in various fields such as finance, business, technology, health, environment, and others. This concept focuses on identifying, assessing, and managing risks associated with the activities or operations of an entity. In management literature, risks can be categorized into several types, including financial, operational, reputational, and strategic risks. The importance of risk management is increasing along with the dynamic changes in the business environment and the complexity of the challenges faced by modern organizations. Organizations face a variety of risks that can interfere with achieving their goals, including financial risks related to market fluctuations, operational risks related to human error or system failures, as well as reputation risks that can affect public image and trust[6].

Threat

The threat is an important concept in various fields, especially in the context of security, risk management, and policy. A threat can be identified as the possibility or potential of an event occurring that could disrupt or damage a particular system, entity, or environment. In security literature, threats are often classified into different types, such as cyber security threats, physical threats, environmental threats, and others[7]. Cyber security threats are threats related to information and communication technology, which include malware attacks, hacking, DDoS attacks, data theft, and other criminal activities based on technology[8].

NIST 800-30

The NIST 800-30 method is a framework issued by the National Institute of Standards and Technology (NIST) in the United States. This framework is designed to help organizations manage information security risks effectively. The NIST 800-30 method offers a systematic and structured approach to identifying, evaluating, and managing information security risks. This framework consists of a series of steps that include risk identification, risk analysis, and risk assessment and response[9].

The first step in the NIST 800-30 Method is the identification of information assets and determining their importance to the organization. Next, an assessment is carried out of potential threats that could threaten these assets. This process involves identifying the source of the threat, the vulnerabilities that may be exploited, and the possible impact[10].

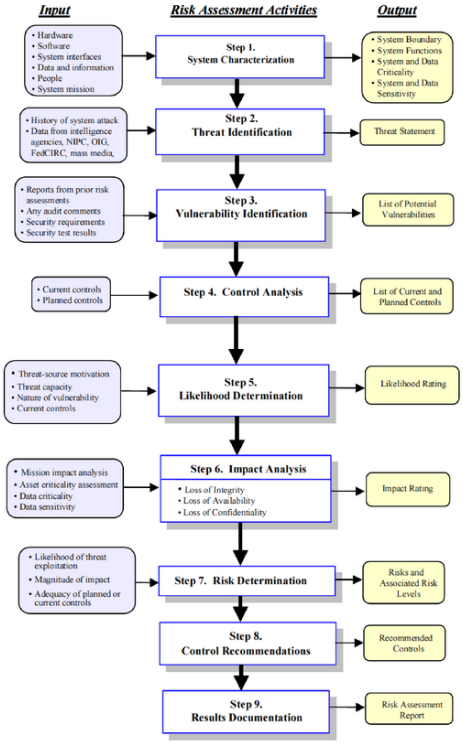

Figure 1. NIST 800-30 Framework

After threat identification, a risk analysis is carried out which involves assessing the likelihood of the threat occurring and its impact. This stage helps in classifying risks into different priority levels according to their probability of occurrence and impact on the organization. The final step in NIST Method 800-30 is the development of a risk response strategy. This includes selecting appropriate risk mitigation methods, whether by reducing the risk, transferring the risk, accepting the risk, or avoiding the risk completely. Academic research and practical implementation of the NIST 800-30 Method have demonstrated its effectiveness in helping organizations manage information security risks. Its use has attracted attention in various industries due to its structured and comprehensive approach[11].

METHODOLOGY

This research focuses on risk analysis and management in the payment and transaction system at Coffeeshop X using the NIST 800-30 method. This research uses a case study approach with qualitative and quantitative methods to gain an in-depth and comprehensive understanding of existing risks and appropriate mitigation strategies. This research was designed as a case study to understand in depth the research subject, namely Coffeeshop X, with special emphasis on risk management in the payment and transaction process[12].

Data collection was carried out through in-depth interviews with the owner, manager, IT staff, and cashier of Coffeeshop X. This interview aimed to identify risks, understand existing procedures, and evaluate awareness of information security risks. In addition, direct observation of payment and transaction processes is also carried out to assess physical and operational security, as well as compliance with established procedures[13].

Document analysis is also an important part of this research, where information security policies, security incident records, financial reports, and IT system audit results are analyzed to understand existing policies and procedures and evaluate incidents that have occurred. Apart from that, a

questionnaire was also used to collect data from Coffeeshop X customers to assess customer perceptions and trust in the security of payment and transaction systems.

Risk identification is carried out using data collected from interviews, observations, and document analysis to identify valuable information assets and determine potential threats and existing vulnerabilities. Risk evaluation is carried out using qualitative and quantitative methods to assess the likelihood and impact of identified risks and classify risks based on priority levels. Risk management is then carried out by developing mitigation strategies based on the results of risk evaluation, as well as determining specific steps to reduce, transfer, accept, or avoid these risks.

Implementation of the NIST 800-30 method is carried out by identifying all information assets relevant to the payment and transaction system at Coffeeshop Potential threats that could impact information assets are noted and vulnerabilities that could be exploited by those threats are identified. Risk analysis is carried out by assessing the likelihood of each threat occurring and its impact on the organization, using a risk matrix to classify risks based on probability and impact. Risk response strategies are then developed and implemented to reduce the risk (mitigation), transfer the risk (for example, with insurance), accept the risk (if the impact is minimal), or avoid the risk (stop high-risk activities).

Evaluation of the effectiveness of the mitigation strategies that have been implemented is carried out through internal audits and feedback from staff and customers. The research results are then reported, including key findings, risk analysis, mitigation strategies, and recommendations for further improvement.

RESULTS AND DISCUSSION

System Characterization

In the context of Coffeeshop X, System Characterization aims to identify and document the critical elements that make up the payment and transaction infrastructure. The systems involved can be divided into two main categories:

1) Hardware System. EDC (Electronic Data Capture) machine used to process credit and debit card payments. Server that stores transaction data and customer information. Internet and local network (LAN) connections that support communication between payment terminals, servers, and other systems. Firewalls, routers, and other devices that protect networks from unauthorized access.
2) Software System. Software that runs on payment terminals and processes transactions. Software that manages transaction and customer data. Security software that protects systems from cyber attacks. Software that performs regular data backups to prevent data loss.

Threat Identification

It can be seen in Table 1, identify the threats that Coffeeshop X may face along with examples and consequences.

Table 1. Threat Identification

No	Threat Type	Examples of Threats	Consequences of Threats
1	Natural disasters	Landslides, Floods, Lightning	Can damage hardware facilities
2	Human Error	Incorrect Software Operation	Software does not obtain valid data and information
3	System Error	Sistem tidak berjalan, Data Corrupt	Software cannot operate

Further explanation of these threats:

1) Natural disasters
   a) Landslide. Can cause physical damage to buildings and the hardware within them.

b) Flood. Can damage electronic devices and cause system failure.
c) Lightning. Can cause electrical surges that damage hardware and networks.

2) Human Error
   a) Incorrect software operation. Errors in using the software can result in invalid data or loss of important data.
   b) User Negligence. Users may fail to update security software or perform backup procedures, increasing the risk of vulnerabilities.
   c) Errors in the System. System Not Running: A major system failure can halt entire business operations.
   d) Corrupt Data. Data corruption can result in the loss of important information and difficulty in recovering transactions.

Identifying and mitigating these threats is important to ensure continued operations and data security at Coffeeshop X.

Vulnerability Identification

Table 2 is a Vulnerability Identification that lists the risks, impacts, and examples of related problems in the MokaPOS environment:

Table 2. Vulnerability Identification

No	Risk	Impact	Examples of Related Problems
1	Hardware Damage	Physical damage to MokaPOS hardware, such as payment terminals, receipt printers, or other devices, may disrupt daily operations.	The payment terminal was damaged due to a water leak or heavy fall.
2	Device Dependency	Over-reliance on a single piece of hardware can increase the risk of system failure if that device is damaged or compromised.	All transactions were disrupted due to damage to the only transaction server.
3	Vulnerability to Theft or Manipulation	Unprotected hardware or lack of physical security systems on devices such as payment terminals can increase the risk of data theft or manipulation.	Customer information is stolen through poorly guarded physical access.
4	Operating System Security Vulnerabilities	If the operating system used on a MokaPOS device is not updated regularly or has unpatched security vulnerabilities, it could provide an opening for malware attacks.	Delayed operating system updates lead to security gaps that are exploited by malware.
5	MokaPOS Application Vulnerability	Flaws or vulnerabilities in the MokaPOS application itself, such as bugs or security gaps, can be a serious problem that allows unauthorized access or data theft.	Theft of customer data through security gaps in the MokaPOS application.
6	Network and Communications Vulnerabilities	If communications between MokaPOS devices and servers or other networks are not properly encrypted, this may increase the risk of hacking or data interception.	Interception of transaction data due to unprotected communications on public Wi-Fi networks.
7	Unnecessary Access Levels	If access rights to MokaPOS devices are granted excessively to users, this may increase security risks if sensitive information or functionality is exposed.	Users with admin access can access and manipulate data that they should not see.

Table 2 can help identify potential security and operational issues that could affect the payment and transaction system at Coffeeshop using MokaPOS. Mitigation measures should be considered to reduce identified risks.

Control Analysis

The following is a control analysis for each risk identified in the MokaPOS system at Coffeeshop X. Table 3 explains the controls that can be implemented to reduce or eliminate existing risks.

Table 3. Control Analysis

No	Risk	Control
1	Hardware Damage	Carry out routine control of the physical and operational condition of hardware, including periodic inspections and preventative maintenance.
2	Operating System Security Vulnerabilities	Regularly update the operating system to address known security vulnerabilities. Make sure the latest patches and updates are always applied.
3	Vulnerability to Theft or Manipulation	Monitoring using CCTV and other physical security systems to prevent data theft and manipulation. Make sure CCTV cameras are installed in strategic areas and connected to a centralized surveillance system.
4	MokaPOS Application Vulnerability	Update the application regularly to reduce bugs and close security gaps. Perform regular software patching and updates according to developer directions.
5	Network and Communications Vulnerabilities	Save Wi-Fi routes or configurations in places that have a strong and stable signal. Use WPA3 encryption to secure your Wi-Fi network and avoid using public networks for sensitive transactions.
6	Unnecessary Access Levels	Limiting user access rights based on the principle of least privilege (only the access rights required for the respective task). Perform regular access audits to ensure there is no inappropriate access.

Based on Table 3, it can be explained as follows:

1) Hardware damage. Be sure to perform regular checks on the hardware, including checking cables, connectors, and other devices to detect potential problems early.
2) Operating System Security Vulnerabilities. Make sure to follow the operating system vendor's security update policy and perform automatic updates whenever possible.
3) Susceptibility to Theft or Manipulation. The use of CCTV and other security systems can help in identifying and preventing suspicious activity. Make sure the CCTV camera is installed properly and can record with adequate resolution.
4) MokaPOS Application Vulnerability. Regularly updating applications will reduce the risk of vulnerabilities that can be exploited by irresponsible parties. Make sure to back up your data before updating.
5) Network and Communication Vulnerabilities. Storing network configurations in a safe place and using strong encryption are important steps to protect data communications. Consider using a VPN to secure data communications between devices.
6) Unnecessary Access Levels. Properly setting access rights based on user needs can reduce the risk of access abuse. Periodically audit access to ensure that only authorized users have access to sensitive information.

By implementing these controls, Coffeeshop X can improve the security and reliability of their payment and transaction systems.

Likelihood Determination

The following is the likelihood determination for each risk identified in the MokaPOS system at Coffeeshop X.

Table 4. Likelihood Determination

No	Risk	Probability of an event that will occur	Possibility of a threat resulting in a bad impact	Overall Possibilities
1	Hardware Damage	Low	High	Moderate
2	Operating System security vulnerabilities	Moderate	High	High
3	Vulnerability to Theft or Manipulation	Low	High	Moderate
4	MokaPOS Application Vulnerability	Moderate	High	High
5	Network and Communications Vulnerabilities	Moderate	Moderate	Moderate
6	Unnecessary Access Levels	Moderate	High	High

1) Hardware damage. The possibility that the event will occur is assessed as Low, but the potential impact if it occurs is high because it could disrupt daily operations. Therefore, the overall probability is rated as Moderate.
2) Operating System security vulnerabilities. The probability that the event will occur is rated as Moderate, but threats that would have a negative impact if they occur are rated as high because they could provide an opening for malware attacks. The overall probability is rated high.
3) Susceptibility to Theft or Manipulation. The probability that the event will occur is assessed as Low, but if it occurs, the negative impact it will have is High, because it could result in theft or manipulation of sensitive data. The overall probability is rated as Moderate.
4) MokaPOS Application Vulnerability. The possibility of an event that will occur is rated as Moderate, with threats that produce a negative impact being rated as High, because vulnerabilities in the MokaPOS application can be exploited for unauthorized access or data theft. The overall probability is rated high.
5) Network and Communication Vulnerabilities. Both the likelihood of the event occurring and the threat of having a negative impact are assessed as moderate. The overall probability is rated as Moderate.
6) Unnecessary Access Levels. The likelihood of the event occurring and the threat having an adverse impact is rated as Moderate, but due to the high potential impact on system security, the overall likelihood is rated as High.

By considering the overall probability value, Coffeeshop X can identify priorities in implementing appropriate security controls to mitigate the identified risks. Risk management measures should focus on risks with a high overall probability.

Impact Analysis

Below is the impact analysis for each identified risk within the MokaPOS system at Coffeeshop X:

Table 5. Impact Analysis

No	Impact Type	Maximum Impact	Description
1	Hardware Damage	High	The impact includes significant operational disruptions, limited functionality, or data loss if no backup exists. This can disrupt customer service and result in revenue loss.
2	Operating System Security Vulnerability	High	The impact can lead to unauthorized system access, data corruption, or loss of control over devices. This can result in theft of important information or serious business operation disruptions.
3	Vulnerability to Theft or Manipulation	High	The impact includes loss of sensitive information or customer data, identity theft, or financial loss due to transaction manipulation or unauthorized data changes.
4	MokaPOS Application	High	The impact can include customer data leaks, transaction fraud,

	Vulnerability		or system disruptions that can interfere with customer service and diminish customer trust.
5	Network and Communication Vulnerability	Moderate	The impact can include illegal data access, misuse of transmitted information, or communication service disruptions that could lead to operational interruptions.
6	Unnecessary Access Levels	High	The impact includes increased security risks due to abuse of access rights, potential data theft, or unauthorized changes to the system or applications that could compromise information integrity.

1) Hardware Damage. Physical damage to MokaPOS hardware, such as payment terminals or receipt printers, can result in significant operational disruptions. Without data backups, data loss can be a serious issue, affecting customer service and reducing revenue.
2) Operating System Security Vulnerability. Unauthorized access to the operating system can lead to data corruption, information theft, and loss of device control. This can cause major disruptions in business operations and potentially harm the company's reputation.
3) Vulnerability to Theft or Manipulation. Lack of physical security for devices can increase the risk of data theft or manipulation. Sensitive customer information can be stolen, identities misused, and transactions manipulated, resulting in financial losses.
4) MokaPOS Application Vulnerability. Deficiencies in the MokaPOS application can lead to customer data leaks, transaction fraud, or system disruptions. This can interfere with customer service and undermine customer trust in Coffeeshop X.
5) Network and Communication Vulnerability. An insecure network can lead to illegal data access and misuse of transmitted information. Communication service disruptions can also cause operational interruptions, but the impact is considered moderate compared to other risks.
6) Unnecessary Access Levels. Granting excessive access rights to users can increase security risks. Abuse of access rights can result in data theft or unauthorized system changes, compromising information integrity and business operations.

Understanding the maximum impact of each risk allows Coffeeshop X to develop appropriate mitigation strategies to reduce potential losses and ensure secure and reliable business operations.

Risk Determination

The following is a risk determination table for the identified risks within the MokaPOS system at Coffeeshop X:

Table 6. Risk Determination

No	Risk	Overall Likelihood	Level of Impact	Overall Risk
1	Hardware Damage	High	Moderate	High
2	Operating System Security Vulnerability	Moderate	High	High
3	Vulnerability to Theft or Manipulation	High	High	High
4	MokaPOS Application Vulnerability	Low	High	Moderate
5	Network and Communication Vulnerability	Moderate	Moderate	Moderate
6	Unnecessary Access Levels	Low	Low	Low

1) Hardware Damage. The overall likelihood is rated high because hardware frequently experiences physical failures. The level of impact is rated moderate because although operational disruptions are significant, mitigation is possible with regular backups and maintenance. The overall risk is rated high given its impact on operations and customer service.
2) Operating System Security Vulnerability. The overall likelihood is rated moderate because regular updates and maintenance can reduce risk. The level of impact is rated high because data corruption or unauthorized access can be highly damaging. The overall risk is rated high due to the serious potential impact on business operations.

3) Vulnerability to Theft or Manipulation. The overall likelihood is rated high because physically unsecured hardware is more vulnerable. The level of impact is rated high because data loss or identity theft can lead to significant losses. The overall risk is rated high considering the severe consequences.
4) MokaPOS Application Vulnerability. The overall likelihood is rated low because regular updates and patches can reduce risk. The level of impact is rated high because data leaks or transaction fraud can harm reputation and operations. The overall risk is rated moderate due to low likelihood but high impact.
5) Network and Communication Vulnerability. The overall likelihood is rated moderate because network protection and encryption can help reduce risk. The level of impact is rated moderate because communication service disruptions can cause operational interruptions but are not highly damaging. The overall risk is rated moderate.
6) Unnecessary Access Levels. The overall likelihood is rated low because access restrictions can be effectively applied. The level of impact is rated low because even if unnecessary access exists, its impact is not significant if managed well. The overall risk is rated low.

Control Recommendations

Below are the control recommendations for each identified threat within the MokaPOS system at Coffeeshop X:

No	Threat	Risk Level	Recommendation
1	Hardware Damage	High	Perform routine maintenance and always check hardware before opening the store.
2	Operating System Security Vulnerability	High	Implement integration and provide a firewall.
3	Vulnerability to Theft or Manipulation	High	Install CCTV and security alarm sensors.
4	MokaPOS Application Vulnerability	Moderate	Use the most up-to-date application version.
5	Network and Communication Vulnerability	Moderate	Monitor the network to detect suspicious activity.
6	Unnecessary Access Levels	Low	Manage access rights to ensure access is only granted for specific tasks.

1) Hardware Damage. Reduce the risk of hardware damage by performing routine maintenance and checks before daily operations to ensure hardware is functioning properly.
2) Operating System Security Vulnerability. Reduce the risk by integrating comprehensive security systems and implementing a firewall to protect the system from unauthorized access.
3) Vulnerability to Theft or Manipulation. Enhance physical security by installing CCTV and alarm sensors to detect and prevent theft or data manipulation.
4) MokaPOS Application Vulnerability. Reduce the risk of application vulnerabilities by always using the latest version of the MokaPOS application to ensure bugs and security flaws are fixed.
5) Network and Communication Vulnerability. Reduce the risk by regularly monitoring the network to detect suspicious activity and take immediate action if anomalies are found.
6) Unnecessary Access Levels. Reduce the risk by strictly managing access rights, ensuring that only authorized users can access specific information or functions according to their tasks.

Implementing these control recommendations will help Coffeeshop X mitigate the identified risks and ensure the security and reliability of its MokaPOS system.

Results Documentation

Below is the results documentation for the identified risks within the MokaPOS system at Coffeeshop X:

Table 7. Results Documentation

No	Description	Likelihood Determination	Impact Analysis	Risk Determination
1	Hardware Damage	Moderate	High	High
2	Operating System Security Vulnerability	High	High	High
3	Vulnerability to Theft or Manipulation	Moderate	High	High
4	MokaPOS Application Vulnerability	High	High	Moderate
5	Network and Communication Vulnerability	Moderate	Moderate	Moderate
6	Unnecessary Access Levels	High	High	Low

1) Hardware Damage:
    a) Likelihood Determination: Moderate
    b) Impact Analysis: High
    c) Risk Determination: High
    d) Explanation: Hardware damage can occur moderately often due to physical wear and tear, but its impact is significant, affecting daily operations and customer service.
2) Operating System Security Vulnerability:
    a) Likelihood Determination: High
    b) Impact Analysis: High
    c) Risk Determination: High
    d) Explanation: There is a high likelihood of security vulnerabilities if the operating system is not regularly updated and protected, leading to severe impacts such as data breaches and operational disruptions.
3) Vulnerability to Theft or Manipulation:
    a) Likelihood Determination: Moderate
    b) Impact Analysis: High
    c) Risk Determination: High
    d) Explanation: The likelihood of theft or manipulation is moderate, but the impact is high due to potential data loss, identity theft, and financial losses.
4) MokaPOS Application Vulnerability:
    a) Likelihood Determination: High
    b) Impact Analysis: High
    c) Risk Determination: Moderate
    d) Explanation: While the likelihood of application vulnerabilities is high, the use of up-to-date software and security patches can moderate the overall risk.
5) Network and Communication Vulnerability:
    a) Likelihood Determination: Moderate
    b) Impact Analysis: Moderate
    c) Risk Determination: Moderate
    d) Explanation: Network and communication vulnerabilities have a moderate likelihood and impact, leading to potential data breaches or communication disruptions.
6) Unnecessary Access Levels:
    a) Likelihood Determination: High
    b) Impact Analysis: High
    c) Risk Determination: Low

d) Explanation: The likelihood of granting unnecessary access levels is high, but the overall risk is low when managed correctly with strict access controls.

Implementing these findings will help Coffeeshop X prioritize and address the most critical risks, ensuring the security and efficiency of its MokaPOS system.

CONCLUSION

The conclusion of this research regarding security and information system architecture at Coffeeshop Analysis of the impact of these risks reveals that the average impact is significant, such as damage to hardware and security vulnerabilities in operating systems, all of which can disrupt the smooth running of business. Faced with the fact that most risks have a very high level of impact and probability, immediate action is urgently needed. This research also produces several control recommendations that need to be implemented by Coffeeshop X. These recommendations include regular hardware maintenance, use of firewalls on operating systems, employee training, regular data backup, and increased security for each access right. The implementation of these controls can be used by Coffeeshop This recommendation aims to improve the security and reliability of the information system, thereby supporting Coffeeshop X operations more efficiently and safely.

REFERENCES

[1] T. Neubauer and M. Pehn, "Workshop-based Security Safeguard Selection with AURUM," *Int. J. Adv. Secur.*, vol. 1, no. 3, pp. 123–134, 2017.

[2] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Comput. Secur.*, vol. 24, no. 2, pp. 147–159, 2005, doi: https://doi.org/10.1016/j.cose.2004.07.004.

[3] A. Setiawan, "Evaluasi penerapan teknologi informasi di perguruan tinggi swasta Yogyakarta dengan menggunakan model Cobit framework," *Semin. Nas. Apl. Teknol. Inf.*, vol. 2008, no. Snati, pp. 1907–5022, 2008, [Online]. Available: https://journal.uii.ac.id/Snati/article/view/175

[4] Iskandar Teddy and Hermadi Irman, "Audit Proses Perencanaan dan Implementasi Sistem Informasi PT Bank XYZ, Tbk dengan Menggunakan Cobit Framework," *J. Apl. Manaj.*, vol. 12, no. 4, 2014.

[5] D. Setiawan and M. P. Halilintar, "ANALISIS GANGGUAN SAMBARAN PETIR TERHADAP KERUSAKAN PERANGKAT IT PUSAT KOMPUTER UNIVERSITAS LANCANG KUNING MENGGUNAKAN METODE COLLECTION VOLUME," in *Prosiding Persidangan Antarabangsa Kelestarian Insan 2015*, 2015, vol. D, pp. 19–20.

[6] T. F. M. Syafei and A. Hidayatullah, "Analisis Penerapan UI/UX Dalam Meningkatkan Pengalaman Pengguna Pada Sistem Reservasi Amadeus," *JUSTINFO | J. Sist. Inf. dan Teknol. Inf.*, vol. 1, no. 1, pp. 1–8, 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1252.

[7] B. Supradono, "MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)," *Media Elektr.*, vol. 2, no. 1, pp. 4–8, 2009, [Online]. Available: http://jurnal.unimus.ac.id

[8] K. J. S. Hoo, "How Much Is Enough ? A Risk-Management Approach to Computer Security," 2000.

[9] W. Syafitri, "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30," *J. CoreIT*, vol. 2, no. 2, p. 6, 2016.

[10] U. Nugraha and R. Istambul, "Implementation of ISO 31000 for information technology risk management in the government environment," *Int. J. Innov. Creat. Chang.*, vol. 6, no. 5, pp.

219–231, 2019.

[11] D. Fitrianah and Y. G. Sucahyo, "AUDIT SISTEM INFORMASI/TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI DI UNIVERSITAS XYZ," *J. Sist. Inf. MTI-UI*, vol. 4, no. 1, pp. 37–46, 2008.

[12] M. Utomo, A. H. N. Ali, and I. Affandi, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," *J. Tek. ITS*, vol. 1, no. 1, pp. 2–7, 2012.

[13] S. Nurhasanah and M. Rusdan, "Development of Front End on Tour and Travel Applications Using Python and Django Framework in PT. Industri Telekomunikasi Indonesia," *J. Informatics Commun. Technol.*, vol. 2, no. 1, pp. 31–38, 2020, doi: 10.52661/j_ict.v2i1.42.