Journal of Education Technology and Information System Vol (01) Ed (02) P.88-97 (2025)
Received November 2024 / Revised February 2025 / Accepted June 2025

Journal of Education Technology and Information System

https://journal.unesa.ac.id/index.php/jetis/

Risk Management Analysis of Information Technology (IT) Asset Security Using ISO 31000 and FMEA

Indira Carisa Dewi[1*], Ghea Sekar Palupi[1]

[1]*Universitas Negeri Surabaya, Surabaya, Indonesia*
indira.20011@mhs.unesa.ac.id, gheapalupi@unesa.ac.id

Abstract. Information technology assets play an important role in business processes at BPS Kota Mojokerto. The absence of a structured policy regarding special handling in terms of managing information technology assets and the lack of understanding of BPS employees regarding security and components of related information technology assets are some of the causes of potential risks at BPS Kota Mojokerto. The purpose of this study is to identify, assess and mitigate risks related to information technology managed by BPS Kota Mojokerto based on the ISO 31000 and FMEA methods. This research method uses qualitative analysis through in-depth interviews and evaluation of SOP documents and related IT assets. The results of the study identified 58 overall risks to IT assets, including 1 very high risk, 1 high risk, 4 medium risks, 30 low risks, and 31 very low risks. The results of the risk management document are used by BPS Kota Mojokerto to minimize risks, as well as to compile a detailed and systematic risk mitigation analysis on information technology assets.

Keywords: FMEA; Information Technology Assets; ISO 31000; Risk Management

1. Introduction

The Central Bureau of Statistics (BPS) of Mojokerto Regency serves to manage statistical data by using an integrated and precise information system, as well as developing technology to improve efficiency in data processing (BPS, 2023). The statistical business process at BPS involves various steps that aim to improve operational efficiency and data quality. According to the Directorate of Information Systems, government institutions that use information systems are required to manage information security to protect information technology assets from various risks (KemenpanRB), 2020). In addition, the regulation of IT implementation in Indonesia is regulated in the Regulation of the Minister of Communication and Information Technology Number 23 of 2012. The regulation clarifies that all aspects related to the utilization of information and communication technology financing for broadband services and applies to the entire territory of the Republic of Indonesia (Kemkominfo, 2012).

Information technology assets play an important role in the operational process of BPS Mojokerto Regency, because these assets are the main source of information for the institution. Based on the results of discussions with BPS employees in the general subdivision, it was stated that there were several problems such as infrastructure management that did not meet information technology asset security standards, the absence of structured policies regarding special handling in the management of information technology assets, and the lack of understanding of BPS employees regarding security management related to aspects and components of technology assets. In addition, there have also been incidents on IT assets, namely server downtime and program improvements that hinder business processes, which cause non-optimal operations or temporary cessation of agency activities. Prior research by (Purwita & Subriadi, 2019) also emphasizes that organizations often struggle to integrate tangible and intangible assessments when evaluating IT investments,

which may contribute to suboptimal risk awareness and governance.

ISO 31000 is a standard designed to provide general principles and guidelines for implementing risk management. ISO 31000 has a clear and measurable structure in its implementation ranging from principles, frameworks, to risk management processes. The principle of risk management is the philosophy of risk management, while the framework is a structured and systematic arrangement of the risk management system, and the process refers to the activity in managing risk sequentially and interconnected with one another (Purba & Rahayu, 2021). Therefore, the purpose of this research is to identify risks based on ISO 31000 and FMEA related to information technology assets used at BPS Mojokerto Regency and provide risk mitigation measures against possible risks to these IT assets (Putri & Iriani, 2024).

2. Theorical Framework

2.1. IT Risk Management

IT risk management can be framed around a set of guiding principles for effective risk management, such as identifying, organizing, and managing risks for the company. In managing IT risks, several processes are required, including risk identification, risk analysis, risk evaluation, risk control, monitoring, and coordination (Karanja & Rosso, 2017). Additionally, IT risk management involves several steps such as risk mitigation, evaluation, assessment, and the risk management framework (Tuma, 2018).

2.2. ISO 31000

ISO 31000 is a guideline or standard for risk management implementation codified by the International Organization for Standardization (ISO). The purpose of ISO 31000 is to serve as an international standard for risk management that can be applied by various types of organizations in addressing different risks within their business processes. In its risk management process, ISO 31000 categorizes risk criteria based on their level of importance. This risk management process consists of six activities: communication and consultation, defining the scope, context, and criteria, risk assessment, risk treatment, recording & reporting, and monitoring & review (Purba & Rahayu, 2021).

2.3. FMEA (Failure Mode and Effect Analysis)

The FMEA (Failure Mode and Effects Analysis) method is a systematic approach used to identify the consequences or impacts of failures in a system or process, as well as to reduce or eliminate the likelihood of such failures occurring. The following are the steps in the FMEA assessment process:

1. Identifying the system and its elements, failures, and their effects.
2. Determining the severity level of the effects of a failure.
3. Determining the frequency or likelihood of the risk occurring (occurrence).
4. Determining the detection level of the cause (detection).
5. Determining the Risk Priority Number (RPN), which represents the risk level of a failure. The RPN value ranges from 1 to 1000; the higher the RPN, the higher the risk of potential failure in the system, design, process, or service. RPN = Severity x Occurrence x Detection (McDermott et al., 2009) .
6. Providing recommendations for actions that can be implemented to reduce the risk level of the failure.

3. Methods

3.1. Research Methodology

This study employs a qualitative research approach, and in determining risk attributes, it is based on ISO 31000 with risk assessment conducted using the FMEA method. As for the data collection technique, it is carried out through interviews (see Figure 1).

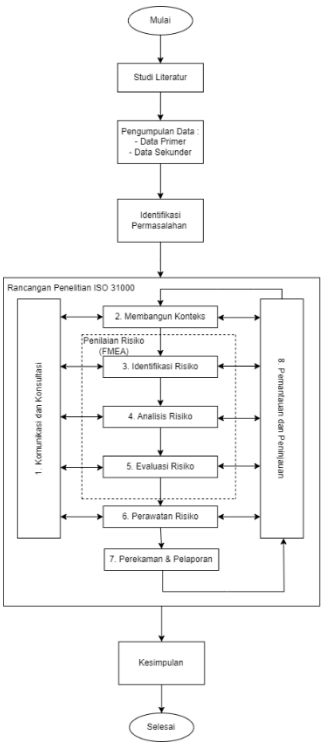

Figure 1 Research Methodology

3.1.1. Literature Review Stages

In this stage, references are searched through books and literature journals that discuss research on risk management using ISO 31000 with the FMEA method, as well as on information technology (IT) assets in Mojokerto City BPS.

3.1.2. Data Collection Stages

At this stage, data collection was carried out using primary data through interviews with Mr. Agung Prasetiyo who serves as IT manager at BPS Mojokerto City, because he knows more about the problems that often occur in information technology (IT) assets at the BPS Mojokerto City office. In addition, secondary data collection was also carried out through literature studies, including 2 e-books, namely information system security books and management and information audit books, 13 journals, and 3 other references regarding risk analysis of information technology (IT) asset security that will be used as references. Data collection also produced several documents related to SOPs owned by the Mojokerto City Statistics Center (BPS).

3.1.3. Problem Identification Stage

From the identification process, the researcher found that the BPS Mojokerto City does not yet have a risk register, and a list of IT asset documents currently owned by the BPS office of Mojokerto City was obtained.

3.1.4. Communication and Consultation Stage

The communication and consultation stage was carried out separately between the researcher and each informant, with a duration ranging from 30 minutes to one hour. The results of the communication and consultation revealed that there is currently no risk management being implemented for the information technology (IT) assets at the BPS office of Mojokerto City.

3.1.5. Context Establishment Stage

The context in the risk management process refers to the environment in which the risk management process is applied. In this stage, the processes involved include the strategic context, organizational context, risk management context, and risk evaluation criteria.

3.1.6. Risk Assessment Stage

This risk assessment stage includes the subprocesses of risk identification, risk analysis, and risk evaluation. In this context, the goal is to identify the organization's information technology assets, the threats to each technology used, the potential risks arising from those threats, and the impact that the organization may face from those risks. The risk analysis process in this study uses Failure Mode and Effects Analysis (FMEA), assessing each risk based on severity, occurrence, and detection to generate a Risk Priority Number (RPN). During the evaluation stage, the identified risks are then evaluated to determine whether they can be tolerated, based on the level of risk.

3.1.7. Risk Treatment Stage

In this stage, all potential risks associated with IT assets are addressed by providing recommendations on how to handle these possible risks. The goal of these suggestions is to minimize the likelihood of these risks occurring, ensuring that IT assets are protected and that business processes can operate optimally.

3.1.8. Conclusion

In this stage, the researcher can draw conclusions and provide recommendations. The conclusion is derived from the findings of this study and is expected to serve as a foundation for evaluation, improvement, and management of information technology (IT) asset risk at BPS Mojokerto City. The recommendations section offers suggestions for future research on IT asset risk management.

4. Results and Discussion

4.1. Context Establishment

Based on ISO 31000, the risk management planning stage aligns with the scope establishment. In ISO 31000, this stage consists of four activities: establishing the strategic context, establishing the organizational context, defining the scope of the risk management process, and developing risk criteria as boundaries for conducting risk management.

4.1.1. Strategic Context

BPS Mojokerto City has a statistical infrastructure integrated with advanced information and communication technology. The operational systems or applications used are updated annually. The security system also has clear and extensive performance indicators, with oversight from the central office. Regarding human resource capabilities, there are three IT employees at BPS Mojokerto City who have been trained to possess professional and competent technical skills.

4.1.2. Organizational Context

According to PERKA BPS, the metadata technical framework (One Data Indonesia) has clear policies based on laws and regulations. This is further reinforced by the BPS vision and mission for 2020-2024 as “a provider of quality statistical data for a prosperous Indonesia.” In its survey or statistical census activities, BPS Mojokerto City involves several stakeholders, such as regional government organizations (OPD), businesses, and the community.

4.1.3. Risk Management Context

Analyzing risk management on IT assets at BPS Mojokerto City shows that the IT assets play a crucial role in the operational business processes of survey activities. If these information technology assets face threats and risks, it will disrupt business processes, causing the operations at BPS Mojokerto City to run suboptimally. Risk management can anticipate losses by

implementing procedures on IT assets to minimize potential risk.

4.1.4. Risk Evaluation Criteria

defines the risk level from lowest, low, medium, high, and highest. Low-risk level is acceptable and requires monitoring, medium-risk level requires risk control, high-risk level requires strict control, and very high-risk level is unacceptable.

4.2. Risk Assessment

In conducting risk assessment, several stages are carried out, namely risk identification, risk analysis, risk evaluation, and the last is risk treatment. By conducting a risk assessment on IT assets at BPS Mojokerto City, it is expected to help in determining the risks that can disrupt activities at the BPS Mojokerto City office. In this case, the questionnaire data uses a table in Microsoft word, while the calculation of the RPN value of the risk uses Microsoft excel to make it easier.

4.2.1. Risk Identification

Risk identification is carried out in accordance with the SOP documents and asset documents listed in SIMAN (Asset Management System). After identifying the risks, the next things that need to be identified are the causes of the risks, the impacts of the risks, and the controls for those risks.

4.2.2. Risk Analysis

In this stage, the assessment is classified into three parts severity, occurrence, and detection, which will later be used to calculate the RPN (Risk Priority Number). Below is the result of the assessment conducted by the author using the FMEA method.

Table 1 The result of risk analysis

No	Category	IT Assets	Risk	Risk Code	Impact of Risk	S	Causes of Risk	O	Control	D	RPN
1	*Hardware*	*Server*	Server down	R-02.01	Obstruction of BPS operational performance process	8	Many users accessing the server at one time or more than the limit	3	Take turns accessing or waiting for the server to return to normal for about an hour.	5	120
		PC and Laptop	PC and laptop damage	R-08	Boot failure occurs and blue screen of death (BSOD) occurs	7	Old hard disk and physical damage to HDD & RAM	3	Carry out regular maintenance, depending on external parties who make repairs	5	105
		Printer and Scanner	Hardware failure	R-16	The printer or scanner is not functioning properly or often turns itself off	7	Damaged and dirty power adapter or cable and sensor	2	Make repairs with the service center in Surabaya	6	84

2	*Software* (Application)	BPS Processing System Program	Software failure	R-25	Disruption to the operational performance of the processing system program	8	New program error or patch occurs in software functionality	4	Make corrections related to errors by IT staff and wait for corrections from the center	7	224
3	*Network*	Biznet and Telkom up to 100 Mbps	Overload request	R-49	Work gets hampered	8	Surge in users accessing the network simultaneously	2	Using ISP network backup alternately	5	80
4	Data	Partner Data HDI Data SUSENAS data SAKERNAS Data KSA Data GDP Data	Backup data failure	R-56	Lost data backup	9	Damage to backup storage media	5	As per the instructions, perform regular backups after activities.	2	90

4.2.3. Risk Evaluation

In this risk evaluation stage, the risks that have been identified and analyzed previously are evaluated and categorized into risk levels. The risk levels are divided into five categories: Very Low, Low, Medium, High, and Very High. The results of this categorization are used to determine the appropriate actions for anticipation, mitigation, and strategies to handle risks so that the operational business processes at BPS can run smoothly.

Table 2 Result of Risk Evaluation

No	Category	IT Assets	Risk	Risk Code	Impact of Risk	Causes of Risk	Control	RPN	Level Risk
1.	*Hardware*	*Server*	Server down .	R-02.01	Obstruction of BPS operational performance process	Many users accessing the server at one time or more than the limit	Take turns accessing or waiting for the server to return to normal for about an hour.	120	*High*
		PC and Laptop	PC and laptop damage	R-08	Boot failure occurs and blue screen of death (BSOD) occurs	Old hard disk and physical damage to HDD & RAM	Carry out regular maintenance, depending on external parties who make repairs	105	*Medium*
		Printer and Scanner	Hardware failure	R-16	The printer or scanner is not functioning properly or often turns itself off	Damaged and dirty power adapter or cable and sensor	Make repairs with the service center in Surabaya	84	*Medium*

No	Category	IT Assets	Risk	Risk Code	Impact of Risk	Causes of Risk	Control	RPN	Level Risk
2.	*Software* (Application)	BPS Processing System Program	Software failure	R-25	Disruption to the operational performance of the processing system program	New program error or patch occurs in software functionality	Make corrections related to errors by IT staff and wait for corrections from the center	224	*Very high*
3.	*Network*	Biznet and Telkom up to 100 Mbps	Request Overload	R-49	Work gets hampered	Surge in users accessing the network simultaneously	Using ISP network backup alternately	80	*Medium*
4.	Data	Partner Data HDI Data SUSE NAS data SAKE RNAS Data KSA Data GDP Data	Backup data failure	R-56	Lost data backup	Damage to backup storage media	As per the instructions, perform regular backups after activities.	90	*Medium*

4.3. Risk Treatment

The risk treatment stage is divided into four steps reducing, avoiding, sharing, and accepting. From the risk evaluation results, risks classified as very high and high were identified, meaning these risks require avoidance or elimination actions. Since these risks have a significant potential to pose a threat, actions to eliminate the risk must be taken to prevent it from occurring. Medium-level risks are handled by reducing them, by taking one or more actions that can minimize the impact or likelihood of the risk occurring. Meanwhile, risks classified as low and very low can be treated by sharing or transferring the risk, as well as accepting the risk.

Table 3 Result of Risk Mitigation

Risk Name	RPN Results	Risk Mitigation Steps	Reference
Software Failure (R-25)	224	- Inspect patch notes , system backups , and performing patch testing on a staging or test server environment when patching occurs . - Do documentation and testing of programs complete and comprehensive before the program starts operated .	(Agustinus et al., 2017.)

Risk Name	RPN Results	Risk Mitigation Steps	Reference
		- Preparing the latest backup so that If system patch occurs can restored - Perform system monitoring For reduce possible patches happen	(Yustanti et al., 2018)
Server Down (R-02.01)	120	- Perform a soft reboot or server recovery first first and hard reboot when server down occurred . - Apply policy management capacity For manage amount connected users in a way simultaneously . - Do checking in a way periodically on each server for resources, amount of data, size transfer data owned whether in accordance with the size of the interface used .	(Hardianto & Dharmawan, 2022)
		- Data center monitoring and necessary there is server maintenance periodic and scheduled	(Rohman et al., 2023.)
		- Do configuration restrictions access to server	(Rohman et al., 2023)
PC and Laptop Damage (R-08)	105	- Identifying symptom damage , turn off the PC and pull out device external and also cable power , and check use diagnostic tool .	(Agustinus et al., 2017)
		- Equipment must maintained with Correct For ensure its availability and integrity	(Zuraidah, 2022)
		- Give not quite enough answer to every employees to use appropriate hardware existing procedures - Maintenance should be scheduled during break time or day holiday employee	
		- Guard use of existing hardware . Immediately report to part technician If found problematic hardware so that it can be direct dealt with	(Fawaji et al., 2018)
Backup Data Failure (R-56)	90	- Ensure original data Still intact , checking configuration and storage space of backup media , and perform recovery tests of the backup process.	Database Administrator Training Course Book r PT. PLN Persero, Nanang Syahroni
		- Renewal procedure in backing up data is with do use RAID configuration	(Rohman et al., 2023.)
		- Make clear procedures and scheduling For perform data backup	Database Administrator Training Course Book r PT. PLN Persero, Nanang Syahroni
		- Develop and implement more robust back-up and recovery strategies and procedures . good , like prepare back-ups of back-up data and store them on various source .	(Emmanuel & Maulany, n.d.)
Printer and Scanner Damage (R-16)	84	- Identifying light indicator or message error , check cable paper and tray, do cleaning and test printing return For inspect is the printer working with Correct .	(Fachrezi, 2021)
		- Give not quite enough answer to every printer users for use right in accordance procedure . - Arrange a maintenance schedule periodically .	
		- Equipment must maintained with Correct For ensure its availability and integrity	(Zuraidah, 2022)

Risk Name	RPN Results	Risk Mitigation Steps	Reference
		- Guard cleanliness and use of existing hardware . Immediately report to part technician If found problematic hardware so that it can be direct dealt with	(Fawaji et al., n.d.))
Request Overload (R-49)	80	- Inspect cPanel page for access resource usage and check use each resource. And use tool monitor network , Wireshark, NetFlow for help identify pattern Then cross .	(Candra et al., 2019)
		- Network must managed and controlled For For guard security systems and applications that use the network including information data inside it .	ook (Yustanti et al., 2018)
		- Network monitoring for ensure in condition good , and also expand bandwidth capacity	(Setiawan et al., 2023)
		- Consider using the most stable , reliable and rarely down ISP own history disturbance - Limit number of requests in term time certain . And use content delivery networks CDN to direct traffic to nearest server location with user .	mmanuel & Maulany, n.d.)
		- It is necessary checking network in a way periodically and add a booster router signal for the system can accessed .	(Rohman et al., 2023)

5. Conclusions

Based on the research results, the following conclusions can be drawn, from the risk management analysis process using ISO 31000 and FMEA at BPS Mojokerto City, ISO 31000 and FMEA were chosen because both offer a systematic, flexible, and integrated approach to risk management. ISO 31000 provides a comprehensive framework, while FMEA offers an in-depth analysis of potential failures. The combination of these two methods can assist organizations in managing risks effectively and efficiently. The risk assessment stages start from identifying IT asset risks, analyzing risks by providing RPN values, to evaluating risks in the form of risk level categorization. The results of the RPN calculation can be a useful tool in risk management, but must be used with caution and accompanied by additional analysis to ensure that the mitigation strategies implemented are effective and appropriate to the situation at hand. 58 potential risks were found, one of which was at a very high level, namely the risk of software failure caused by errors in new programs or patches in software functionality, with an RPN value of 224. Mitigation steps that can be taken include checking patch notes and system backups, documenting and testing programs before operation, and preparing backups and monitoring the system continuously. One risk falls into the high level, namely the risk of server downtime caused by the number of users accessing the server at the same time or exceeding the limit, with an RPN value of 120. Mitigation steps taken include performing soft and hard reboots, conducting regular data center monitoring, server maintenance, and configuring access restrictions. Risks from technical factors are often more significant due to their immediate and large impact, as well as the uncertainty associated with system failure. Meanwhile, human factors, while important, can be managed more effectively through good training and procedures.

References

Agustinus, S., Nugroho, A., & Cahyono, A. D. (n.d.). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS. *J. RESTI Rekayasa Sist. Dan Teknol. Inf*, *1*(3), 250–258. https://doi.org/10.29207/resti.v1i3.94.

Candra, R. M., Sari, Y. N., Iskandar, I., & Yanto, F. (n.d.). *Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018*.

Emmanuel, P. N., & Maulany, R. (n.d.). *Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE*. Allegro pada Indonesia Publishing House.

Fachrezi, M. I. (n.d.). MANAJEMEN RISIKO KEAMANAN ASET TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000:2018 DISKOMINFO KOTA SALATIGA. *JATISI J. Tek. Inform. Dan Sist. Inf*, *8*(2), 764–773. https://doi.org/10.35957/jatisi.v8i2.789.

Fawaji, M. R., Santosa, I., & Nurtrisha, W. A. (n.d.). Manajemen Risiko SIMRS Unit Rekam Medis Di Rumah Sakit Al-Ihsan. *Menggunakan ISO*, *31000*(2018).

Hardianto, F. A., & Dharmawan, Y. S. (n.d.). Manajemen Risiko TI ISO 31000 Dengan Cobit 5 Dan FMEA (PT. XYZ. *Jurnal SITECH : Sistem Informasi dan Teknologi*, *4*(2), 133–146. https://doi.org/10.24176/sitech.v4i2.6649

Karanja, E., & Rosso, M. A. (2017). The role of IT risk management in IT governance: A literature review. *Journal of Information Systems*, *31*(1), 35–55. https://doi.org/10.2308/isys-51483

McDermott, R. E., Mikulak, R. J., & Beauregard, M. R. (2009). *The basics of FMEA*. Productivity Press. https://doi.org/10.1201/9781439809617

Peraturan Menteri Komunikasi Dan Informatika Nomor 23 Tahun 2012 Tentang Pengelolaan Penyelenggaraan Jaringan Telekomunikasi (2012). https://jdih.kominfo.go.id/

Peraturan Menteri PANRB Nomor 59 Tahun 2020 Tentang Pemantauan Dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (SPBE) (2020). https://jdih.menpan.go.id/

Purba, J. T., & Rahayu, R. (2021). Enterprise risk management implementation in the public sector based on ISO 31000. *Journal of Risk and Financial Management*, *14*(9), 431. https://doi.org/10.3390/jrfm14090431

Purwita, A. W., & Subriadi, A. P. (2019). Information technology investment: In search of the closest accurate method. *Procedia Computer Science*, *161*, 300–307. https://doi.org/10.1016/j.procs.2019.11.127

Putri, F. Z., & Iriani. (2024). Analisis manajemen risiko berbasis ISO 31000 untuk mengelola risiko operasional Di bidang X Pada perusahaan dinas XYZ. *Jurnal Ekonomi Dan Bisnis Digital*, *1*(3), 433–444. https://jurnal.ittc.web.id/index.php/jebd/article/view/569

Rohman, A. F., Ambarwati, A., & Setiawan, E. (n.d.). Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S. *INTECOMS: Journal of Information Technology and Computer Science*, *3*(2), 298–310. https://doi.org/10.31539/intecoms.v3i2.1854

Setiawan, I., Riyanto, R., Yunita, I. R., & Saputra, J. P. B. (2023). Manajemen Risiko Sistem Informasi Student Service Center Menggunakan Metode OCTAVE Allegro. *Jurnal Rekayasa Informasi*, *12*(2), 82–88.

Statistik, B. P. (2023). *Badan Pusat Statistik Kabupaten Mojokerto: Profil dan layanan statistik*. BPS. https://mojokertokab.bps.go.id/

Tuma, K. (2018). *Risk management in information technology: Best practices for managing and controlling IT risks*. Springer. https://doi.org/10.1007/978-3-662-56775-1

Yustanti, W., Bisma, R., Qoiriah, A., & Prihanto, A. (2018). *Keamanan Sistem Informasi*. Zifatama Jawara.

Zuraidah, E. (2022). *Audit Sistem Informasi dan Manajemen: Menggunakan COBIT 5 dan Case Study*. Teknosain.