Journal of Information Systems and Informatics

Vol. 4, No. 3, September 2022 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

http://journal-isi.org/index.php/isi Published By DRPM-UBD

Information Technology Risk Management Analysis Using ISO: 31000 at PT. XYZ

Vania Rizqita Putri[1], Agustinus Fritz Wijaya[2]

[1]Information System Departement, Satya Wacana Christian University, Salatiga, Indonesia
Email: [1]682019105@student.uksw.edu, [2]agustinus.wijaya@uksw.edu

Abstract

PT. XYZ is one of the branch offices of banking subsidiaries in Indonesia that focuses on providing leasing facilities, investment and working capital. As a company, PT. XYZ is inseparable in the use of information technology which gives rise to various possible risks that exist. Therefore, it is necessary to have an analysis of information technology risk management in PT. XYZ. Through this research, it is hoped that it can help PT. XYZ in identifying possible risks that occur to the company, as well as actions that must be taken in the face of such risks. The framework used in this study is the ISO 31000 framework. Based on the results of this study, 13 possible risks that have low risk levels (R01, R02, R03, R04, R05, R07, R08, R12, R13, R15, R16, R20 and R21), 6 possible risks that have medium risk levels (R06, R09, R10, R11, R14 and R18), as well as 2 possible risks that have high risk levels (R17 and R19). In addition, a risk treatment proposal was produced that can be used as a reference by PT. XYZ to minimize losses caused by these risks.

Keywords: information technology, risk management, ISO 31000

1. INTRODUCTION

PT. XYZ is one of the branch offices of banking subsidiaries in Indonesia that focuses on providing leasing facilities, investment and working capital. In its application, the company's business processes are inseparable from information technology. Information technology is an important component that can support company activities, both main activities and supporting activities. It is undeniable that the use of information technology in companies has various challenges and possible risks that occur. Risk is a possibility that can cause danger, resulting in not optimal company business processes. Based on the possible risks that exist, it is necessary to have risk management in information technology in order to minimize the possibility and impact that will be caused.

Risk management is a process of identifying, analyzing, assessing, controlling, and trying to avoid, minimize or even eliminate unacceptable risks [1]. Risk management is important to do in every project to be carried out by the company. Risk management is carried out to protect the company from risks that hinder the achievement of goals and various things that have the potential to harm the company. Risk management is expected to be a tool for companies in making the right decisions to minimize losses to be experienced [2].

There is one of the risks that has occurred in PT. XYZ is a data mutation that results in a server down. Therefore, through this research, an information technology risk management analysis will be carried out at PT. XYZ using iso 31000 framework. ISO 31000 is a framework published by the International Organization for Standardization (ISO) and regulates the risk management of companies or organizations. The aim of ISO is to provide universally recognized principles and guidelines for risk management. Based on the framework, there are 2 stages, namely, risk assessment and risk treatment. The results obtained in this study are risk assessment in the form of identification of possible risks, risk analysis and risk evaluation. As well as risk treatment that contains proposed actions that the company can take in minimizing losses. This research is expected to assist companies in recognizing and managing risks and events that may arise, minimize their impact and determine appropriate risk handling.

The previous research that became a reference in this study, as conducted by Kanantyo et al., 2021 with the title "Information Technology Risk Analysis Using ISO 31000 (Learning Management System SMPN 6 Salatiga)". There are 26 possible risks that can interfere with the use of the Moodle (Learning Management System) application. The final result of this study is in the form of risk identification, risk level and proposed actions that need to be taken in minimizing risk [3]. Citra Christian & Sitokdana, 2022 with the title "Information Technology Risk Analysis at BANK ABC Using iso 31000 Framework". There are 16 possible risks that may interfere with m-banking performance. The results obtained in this study are the level of risk and proposed actions that must be taken before the possibility of such risks interfering with performance around m-Banking [4]. Prabowo & Wijaya, 2022 with the title "Risk Management Analysis on KKM LKF FTI UKSW Website Using ISO 31000 Framework". There are 16 possible risks that can interfere with the use of the KKM LKF FTI website. The results of this study are the level of risk and proposed actions that can be used as a reference for LKF FTI so that the use of the website can be carried out optimally [2].

2. METHOD

The research was conducted using qualitative research methods. According to Saryono (2010: 49), qualitative research is research used to investigate, discover, describe, and explain the qualities or privileges of social influences that cannot be explained, measured or described through a quantitative approach. There are several stages in this study, as can be seen in Figure 1.

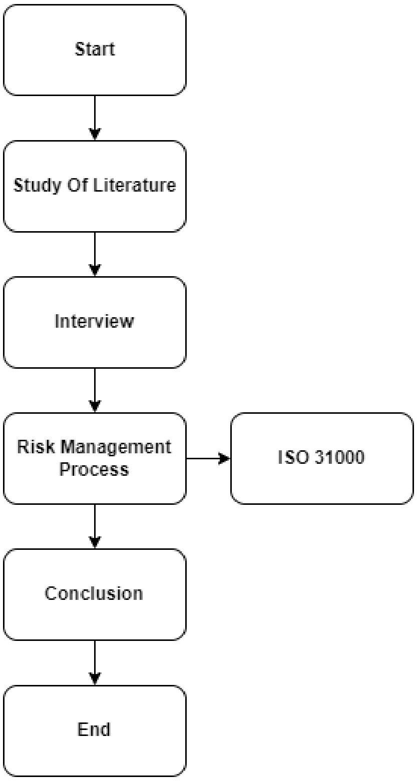

Figure 1. Stages of Research

The following are the stages in the research:

1. Literature Studies
   The stage of information collection by conducting data assessment through various sources such as books and scientific papers related to research and relevant for use with current circumstances.
2. Interview
   The question and answer process between the researcher and the informant by providing questions related to issues, problems or problems that are in accordance with the existing situation, conditions and reality and still guided by the framework used.
3. Risk Management Process
   Based on ISO 31000 Framework, the risk management process is divided into two stages, namely risk assessment and risk treatment. The risk assessment is further divided into three stages, namely risk identification, risk analysis and risk evaluation [5].
4. Conclusion
   The last stage in the study where conclusions are drawn based on the results and discussions that have been obtained.

3. RESULTS AND DISCUSSION

3.1. Risk Assessment

Based on the framework used, the risk assessment process consists of 3 stages, namely risk identification, risk analysis and risk evaluation.

3.1.1. Risk Identification

At the risk identification stage, an asset identification process is carried out, identifying possible risks and identifying the impact of possible risks obtained.

3.1.1.1. Asset Identification

The asset identification process is carried out by classifying by categories, namely data, hardware, and software. The following are the results of the identification of existing assets in the company, can be seen in Table 1.

Table 1. Asset Identification

No	Data	Hardware	Software
1	Customer BPKB	Cable LAN	Consumer Data Information System
2	Customer Card	CCTV	Company Portal
3	Data Dealer	Computer	Data Information System Personnel Information System
4	Dealer Billing Data	Fingerprint	Marketing Apps
5	Debtor Data	Laptop	Survey Application (Marketing)
6	Employee Data	Photocopier	
7	Fiduciary	Printer	
8	Financing Agreement Data	Projector	
9	Insurance Airline Data	Router	
10	Invoice	Scanner	
11	Insurance Policy	Server	
12	Purchase Order	Smartphone	

Based on the asset identification stages, there are 12 data, 12 hardware and 5 software that support the company's business processes.

3.1.1.2. Identify Possible Risks

The process of identifying possible risks is carried out by classifying based on factors that often arise in the company such as natural and environmental factors, human factors, and system and infrastructure factors. The following results identify the possible risks that exist in the company, can be seen in Table 2.

Table 2. Identify Possible Risks

Factor	Code	Possible Risks
Nature and Environment	R01	Flood
	R02	Earthquake
	R03	Fire
	R04	Lightning
	R05	Landslide
Human	R06	Data and information are accessed by unauthorized parties
	R07	Human Error
	R08	Lack of socialization of the use of the latest information systems
	R09	Data falsification survey
	R10	Abuse of access rights
Systems and Infrastructure	R11	Data lost
	R12	Corrupted data
	R13	Hardware malfunctions
	R14	System malfunctions
	R15	Power outages
	R16	Overheat
	R17	Full storage
	R18	Unscheduled maintenance process
	R19	Server down
	R20	Software cannot improve the quality of company performance
	R21	User interface difficulty

Based on the process of identifying possible risks, 21 possible risks were found which were classified into 3 factors. In natural and environmental factors there are 5 possible risks. In the human factor there are 5 possible risks. In system and infrastructure factors, there are 11 possible risks.

3.1.1.3. Identify Risk Impacts

The process of identifying the impact of risks is carried out based on the results of the identification of possible risks. The following results identify the impact of existing risks on the company, can be seen in Table 3.

Table 3. Risk Impact Identification

Code	Possible Risks	Impact
R01	Flood	Infrastructure damage and some business processes are hampered.

R02	Earthquake	Infrastructure breakdown and entire business processes have stalled.
R03	Fire	Damage to the company's infrastructure, and business processes are at a standstill.
R04	Lightning	Infrastructure damage and some business processes are hampered.
R05	Landslide	Infrastructure breakdown and entire business processes have stalled.
R06	Data and information are accessed by unauthorized parties	Data and information are misused by unauthorized parties.
R07	Human Error	The service process on data input does not run optimally.
R08	Lack of socialization of the use of the latest information systems	Business processes are not running optimally.
R09	Data falsification survey	The debtor's data is inaccurate so that there is a validation error in the credit analyst.
R10	Abuse of access rights	Resulting in data information leakage and allowing data manipulation.
R11	Data lost	Obstruction of ongoing business processes.
R12	Corrupted data	Inaccurate data.
R13	Hardware malfunctions	Business processes are not running optimally.
R14	System malfunctions	The database is inaccessible, hampering running business processes.
R15	Power outages	The cessation of the company's activities.
R16	Overheat	Business processes are not running optimally.
R17	Full storage	The data is automatically deleted by the system.
R18	Unscheduled maintenance process	An error occurred in the system used.
R19	Server down	The database cannot be accessed so that business processes do not run optimally.
R20	Software cannot improve the quality of company performance	Business processes are not running optimally.
R21	Elusive user interface	Business processes are not running optimally.

Based on this process, the impact of every possible risk that arises for the company has been identified.

3.1.2. Risk Analysis

At the stage of risk analysis, it is carried out by determining the value of the possible risks that have been identified in the previous stage. There is a table of Likelihood criteria that have been classified into five criteria based on the number of possible risks that occur in a certain period of time. The following likelihood assessment criteria can be seen in Table 4.

Table 4. Likelihood Assessment Criteria

Likelihood		Description	Frequency per Genesis
Value	Criterion		
1	Rare	The risk almost never occurs	>5 Years
2	Unlikely	Such risks are rare	2-5 Years
3	Possible	These risks sometimes occur	1-2 Years
4	Likely	Such risks are common	7-12 Months
5	Certain	Such risks almost always occur	1-6 Months

In addition to assessing the possibility of risks appearing using Likelihood, at the risk analysis stage, an assessment of how much impact is caused to affect the company's performance. The following assessment criteria of the impact, can be seen in Table 5.

Table 5. Impact Assessment Criteria

Likelihood		Description
Value	Criterion	
1	Insignificant	Risks do not interfere with the activities and business processes of the enterprise.
2	Minor	Activity in the company is slightly hampered, but it does not interfere with the company's core activities.
3	Moderate	Risks interfere with the course of the company's business processes, so that part of the company's activities are hampered.
4	Major	Risks hinder almost the entire business process of the enterprise.
5	Catastrophic	Risks disrupt the thorough course of business processes and completely stop the company's activities.

After determining the likelihood criteria in Table 4, and the impact criteria in Table 5, the next stage is to assess each possible risk that exists in the company. The following results of the assessment of possible risks can be seen in Table 6.

Table 6. Assessment of Possible Risks Based on Likelihood and Impact

Code	Possible Risks	Likelihood	Impact
R01	Flood	1	1

R02	Earthquake	1	2
R03	Fire	1	3
R04	Lightning	1	1
R05	Landslide	1	2
R06	Data and information are accessed by unauthorized parties	1	4
R07	Human Error	2	1
R08	Lack of socialization of the use of the latest information systems	1	3
R09	Data falsification survey	2	3
R10	Abuse of access rights	1	4
R11	Data lost	2	3
R12	Corrupted data	1	3
R13	Hardware malfunctions	1	2
R14	System malfunctions	2	3
R15	Power outages	3	1
R16	Overheat	2	2
R17	Full storage	5	3
R18	Unscheduled maintenance process	3	3
R19	Server down	5	3
R20	Software cannot improve the quality of company performance	3	1
R21	Elusive user interface	1	1

Based on the risk assessment process in Table 6, it can be seen that every possible risk that exists in the company has a likelihood value, namely how often the risk occurs and impact, namely how much impact is caused by a risk.

3.1.3. Risk Evaluation

At the risk evaluation stage, an evaluation process is carried out on the possible risks that existed in the previous stage. Based on the results of the existing analysis, it is then entered into the risk evaluation matrix. The following is the risk evaluation matrix, which can be seen in Table 7.

Table 7. Matrix Risk Evaluation

Likeliho	**Certain**	5	medium	medium	high	high	high
	Likely	4	medium	medium	medium	high	high
	Possible	3	low	medium	medium	medium	high
	Unlikely	2	low	low	medium	medium	medium
	Rare	1	low	low	low	medium	medium
			1	2	3	4	5

o d		Insignificant	Minor	Moderate	Major	Catastrophic
	Impact					

The risk evaluation matrix is categorized into 3 risk levels, namely low, medium, and high. Risks that have a low risk level will be colored green. Risks that have a medium risk level will be yellow. Risks that have a high risk level will be colored red. The results of the risk evaluation of the company. can be seen in Table 8.

Table 8. Results of Risk Evaluation Using Matrix

Likelihood							
	Certain	5	🟨	🟨	🟥 R17 R19	🟥	🟥
	Likely	4	🟨	🟨	🟨	🟥	🟥
	Possible	3	🟩 R15 R20	🟨	🟨 R18	🟨	🟥
	Unlikely	2	🟩 R07	🟩 R16	🟨 R09 R11 R14	🟨	🟨
	Rare	1	🟩 R01 R04 R21	🟩 R02 R05 R13	🟩 R03 R08 R12	🟨 R06 R10	🟨
			1	2	3	4	5
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
	Impact						

Based on the matrix above, there are 26 possible risks that have been categorized into 3 risk levels. The following possible risks with Likelihood and Impact have been arranged based on high to low levels, can be seen in Table 9.

Table 9. Categorization of Possible Risks Based on Risk Levels

Code	Possible Risks	Likelihood	Impact	Risk Level
R17	Full storage	5	3	High
R19	Server down	5	3	High
R06	Data and information are accessed by unauthorized parties	1	4	Medium
R09	Data falsification survey	2	5	Medium
R10	Abuse of access rights	1	4	Medium
R11	Data lost	2	5	Medium
R14	System malfunctions	2	3	Medium
R18	The maintenance process is not scheduled	3	3	Medium

R01	Flood	1	1	Low
R02	Earthquake	1	2	Low
R03	Fire	1	3	Low
R04	Lightning	1	1	Low
R05	Landslide	1	2	Low
R07	Human Error	2	1	Low
R08	Lack of socialization of the use of the latest information systems	1	3	Low
R12	Corrupted data	1	3	Low
R13	Hardware malfunctions	1	2	Low
R15	Power Outages	3	1	Low
R16	Overheat	2	2	Low
R20	Software cannot improve the quality of company performance	3	1	Low
R21	Elusive user interface	1	1	Low

In Table 9, 26 possible risks were obtained that had been categorized based on their risk levels. There are 2 possible risks categorized into high levels, namely R17 and R19. There are 6 possible risks categorized into medium levels, namely R06, R09, R10, R11, R14 and R18. There are 13 possible risks categorized into low levels, namely R01, R02, R03, R04, R05, R07, R08, R12, R13, R15, R16, R20 and R21.

3.2. Risk Treatment

Possible risks that have been identified and assessed are then carried out at the stage of risk treatment. At this stage, a proposed action will be given against the possibility of company risk. The following treats risk as a proposed action that a company can take, as can be seen in Table 10.

Table 10. Treat the Risk

Code	Possible Risks	Risk Level	Treat the Risk
R17	Full storage	High	• Perform data backups periodically. • Perform cleaning on the PC to prevent the appearance of viruses / malware that can cause corrupted data.
R19	Server down	High	• Perform regular system repairs and updates.

			• Report problems that occur when using the system to the center so that immediate repairs are made to stem.
R06	Data and information are accessed by unauthorized parties	Medium	• Provide access restrictions to each user with good data and system security.
R09	Data falsification survey	Medium	• Validate the survey data accurately by ensuring that the 5C category (Character, Capacity, Capital, Collateral, Condition) has been met.
R10	Abuse of access rights	Medium	• Provide access restrictions to each user with good data and system security.
R11	Data lost	Medium	• Perform data backups periodically.
R14	System malfunctions	Medium	• Perform regular system repairs and updates. • Report problems that occur when using the system to the center so that system repairs are immediately carried out.
R18	The maintenance process is not scheduled	Medium	• Ask the center periodically about the maintenance schedule so that parties from the branch office can provide announcements to users no later than 30 to 60 minutes before the maintenance process runs. • Provide proposals to the central department to schedule maintenance processes during employee rest hours.
R01	Flood	Low	• Storing all company assets in a high place or far from the reach of floods.
R02	Earthquake	Low	• Providing a safe haven for company assets.

R03	Fire	Low	• Setting up a fire extinguisher. • Keep assets away from areas where there is frequent fire contact.
R04	Lightning	Low	• Installing a lightning rod.
R05	Landslide	Low	• Providing a safe haven for company assets
R07	Human Error	Low	• Conduct training on each hr.
R08	Lack of socialization of the use of the latest information systems	Low	• Socialize to users regularly if there are system updates.
R12	Corrupted data	Low	• Perform data backups periodically. • Perform cleaning on the PC to prevent the appearance of viruses / malware that can cause corrupted data.
R13	Hardware malfunctions	Low	• Use existing hardware in the company carefully. • Keep the hardware and the surrounding environment of the hardware located. • Report all problems found in the company's hardware to the technicians in the company so that they can be corrected immediately.
R15	Power Outages	Low	• Provide an electrical generator set with the required power. • Prepare Uninterruptible Power Supply (UPS).
R16	Overheat	Low	• Does not open too many applications on the computer. • Periodically delete used data.
R20	Software cannot improve the quality of company performance	Low	• Improving the quality of the software that the company uses.

R21	Elusive user interface	Low	• Create an easy-to-understand view of the system. • Conducting socialization of the use of the system.

Based on the proposed actions that have been given, it is expected to minimize the possibility of company risk.

4. CONCLUSION

Information Technology Risk Management Analysis Research Using ISO: 31000 at PT. XYZ has two processes, namely risk assessment and risk treatment. In the risk assessment stage, there are three stages, namely risk identification, risk analysis and risk evaluation. From the information technology risk management analysis process, 21 possible risks were obtained that could threaten the business processes of PT. XYZ. Based on the results of the study, there are 13 possible risks with low risk levels, namely floods, earthquakes, fires, lightning, landslides, human error, lack of socialization of the use of the latest information systems, damaged data, hardware damage, power outages, overheating, software cannot improve the quality of company performance, and user interfaces that are difficult to understand. Then, 6 possible risks were found that have a medium risk level, namely data and information accessed by unauthorized parties, falsification of survey data, misuse of rights access, lost data, system damage and unscheduled maintenance processes. In addition, 2 possible risks are obtained that have a high-risk level, namely full storage, and server down. Expected PT. XYZ can use the results of this study as a guideline to minimize the possibility of risks that can threaten the company's business processes by applying risk treatment which can be seen in Table 10.

REFERENCE

[1] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, “Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ,” *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, pp. 91-96, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

[2] D. Prabowo and A. F. Wijaya, “Risk Management Analysis on KKM LKF FTI UKSW Website Using ISO 31000 Framework,” *Journal of Information Systems and Informatics*, vol. 4, no. 1, pp. 65, Mar. 2022, [Online]. Available: http://journal-isi.org/index.php/isi.

[3] P. Kanantyo, and F. S. Papilaya, “Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6

Salatiga)," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 4, pp. 1896-1908, Des . 2021. [Online]. Available: http://jurnal.mdp.ac.id.

[4] H. Citra Christian and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC Menggunakan Framework ISO 31000," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no.1, pp. 735-748, Mar. 2022. [Online]. Available: http://jurnal.mdp.ac.id.

[5] ISO, *Risk management — Guidelines*, ISO 31000:2018. 2018.

[6] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 : 2018 (STUDI KASUS: CV. XY)," *SEBATIK* , vol.#, no.#, pp. 277-284, Jun. 2019.

[7] Monica, D. Kurniawan, and R. Prabowo, "Analisis Manajemen Risiko Sistem Informasi Pengelolaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000," *Jurnal Komputasi*, vol. 8, no. 1, pp. 83-90, Apr. 2020.

[8] S. D. Fitri, D. L. Setyowati, and K. Duma, "Implementasi Manajemen Risiko Berdasarkan ISO 31000:2009 pada Program Perawatan Mesin di Area Workshop PT. X," *Faletehan Health Journal*, vol. 6, no. 1, pp. 16–24, Mar. 2019, [Online]. Available: www.journal.lppm-stikesfa.ac.id/ojs/index.php/FHJ.

[9] S. Agustinus, A. Nugroho, and A. Dwika Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *Jurnal Resti*, vol. 1, no. 3, pp. 250–238, Des. 2017, [Online]. Available: http://jurnal.iaii.or.id.

[10] T. F. Rahardian and A. F. Wijaya, "Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000," *Journal of Information Systems and Informatics*, vol. 4, no. 2, pp. 428-443 , Jun. 2022, [Online]. Available: http://journal-isi.org/index.php/isi.

[11] A. Rahmawati, A. F. Wijaya, A. R. Fakultas, and T. Informasi, "ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI ITOP Penulis Korespondensi." *Jurnal SITECH*, vol. 2, no. 1, pp. 13-20, Jun. 2019, [Online]. Available: http://www.jurnal.umk.ac.id/sitech.

[12] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "ANALISIS RISIKO TEKNOLOGI INFORMASI PADA APLIKASI SAP DI PT SERASI AUTORAYA MENGGUNAKAN ISO 31000," *SEBATIK*, vol.#, no.#, pp. 36-42, Jun. 2019.

[13] R. P. Pangestu and A. F. Wijaya, "Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ," *Jurnal Bina Komputer*, vol. 2, no. 2, pp. 1-14, Jun. 2020.

[14] N. V. Richardo and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Perusahaan Toko Surabaya Cabang Surakarta," *Journal of Information Systems and Informatics*, vol. 3, no. 1, pp. 13-30, Mar. 2021, [Online]. Available: http://journal-isi.org/index.php/isi.

[15] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.