Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE)
Vol. 6, No. 2, September 2025, pp. 966~977
ISSN: 2721-3838, DOI: 10.30596/jcositte.v6i2.26392

Risk Management Analysis of Information Technology with Failure Mode and Effect Analysis Method at PT XYZ

Adisty Kharisma Virgiawan [1], Rusmala Santi[2], Aminullah Imal Alfresi [3]
[1,2,3]Department of Science and Technology, UIN Raden Fatah Palembang, Indonesia

ABSTRACT

PT Kencana Inti Perkasa is a company engaged in the management of crude palm oil (Crude Palm Oil) which uses information technology for its smooth operations. In the company there are potential information technology risks that can have an impact on the company so that they need to be identified and given an assessment. Risk problems that occur in PT Kencana Inti Perkasa's information technology are damaged hardware, virus attacks, risks to data, and risks to the network. This research aims to produce RPN values, get a list of risk priorities and develop recommendations for control measures using the Failure Mode and Effect Analysis method. This process involves identifying failure modes, assessing the severity, frequency of occurrence, and detectability of each failure mode. The final result of this research found that there are 30 failure modes consisting of 4 risks categorized as High, 2 risks categorized as Medium, 22 risks categorized as Low, and 2 risks categorized as Very Low. The highest Risk Priority Number (RPN) value, 167.83 and in the High category, arises from the incorrect use of printers caused by human error, including technological resources that are routinely utilized by the company. Another risk in the High category is the slow network capacity with an RPN of 152.06. Furthermore, computer damage due to virus attacks obtained an RPN value of 122.26, while illegal access to PC information was also categorized as High with an RPN value of 121.09, which belongs to the company's vital technology resources. These findings indicate that these risks need to be the main focus in handling, considering the high RPN value indicates a significant level of urgency.

Keyword : Information Technology; **Failure Mode and Effect Analysis**; **Risk Priority Number**.

Corresponding Author:
Adisty Kharisma Virgiawan,
Department of Science and Technology
UIN Raden Fatah Palembang, Indonesia
Email : adistykharisma02@gmail.com

Article history:
Received Aug 28, 2025
Revised Aug 30, 2025
Accepted Sep 7, 2025

1. INTRODUCTION

The development of information technology is progressing rapidly, with many companies using information technology to facilitate their operations. The information generated must be reliable and reflect the actual conditions, as it can be used as a basis for decision-making (Ulfa Mauludina et al., 2023). However, the use of information technology in solving problems can also pose various risks. The uncertainty experienced by companies can have either positive or negative effects. If such uncertainty results in detrimental impacts, this is referred to as risk (Lestari et al., 2024). Risk is the impact of uncertainty on objectives, which can be either positive or negative, meaning that risk encompasses potential situations that may hinder the achievement of objectives and targets, whether for organizations or individuals (Wicaksono & Octaviani, 2023). Without risk management, businesses will face greater problems because they do not consider the potential risks that may arise (Harini Fajar Ningrum, 2022). Risk management is a discipline that studies how companies implement actions to identify and address various issues using a comprehensive and systematic managerial approach (Putu Sugih Arta et al., 2021).

The stages of risk management include establishing the context of the problem, identifying potential risks, assessing the identified risks, and addressing the potential risks that are found (Yuli Anita et al., 2023). Risk management analysis is necessary as a systematic process to monitor and address various risks faced by the organization, so that potential disruptions can be identified and appropriate mitigation measures can be taken. Thus, risk management analysis plays an important role in ensuring operational stability and business continuity. PT Kencana Inti Perkasa is a company operating in the crude palm oil production sector. PT Kencana Inti Perkasa has utilized information technology to support the smooth running of its operational activities. Information technology, in the broadest sense, can also be defined as technology used to collect, store, process, and distribute information (Sani &

Pusparini, 2024). For example, print media is now transitioning to digital media, where information can be easily accessed via computers or smart devices (Taufik et al., 2022). Preliminary observations and interviews conducted with IT Support at PT Kencana Inti Perkasa revealed that the company's information technology includes hardware, software, networks, data, and brainware, and that there have been several risks associated with the company's information technology.Risks that have occurred in PT Kencana Inti Perkasa's information technology include hardware damage, virus attacks, and data risks such as information leaks, information breaches, capacity overload, and data loss, as well as network risks such as network connection interruptions, IP addressing errors, and decreased network connectivity. These risks indicate that the company's information technology still has weaknesses that are susceptible to various disruptions that could hinder operational efficiency.

The overall impact of the risks that have occurred in information technology at PT Kencana Inti Perkasa is very significant to the continuity of the company's operations. Damage to hardware can result in the cessation of operational activities that depend on the use of that equipment. Meanwhile, virus attacks on the system can cause disruptions to operations and reduce device performance. Risks related to data have a significant impact on information security and availability, which ultimately can hinder decision-making processes.In addition, network problems such as connection interruptions can disrupt smooth communication, slow down access to data, and reduce overall productivity. If these risks are not immediately addressed with appropriate measures, the company risks suffering losses in its operations. Therefore, risk management analysis in information technology is crucial to protect IT assets and ensure the continuity of the company's operations.

This study focuses on assessing information technology resources, including hardware such as computers, printers, switches, and servers; software such as antivirus and BIPO HRMS V2; and networks, namely the use of the internet, data, and human resources such as IT Support, HR Staff, Assistant Mill Manager, Mill Manager, and legal. In analyzing information technology risks, the Failure Mode and Effect Analysis method was chosen because it can evaluate risks systematically and identify potential impacts effectively. Failure Mode and Effect Analysis is a method applied to enhance the reliability and security of a process by identifying potential failures, known as failure modes in that process (Alijoyo et al., 2020).Each failure mode is assessed based on three main parameters: severity (S), occurrence (O), and detectability (D). Failure Mode and Effect Analysis helps companies prioritize risks that need to be addressed immediately, so that mitigation efforts can be carried out in a more focused and structured manner.

Based on this background, PT Kencana Inti Perkasa does not yet fully understand the potential disruptions to the company's information technology. Therefore, this research plays an important role in analyzing the risk assessment of PT Kencana Inti Perkasa's information technology. The topic of this research is “Information Technology Risk Management Analysis Using the Failure Mode and Effect Analysis Method at PT Kencana Inti Perkasa.” This research aims to provide a list of risks and their mitigation measures. The mitigation recommendations provided are expected to help PT Kencana Inti Perkasa reduce risks and overcome potential problems.

2. RESEARCH METHOD

This study applies an evaluation research method. Evaluation is a process of assessing or measuring a particular object or condition in order to obtain information in the form of values that can be used as a basis for decision making (Ambiyar & Muharika, 2019). Evaluation research utilizes structured scientific procedures, which include data collection through techniques such as observation, interviews, questionnaires, or direct observation, as well as data analysis based on predetermined indicators or criteria. Additionally, this research aims to systematically assess and identify various potential risks that arise in the implementation or management of information technology within an organization. The evaluation results are then used as a basis for determining risk management priorities and developing appropriate mitigation strategies or corrective actions.

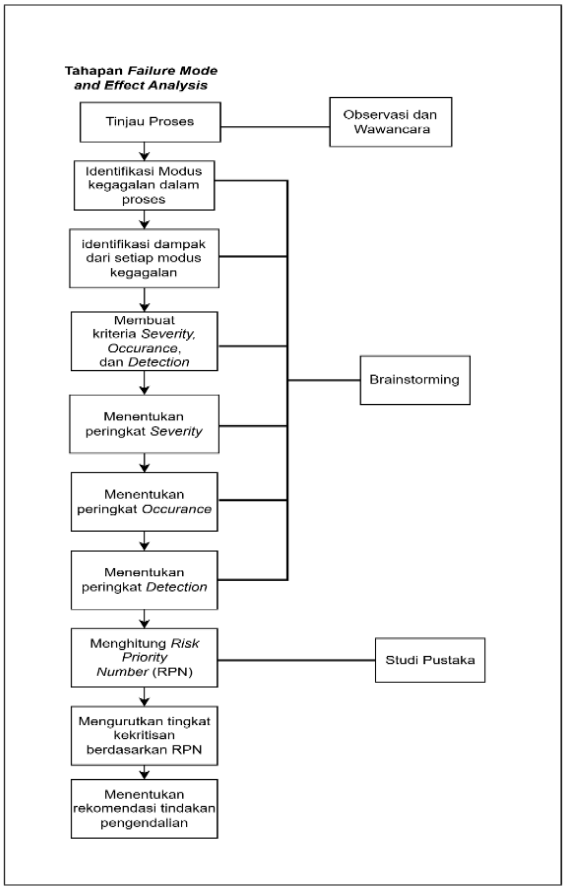

Figure 1. research stages

2.1 Review the Process

The first step is to review the existing processes at PT Kencana Inti Perkasa by conducting observations and interviews. Collect information related to workflows and activities.

2.2 Identify Failure Modes in the Process

This stage involves gathering information about problems that may arise during operations. Hold discussions to identify possible failure modes.

2.3 Identify the Impact of Each Failure Mode

After identifying problems or risks, this stage involves creating a list of risks along with their causes and potential effects. Conduct brainstorming sessions to create a list of risks and their potential effects.

2.4 Creating Severity, Occurrence, and Detection criteria

When determining the criteria for the S, O, and D parameters, brainstorming was conducted with respondents to agree that all three parameters should use the same scale. If the severity parameter (S) is expressed on a scale of 1 to 10, with 1 as the minimum value and 10 as the maximum value, then the other parameters need to use a comparable scale.

Table 1. Severity Scale

Impact	Severity Criteria	Rating
Danger, Failure occurs without warning	The failure has a significant impact on all of the company's operations and can have very serious consequences, occurring without prior warning.	10
Serious, failure occurs with warning	This failure affects all of the company's operational activities and has a significant impact, marked by a prior warning.	9
Extreme	Loss of primary functions can cause failures that impact all core business processes, leading to the cessation of operational activities.	8
Major	A decline in primary functions can result in failures that affect a number of core business processes, preventing operations from running at full capacity.	7
Significant	The loss of supporting functions can cause failures that impact all supporting business processes, where operations continue but with reduced performance, thereby affecting the results produced.	6
Moderate	Degradation of supporting functions can result in failures in several supporting business processes, with operations experiencing a gradual decline.	5
Low	Operations can still continue, but there is a >75% likelihood that this will disrupt business processes.	4
Minor	Operations can still be carried out, but there is a 50% chance that this will disrupt business processes.	3
Very minor	Operations can still be carried out, with less than a 25% chance of disrupting business processes.	2
No impact	No impact on operations	1

Probability of failure	Probability of failure	Rating
Failure is almost inevitable	1 failure every day	10
Very high	1 failure every week	9
High	1 failure every 2 weeks	8
Relatively high	1 failure every month	7
Moderate to high	1 failure every 3 months	6
Moderate	1 failure every ½ year	5
Relatively low	1 failure every 10 months	4
Low	1 failure every year	3
Very low	1 failure every 2 years	2
Almost impossible	1 failure every >3 years	1

Table 2. Occurance Scale

Table 3. Detection Scale

Probability of failure detected	Criteria based on current control design	Rating
Almost impossible Currently	there are no controls in place, so it cannot be detected or analyzed.	10
Very remote	The cause or mode of failure is difficult to detect.	9
Remote	There are only limited controls in place to detect the possibility of failure.	8
Very low	Controls are available, but their ability to detect potential failures is very low.	7

Low	Controls are in place, but their ability to detect potential failures is low.	6
Moderate	There are controls with sufficient detection capabilities to identify potential failures.	5
Moderately high	There are controls with sufficient, even high, capabilities to detect potential failures.	4
High	There are controls with high capabilities to detect potential failures.	3
Very high	There are controls that can detect potential failures with very high capabilities.	2
Almost certain	Controls are almost certain to identify the causes of failure.	1

2.5 Determining Severity Rating

Severity is an initial assessment in risk analysis. Determining the severity rating is a step to assess the extent of the impact or damage caused by a risk or problem. This impact is assessed using a scale from 1 to 10.

2.6 Determining Occurrence Rating

Occurrence is the probability or rate of occurrence of a cause that could potentially cause failure in a process or system. Determining occurrence rankings (likelihood of occurrence) is the process of assessing how often a risk or problem can occur. Occurrence is assessed using a scale from 1 to 10.

2.7 Determining the Detection Rating

Determining the detection level is the process of assessing the extent to which a problem or risk can be detected before it occurs or before it has a negative impact. The detection assessment uses a scale ranging from 1 to 10.

2.8 Calculating the Risk Priority Number (RPN)

At this stage, calculations are performed by multiplying the weights derived from severity, occurrence, and detection based on the guidelines. As a guideline, a high RPN value indicates that information technology should be addressed with the highest priority. The relationship between RPN parameters is formulated as follows:

$$RPN = S \times O \times D$$

Explanation:
S = Severity (Level of severity)
O = Occurrence (Level of occurrence)
D = Detection (Level of detection)

2.9 Ranking the criticality level of RPN

The next step is to determine the criticality level of each risk based on the RPN calculation results. Ranking the criticality level based on RPN is a step to prioritize risks by ranking the calculated RPN values. Risks with the highest RPN are considered the most critical and need immediate attention or handling.

Table 4. RPN Criteria

Level Risiko	Skala Nilai RPN
Very Low	X < 20
Low	20 ≤ x < 80
Medium	80 ≤ x < 120
High	120 ≤ x < 200
Very High	x > 200

2.10 Determine control action recommendations
In this final step, recommendations will be provided for measures to address risks that require special attention.

Population and Sample
The sample consists of elements that represent the population. The population focused on in this study is the Functional Department and Middle Management. The total population at PT Kencana Inti Perkasa is 18 people. There are several sampling techniques, one of which is purposive sampling. In this study, the sample taken consists of people who are considered to be most knowledgeable or skilled in the information needed by the researcher (Amruddin et al., 2022).
The respondents selected as samples for this study include IT Support, HR staff, Assistant Mill Manager, Legal, and Mill Manager as the responsible party. These respondents were selected because they have a direct connection to the object being studied and are able to provide relevant data and insights.

3. RESULTS AND DISCUSSION

This study involved the application of all stages of the Failure Mode and Effects Analysis method. The results of each stage of Failure Mode and Effect Analysis are as follows. The process review was conducted to understand the business flow at PT Kencana Inti Perkasa. There are two main processes at PT Kencana Inti Perkasa, namely the purchasing and sales processes, as well as four business processes using BIPO HRMS V2 in human resource management. Through this system, employee attendance records are recorded automatically and in real time, either through a mobile application or integrated devices, thereby minimizing errors and manipulation of attendance data. In addition, BIPO HRMS V2 also makes it easy for employees to access information related to salary payments. Not only that, this system also supports claims submissions for specific purposes, such as health expense reimbursements, which can be submitted and monitored digitally. Another feature is leave requests, where employees can submit leave requests directly through the system and monitor the approval status without the need for manual processes. The use of BIPO HRMS V2 helps PT KIP create a more structured, accurate, and easily accessible HR management system for all employees.

A. List of Information Technology Assets

Table 5. Information Technology Assets

Category	Description	Assets
Hardware	PC/Desktop	27 Unit Dell Optiplex Core-i5, 16 GB, SSD 512
	AC	8 unitmerek Mitsubishi dan Sharp
	Server	HP ProLiant Gen 10, Processor: Intel Xeon Gold, Storage: 4TB , RAM: 32 GB
	CCTV	16 Unit merek Hikvision
	Printer	1 Unit Merek Fuji Xerox
	Genset	1 Unit Merek Cummin
	Ups	10 Ups Prolink Pro700
	Switch	3 Aruba Switch
	Rak Server	1 Indorack 31U
	Router AP	4 Unit Merek Aruba
	Router	3 Mikrotik RB3011
Software	Antivirus	Symantec Endpoint Protection
	Operating System	Windows 11 Pro
	Microsoft Office	Microsoft Office 365
	Database	Sql
	Cloude	Google Cloud dan OneDrive
	Human Resource Management Application	BIPO HRMS V2
Network	Telkomsel	Astinet PT. Telkom dan 4G Telkomsel
Data	Employee Data	Employee Information

Claim Data	Health Claim Information
BPJS Data	Employee BPJS Information

B. Failure Mode Analysis

Table 6. Failure Mode Analysis

Failure mode	Cause
Computer Damage	Virus attacks
Computers cannot be used	Damage to computer components: damaged monitors, damaged keyboards, etc.
Computer device out of order	The age of the technology used
Loss of PC components	Theft
PC information accessed illegally	Weak access protection or computer not password protected
Server down	Power outage during maintenance by PLN so the system cannot be accessed
Network connectivity decreased	Network failure
Spread of information	Misuse of access rights
Information or data breach	Sharing passwords
Data in the system does not match physical data	Errors in data entry
Data loss	Software and network failure
System failure	Late license renewal
Virus attack	Antivirus unable to detect and prevent viruses from entering
Network connection lost	Damaged network device or power outage
IP addressing error	Human error
Slow network capacity	Insufficient capacity provided
Network failure	Network configuration manipulation
Falsification or misuse of access rights and authority	Granting access rights to outside parties.
Human error	Data entry errors and use of system devices

C. Risk Priority Number (RPN) value

After obtaining assessments from five respondents, the assessments were averaged to represent each parameter, namely Severity, Occurrence, and Detection. Then, the RPN was calculated. This study identified 30 modes of information technology failure that produced the highest RPN (Risk Priority Number) value in the High category, namely 167.83, which was obtained from printer misuse, and the lowest RPN value, namely 17.76, in the Very Low category for the risk of forgery and misuse of access rights and authority. Then, all components were grouped into vital company technology resources and technology resources frequently used by the company.

1. Company's Vital Technology Resources

Based on the overall analysis results, the risk of slow network capacity with an RPN of 152.06 is the most significant management risk, while the network component is the most influential component for the company's operational continuity because it is the backbone of connectivity for all IT resources. In addition, the hardware component, namely computers, with the risk of computer damage due to virus attacks with an RPN of 122.26 and illegal access to PC information with an RPN of 121.09 caused by weak access protection and computers not being password-protected, is also one of the components that

most influences operational continuity due to the high RPN value obtained, which affects the company's operational processes.

Item	*Process Function (Category)*	*Potential Failure Mode (Process Defects)*	*Potential Effects of Failure*	*Potential Causes*	RPN
Hardware	Computer	Computer Damage	Operational activities and performance are hampered	Virus attacks	122.26
		Computer cannot be used	Operational activities and performance are hampered	Damage has occurred to computer components: damaged monitor, broken keyboard damaged, etc.	20.94
		Computer devices out of order	Operational activities and performance is hampered	The length of time the technology has been in use	32.77
		Loss of PC components	Financial losses	Theft	25.87
		Illegal access to PC information illegal	Stealing information that harms the company	Weak access rights protection or computers not password protected	121.09
	Network devices	Network failure	Operational activities and performance is hampered	Network configuration manipulation of the network	18.48
		Network device failure network	Operational activities and performance	Natural disasters such as fires, floods, lightning strikes, etc.	23.52
		Loss of components of network devices	Operational activities and performance are hampered	Theft	29.57
	Server	Server damage	Server is unusable	The server overheated and caught fire	37.89
		Server down	Operational activities and performance are hampered	Power outage during *maintenance* from PLN, causing the system to be inaccessible accessed	36.50
		Server overheating	Operational activities and performance were hampered	Air conditioning not working in the room server	40.96
Software	Antivirus	Virus attack	Operational activities and performance is hampered	Antivirus unable to detect and prevent viruses that in	44.62
	BIPO HRMS V2	System failure	Business processes are hampered and	Delayed license renewal	48.05
				data input cannot be performed	
Network	Internet	Network connection lost	System inaccessible	Device malfunction Network or power outage	33.79
		IP addressing error	Network cannot connect	Human error	27.78
		Slow network capacity	Slow browsing (Web pages load very slowly)	Provided capacity is insufficient	152.06
		Network connectivity is declining	Backup failure and system error.	Network failure	87.55
Data	Data	Information leakage	Sensitive information leak (Data confidentiality)	Abuse of rights access	26.94
		Full capacity	Unable to store data	No checks were ever performed on the server's memory capacity has been used	30.72
		Information or data breach	Important information leaked or lost	Sharing passwords	41.18
		Data on the system with physical data does not match	Data integrity	Errors in data entry	73.73
		Data loss	Data integrity and availability	Software and network failures network	38.30
Brainware	*IT Support, HR Staff, Mill Manager Assistant, Mill Manager*	Falsification or misuse of access rights and authority	Violation of policies and misuse of data, system manipulation	Granting access rights to external parties	17.76
		Human error	Professionalism	Data entry errors and use of system devices	58.75
		Lack of awareness of cyber threats threats	Malware intrusion, system affected by ransomware	Failure to recognize phishing, clicking on links	24.19

Figure 2. Company's Vital Technology

2. Technology Resources Routinely Used by Companies

Item	*Process Function (Category)*	*Potential Failure Mode (Process Defects)*	*Potential Effects of Failure*	*Potential Causes*	*RPN*
Hardware	Printer/scanner	Printer/scanner malfunction	Unable to print data and perform scans data.	Natural disasters such as floods, fires, lightning strikes lightning strikes.	28.08
		Loss of printer/scanner	Financial loss	Theft	49.9
		Incorrect use of printer	Unable to print and scan data	Human error	167.83
	Switch	Damaged port	Device cannot connect to the network	Unstable electrical voltage	63.36
		Switch overload	Performance is declining and the network is slowing down	Too many devices connected	91.17

Figure 3. Company's Routine Technology

The table above shows the technological resources that are routinely used by the company, including printers/scanners and switches. Printers and scanners are susceptible to damage due to natural

disasters and loss due to theft, but the highest risk arises from misuse, with an RPN value of 167.83, which has the potential to halt the printing and scanning of important documents. This confirms that human error is still the biggest risk factor for routine devices. For network switches, the risk of overload due to too many connected devices has an RPN value of 91.17, followed by port damage due to unstable electrical voltage with an RPN of 63.36. Printer misuse caused by human error does have the highest RPN value, namely 167.83, indicating that this risk is serious enough to be taken into account. However, printers are categorized as routinely used tools, not as vital technological resources for companies such as servers or core networks. This means that even though printer damage or failure due to misuse can hinder the process of printing and scanning documents, the impact is still limited to administrative or documentation activities and does not stop the company's overall business operations.
In other words, printers still play an important role in supporting the smooth running of daily work, but they are not components that are crucial to the overall business process. Therefore, although the risk of printer misuse should be managed through training and standard procedures, the priority of risk mitigation can be adjusted compared to resources that are truly vital to the continuity of the company's core operations.

Based on the results of data processing using the Failure Mode and Effect Analysis method, 30 failure modes were found spread across various risk categories, namely 4 High risks, 2 Medium risks, 22 Low risks, and 2 Very Low risks. The RPN calculation results show that the risk with the highest overall priority is printer misuse with an RPN value of 167.83, which is classified as High Risk. This risk arises from human error, namely employees' lack of understanding of the correct printer usage procedures, resulting in the printer being unable to print or scan data. Furthermore, slow network capacity with an RPN of 152.06 is a significant problem due to the limited network capacity provided, resulting in slow browsing because web pages take a long time to load. This risk is categorized as High Risk. Computer damage due to virus attacks with an RPN of 122.26, which is also classified as High Risk, is also a serious concern, as it can hamper company operations and performance. In addition, the risk of illegal access to PC information with an RPN of 121.09, which is categorized as High Risk, confirms the weak security of access rights and password control on computers, which can have a detrimental impact on the company in the form of information theft. These risks fall into the High category, which means they require immediate attention and handling due to their significant potential impact on company operations.

D. Determining Control Recommendations

Table 7. Control Recommendations

No	Risk	Problem	Control Measures	Reference
1	The existence of incorrect printer usage	Human Error, (Employees who do not understand the usage procedures may operate the printer features incorrectly)	a. Provide training and technical supervision on printer usage to employees so that they understand the correct usage procedures and can operate the printer features appropriately. b. Create clear and easy-to-understand SOPs (Standard Operating Procedures) for printer use and ensure that employees always follow these procedures.	(Putra et al., 2023)
2	Slow network capacity	Insufficient capacity provided	a. Increasing network capacity. In addition, limiting the applications that can be opened and establishing SOPs for the	(Zulvi, 2022)

				use of applications and computers.	
			b.	Implementing load balancing techniques. Load balancing can distribute the workload evenly across various network resources such as servers, routers, and network links, thereby optimizing the utilization of CPU, memory, and bandwidth. In this way, no resources are wasted or underutilized, improving overall network performance.	(Sabila et al., 2024)
3	Computer damage	The existence of a virus attack	a.	Installing a firewall, antivirus, and Deep Freeze to protect the system from virus attacks and data breaches.	(Anisah et al., 2021)
			b.	Perform regular antivirus database updates at least once a week to ensure that the antivirus can detect the latest viruses and perform a full scan of the entire computer system using the latest antivirus to detect and remove existing viruses.	(Murdowo, 2023)
4	PC information accessed illegally	Weak access rights protection or computers not password protected	a.	Adopt stronger authentication methods, such as multi-factor authentication (MFA), to reduce the risk of unauthorized access due to weak passwords and improve security regulations and standards, such as following ISO 27001 to strengthen access governance and data protection.	(Permana et al., 2025) (Adelika & Nurbaiti, 2023)
			b.	Change passwords regularly and ensure that passwords are sufficiently strong and encrypted to improve access security. Provide training to employees on the importance of maintaining	

	data confidentiality and proper security practices.

4. CONCLUSION

1. This study successfully identified various information technology risks at PT Kencana Inti Perkasa. From the assessment results, 30 failure modes were identified across various risk categories, namely 4 High risks, 2 Medium risks, 22 Low risks, and 2 Very Low risks.

2. The highest Risk Priority Number (RPN) in the High category is 167.83, which is errors in printer usage due to human error categorized as a technology resource routinely used by the company. Other risks include slow network capacity with an RPN value of 152.06. Then there is computer damage caused by virus attacks with an RPN value of 122.26, as well as illegal access to PC information, which is also categorized as High with an RPN value of 121.09, categorized as a vital technological resource of the company.

3. The risk of slow network capacity as a vital technological resource of the company is a major threat because it affects connectivity and overall business processes. The risk of computer damage and illegal access to computers as vital hardware also has a significant impact on company operations. Meanwhile, the risk of printer misuse as a routine technological resource has a limited impact only on administrative activities.

REFERENCES

Alijoyo, A., Wijaya, B., & Jacob, I. (2020). *Failure Mode Effect Analysis Analisis Modus Kegagalan dan Dampak*. CRMS Indonesia. www.lspmks.co.id

Ambiyar, & Muharika. (2019). *Metodologi Penelitian Evaluasi Program* (1st ed.). Alfabeta cv.

Amruddin, dkk, Muskananfola, I. L., Febriyanti, E., Pandie, F. R., & Goa, M. Y. (2022). *Buku Metodologi Penelitian Kuantitatif dan Kualitatif* (A. Munandar, Ed.). CV. MEDIA SAINS INDONESIA.

Anisah, D., Medina, N. Z., Nuraini, A. R., Siti, K. M., & Kraugusteelianan. (2021). Manajemen Risiko Sistem Informasi Rumah Sakit (Studi Kasus : Rumah Sakit EMC Tangerang). *Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA)* . https://www.emc.id/id/hospitals/emc-

Harini Fajar Ningrum. (2022). *Manajemen Risiko* (Harini Fajar Ningrum, Ed.). MEDIA SAINS INDONESIA.

Lestari, I. P., Purwani, F., & Gunawan, C. E. (2024). *Manajemen Risiko Aset Teknologi Informasi* (1st ed.). Noer Fikri Offset .

Murdowo, S. (2023). Mengenal Lebih Dalam Tentang Virus-Virus Komputer dan Perilakunya. *Jurnal INFOKAM*, *19*(1).

Permana, A. R., Anindita, R., Zainol, Z., & Quinn, A. (2025). Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *3*(2), 137–146. https://doi.org/10.33050/mentari.v3i2.744

Putra, A. E., Wijaya, D. K., & Islahudin, N. (2023). Perbaikan proses printing menggunakan metode DMAIC dan 5S untuk mengurangi waste proses di UKM limit screen printing Semarang. *JENIUS : Jurnal Terapan Teknik Industri*, *4*(1), 98–107. https://doi.org/10.37373/jenius.v4i1.468

Putu Sugih Arta, I., Gede Satriawan, D., Kadek Bagiana, I., Loppies, Y., Agusetiawan Shavab, F., Matari Fath Mala, C., Malik Sayuti, A., Agnes Safitri, D., Berlianty, T., Julike, W., Wicaksono, G., Marietza, F., Rustandi Kartawinata, B., & Utami, F. (2021). *Manajemen Risiko Tinjauan Teori dan Praktis*. Widina Bhakti Persada Bandung. www.penerbitwidina.com

Sabila, K., Rahayu, S., & Sumarni, T. (2024). Peningkatan Efisiensi Penggunaan Sumber Daya Jaringan Melalui Teknik Load Balancing. *CEMERLANG : Jurnal Manajemen Dan Ekonomi Bisnis*, *4*(3), 31–41. https://doi.org/10.55606/cemerlang.v4i3.2989

Sani, A., & Pusparini, N. N. (2024). *Riset Teknologi Informasi (Sebuah Pemahaman dan Implementasi)* (1st ed., Vol. 1). PT Penamuda Media.

Taufik, A., Sudarsono, B. G., Budiyantara, A., Sudaryana, K., & Muryono, T. T. (2022). *Pengantar Teknologi Informasi* (J. Hutahaean & M. Amin, Eds.; 1st ed.). CV. Pena Persada.

Ulfa Mauludina, N., Mukaromah, S., & Wulansari, A. (2023). Pengukuran Tigkat Kapabilitas Manajemen Risiko Keamanan Informasi Pada Seksi Persandian Menggunakan COBIT 5. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi (SITASI) 2023 Surabaya*, 6–7.

Wicaksono, D. P., & Octaviani, A. (2023). *Manajemen Risiko*. Pustakabarupress.

Yuli Anita, S., Tanti Kustina, K., Wiratikusuma, Y., Sudirjo, F., Sari, D., Rupiwardani, I., Nugroho, L., Rakhmawati, I., Kesumawati Harahap, A., Anwar, S., Apriani, E., & Luh Ketut Ayu Sudha Sucandrawati, N. (2023). *Manajemen Risiko* (D. P. Sari, Ed.; 1st ed.). PT Global Eksekutif Teknologi. www.globaleksekutifteknologi.co.id

Zulvi, M. S. (2022). Jurnal Politeknik Caltex Riau Manajemen Risiko Teknologi Informasi Menggunakan Metode Fmea (Studi Kasus: Diskominfo Pemprov Riau). *Jurnal Komputer Terapan*, *8*(2). https://jurnal.pcr.ac.id/index.php/jkt/