JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 8, No. 1, Maret 2023, Pp. 211-217

IT RISK MANAGEMENT ANALYSIS ON BANK XYZ E-BANKING SERVICE SYSTEM USING ISO 31000

Hafiz Izzamufid Ash Siddiqi*[1], Eko Darwiyanto[2] , Yudi Priyadi[3]

1. Telkom University, Bandung, Indonesia
2. Telkom University, Bandung, Indonesia
3. Telkom University, Bandung, Indonesia

Article Info

Keywords: Risk Management, ISO 31000, E-Banking, Risk Assessment

Article history:
Received 15 November 2022
Revised 29 November 2022
Accepted 6 December 2022
Available online 1 March 2023

DOI :
https://doi.org/10.29100/jipi.v8i1.3325

* Corresponding author.
Corresponding Author
E-mail address:
hafizashsiddiqi@student.telkomuniversity.ac.id

ABSTRACT

The growth of information technology is now forcing businesses to innovate, one of which is in the banking sector. Electronic banking or e-banking is a new system in the banking world, where the existence of e-banking can make it easier for customers to carry out banking activities. Bank XYZ has also used this e-banking service system where the services are Mobile Banking, Personal Internet Banking, Corporate Internet Banking. but there are several risks that may occur ranging from low to high level risk. The purpose of this research is to carry out a risk assessment using the ISO 3100 risk management standard on the e-banking application of Bank XYZ. The results show that there are 20 possible risks that occur and are divided into two categories, namely those that may occur from outside and from within the company. Risk analysis shows that risk has several types of impacts from small scale to disaster scale. There are also several types of risk management depending on the type of risk and the priority level of the risk, namely risk avoidance, risk sharing, risk mitigation, and risk acceptance.

I. INTRODUCTION

THE role of technology in human activities at this time is indeed very large. Almost all organizations have opened their eyes by paying attention to technological developments, especially information technology[1]. In recent years, as a result of the development of industry 4.0 and competition between competitors, Information Technology is one of the important needs for every company or business organization, this is proven by almost all business organizations or companies that have used it in all of their business value chains.[2]. However, with the existence of this information technology, it is undeniable that there are risks that can result in delays and even not achieving the goals of using information technology if these risks are not addressed and managed properly[3].

The development of information technology in the banking world has brought changes in the approach to business strategies carried out by companies, by placing information technology as the main element in the development of innovation in products and services[4]. Examples of the use of information technology are in electronic banking (e-banking) services, e-banking products in the form of ATMs, Mobile Banking, Phone Banking, and Message Banking, some of which are innovations in services where changing manual transaction services are based on technology.[5]

Bank XYZ is one of the banking companies which is a regional-owned bank. With a service system based on information technology, of course, Bank XYZ has IT risks. Some of the risks and problems that can arise due to the incorrect application of information technology can cause business process losses such as financial losses, the company's reputation will decline due to a decrease in the level of public trust, and others.[6].

Problems that arise in XYZ banks include an error where when making a transaction, it cannot continue the transaction. This happens because of a disturbance in the network infrastructure, with this problem causing the system to be unable to perform transactions.

Another problem that arises at Bank XYZ is a problem with the application server, where the server is sometimes full at hours that are not the time to do maintenance, with this problem it makes it less convenient to make transactions because the system feels slow, and even transaction failures occur. Seeing the importance of the system for the company, the researcher wants to conduct an analysis and audit of XYZ Bank's E-banking service system

Therefore, IT risk management analysis is needed so that these risks can be avoided or mitigated if they occur. Based on this background, this research will implement IT Risk Management using the ISO 31000 standard which will focus on the risk aspects of the service system[7]. As has also been used in a research journal entitled "Risk Analysis of Microfinance Conversion Based on ISO 31000 PT. Bank BRI Syariah. Tbk Aceh" which both use the ISO 31000 Framework in their research, but the journal is limited to the scope of research in the section organizational finance. so that in this study, researchers want to take another scope, namely the problem of organizational application services.

In the ISO 31000 analysis there are several stages, namely, Communication and Consultation, Establishing the Context, Risk Assessment, Risk Treatment, Monitoring and Review, and Recording and Reporting.[8][9].With the risk research using ISO 31000, this will produce a document containing risk mapping and risk treatment which will later become one of the references in Bank XYZ application services.

II. Research Methodology

The research method used in this study is qualitative analysis. The qualitative method is defined as an approach to understanding a symptom or event. To understand the incident, it is necessary to interview the research participants or participants by asking general and broad questions. This information is then collected and analyzed[10]. The final result of qualitative research is in the form of a written report. The data obtained from Bank XYZ is then used in an analysis using the ISO 31000 framework to determine the types and levels of existing risks.

A. Data sources

The data used in this study are primary and secondary data. where primary data is obtained by conducting interviews with people with an interest in application service problems. secondary data obtained from journals, books and several articles[11]

B. Data Analysis

The research was conducted at Bank XYZ by using the data that has been taken. the analysis process is carried out using the ISO 31000 framework, by conducting a risk assessment based on the process carried out by ISO 31000[12].

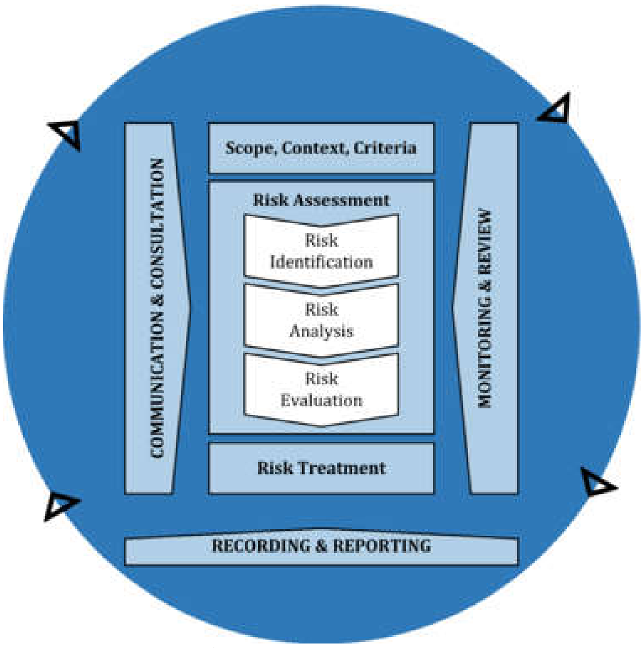


Figure 1. ISO 31000 Process

From figure 1 is a process in ISO 31000 which can be explained as follows :

1) Communication and Consultation (Communication and Consultation)
In this study, the communication and consultation stages are carried out with stakeholders which are very important because they can give consideration to risks and make assessments based on their perceptions of risk [13].
2) Establishing the Context (Establishing the Context)
In determining the context, four things must be determined, namely, internal context, external context, risk management context, and risk criteria[13].
3) Risk Assessment
In ISO 31000 Risk Assessment includes three overall processes, namely risk identification, risk analysis, risk evaluation.

a) Risk Identification

In this study, risk identification was carried out by direct interview or by questionnaire to the party responsible for it. Following is the risk identification process:

1. Define organizational units, and information technology
2. Define crucial activities in the organization
3. Determine the goods and people involved in these crucial activities
4. Determine the form of loss suffered by the organization
5. Determine the cause of the loss
6. Make a risk list

b) Risk Analysis

In this study, risk analysis was carried out qualitatively, because qualitative risk analysis is a quick analysis and is relatively easy to use to identify impacts (*Impact*) and likelihood (Likelihood) that can be used as material for risk evaluation [13]. In qualitative risk analysis, the process of determining priorities for analysis is carried out by combining the probability of risk occurrence and impact. When the probabilities and impacts have been identified, an evaluation will be carried out to determine the risks that must be addressed first or the risks that have the highest priority (high-priority risk).

TABLE I
LIKELIHOOD CRITERIA

Likelihood		Information	percentage
Rating	Criteria		
1	Rare	Risk almost never happens	0 - 10%
2	Unlikely	Risk is rare	> 10% - 30%
3	possible	Risk sometimes happens	> 30% - 50%
4	likely	Risk often occurs	> 50% - 70%
5	certain	Risk is bound to happen	>70%

TABLE II
IMPACT CRITERIA

Impact		Information
Rating	Criteria	
1	Insignificant	Does not interfere with organizational activities and operations
2	Minor	Activities are disrupted but do not hinder the core activities of the organization
3	Moderate	Activities are disrupted so that it inhibits core activities and experiences delays
4	Major	Inhibits almost all organizational business activities and processes
5	Catastrophic	Having a total disruption so that the activity stops completely and the organization's business processes are not achieved

4) Risk Treatment

At this stage there are several strategies for risk management, namely:

a. Avoid

This strategy is a step to eliminate the possibility of a risk occurring, by not doing or continuing activities that may pose a risk

b. Share

is a strategy that transfers or shares the impact of risk and responsibility to one or more third parties, this strategy only transfers the risk not eliminates it

c. Receive or retain

This strategy is used if the company has decided to accept the risk with certain considerations, which are still within the reasonable limits that can be accepted by the organization

5) Monitoring and Review

This is a stage carried out throughout the risk management process where routine monitoring of all running processes is carried out

6) Recording and Reporting

At this stage, every risk management process is carried out, and records and documents are collected to become evidence and reports that activities have been carried out.

III. Result and Discussion

A. *Risk Identification*

Based on the results of interviews and data collection from several documents, 20 risks may occur and are classified into 2 types, and the risks are categorized in the "R" code

TABLE III
MAIN RISK

Context	RC	Question
INTERNAL	R1	System Not Responding Or Time Out
	R2	The System Doesn't Run Due To The Company's Environment
	R3	System Accessed Something Unauthorized
	R4	Server Down
	R5	Incorrect System Data
	R6	System Bugs
	R7	Hardware Damage
	R8	Lost Or Stolen Device
	R9	There Is A Virus
	R10	Unscheduled Maintenance
	R11	Slow System Responding
	R12	Customer Request
	R13	Case Of Fire
EXTERNAL	R14	Float
	R15	Earthquake
	R16	Landslide
	R17	Hurricanes
	R18	Terrorism
	R29	There Was A Pandemic That Made The System Problematic
	R20	Affected By Hackers And Cybercrime Attacks

B. *Risk Analysis*

1) Impact and Likelihood analysis

the parameters used are likelihood and impact criteria, these parameters are used as an assessment of the XYZ bank application service

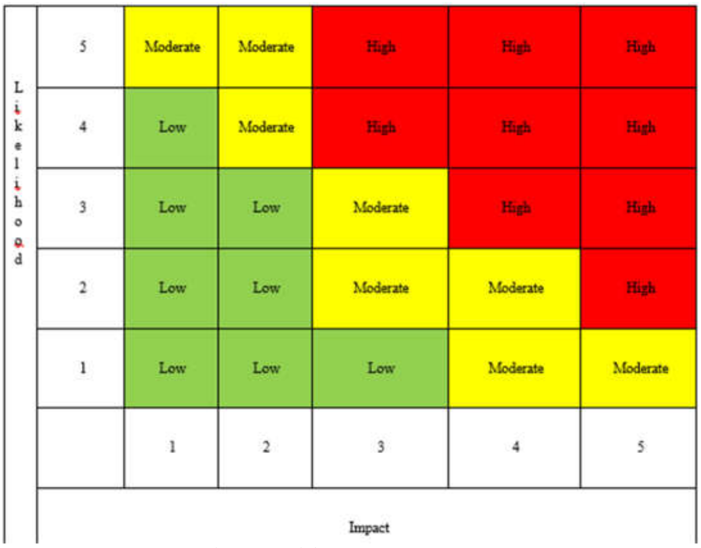
TABLE IV
RISK ASSESSMENT

Context	RC	Question	Impact	Probability
Internal	R1	System Not Responding Or Time Out	3	3
	R2	The System Doesn't Run Due To The Company's Environment	4	2
	R3	System Accessed Something Unauthorized	4	3
	R4	Server Down	4	3
	R5	Incorrect System Data	4	2
	R6	System Bugs	3	3
	R7	Hardware Damage	3	3
	R8	Lost Or Stolen Device	3	2
	R9	There Is A Virus	4	3
	R10	Unscheduled Maintenance	3	3
	R11	Slow System Responding	3	4
	R12	Customer Request	1	5
	R13	Case Of Fire	5	1
EXTERNAL	R14	Float	4	3
	R15	Earthquakes	5	4
	R16	Landslides	2	2
	R17	Hurricanes	4	4
	R18	Terrorism	5	1

R19	There Was A Pandemic That Made The System Problematic	4	1
R20	Exposed To Hacker Attacks And Cybercrime	5	2

2) Risk Analysis

based on the results of the assessment conducted at bank XYZ, a risk analysis was carried out to map the value of the risk, which in this analysis used three levels, namely, low, moderate, and high. This mapping is useful for determining the priority level of the risk so that it can be handled properly



Likelihood						
	5	Moderate	Moderate	High	High	High
	4	Low	Moderate	High	High	High
	3	Low	Low	Moderate	High	High
	2	Low	Low	Moderate	Moderate	High
	1	Low	Low	Low	Moderate	Moderate
		1	2	3	4	5
	Impact					

Figure 2. Risk Map

TABLE V
RISK MAPPING RESULT

Context	RC	Question	Analysis
Internal	R1	System Not Responding Or Time Out	Moderate
	R2	The System Doesn't Run Due To The Company's Environment	Moderate
	R3	System Accessed Something Unauthorized	High
	R4	Server Down	High
	R5	Incorrect System Data	Moderate
	R6	System Bugs	Moderate
	R7	Hardware Damage	Moderate
	R8	Lost Or Stolen Device	Moderate
	R9	There is a virus	High
	R10	Unscheduled Maintenance	Moderate
	R11	Slow System Responding	High
	R12	Customer Request	Moderate
	R13	Case of fire	Moderate
External	R14	Float often occur?	High
	R15	frequent earthquakes?	High
	R16	Do landslides often occur?	Low

R17	frequent natural disasters, strong winds, hurricanes?	High
R18	the occurrence of terrorism	Moderate
R19	there is a pandemic that makes the system problematic	Moderate
R20	exposed to hacker attacks and cybercrime	High

Based on table V , the risks found are mostly at moderate and high levels. there is also a risk at the low level, namely R16

3) Risk Evaluation

The results of the assessment of the risk evaluation are based on the values obtained in the risk mapping and the determination of risk priorities is carried out. the priority level is determined based on the following categories.

TABLE VI
RISK PRIORITY PARAMETERS

Risk rating	Priority	Description
1	Low	The repair can be delayed, but the impact is small on the organization
2	Moderate	Can be repaired immediately, can also be postponed, and the impact is moderate for the organization
3	High	It must be repaired as soon as possible, the impact is very disturbing

TABLE VII
RISK EVALUATION RESULT

Risk rating	Priority	Risk Code
1	Low	R12
2	Moderate	R1,R2,R5,R7,R8,R10,R11,R14,R16,R19
3	Priority	R3,R4,R9,R13,R15,R17,R18,R20

The priority risks are internal risk (R3, R4, R9, R13) and external risk (R15, R17, R18, R20). This risk must be handled as soon as possible because it will affect the performance of application services and have a big impact on the application of XYZ Bank E-Banking services. Risks in the moderate category can be responded to directly but can also be delayed because the impact is not too large and does not affect the performance of application services too much. And for risks with low priority, the handling can be delayed because the impact given by the risk is not too large or even small when the risk arises

4) Risk Treatment

To take action when the possibility of such risk occurs in XYZ Bank, each risk has its own treatment

TABLE VIII
RISK TREATMENT

Priority level	Risk Code	Risk Treatment
priority	R3	limitation of granting access to the system
	R4	perform scheduled server checks
	R9	use third parties as guarantors and protection such as antivirus
	R13	provide emergency extinguishers, server rooms are separate and specially protected
	R15	specially protected server room, and perform server data backup
	R17	add emergency power generator
	R18	improve the quality of security in the office environment
	R20	software security updates regularly and can use third parties to help software security
Moderate	R1	do periodic system checks
	R2	employee behavior must be considered
	R5	Have a data checkers
	R7	have at least 5 pcs hardware backup for each component
	R8	perform regular device checks
	R10	perform maintenance scheduling when the application is not busy in use
	R11	perform application garbage cleaning and software updates
	R14	improving the quality of water drainage around the office environment
	R16	add a server in another location as a backup
	R19	maintain and pay attention to the health of employees who are responsible for the system
Low	R12	receive customer feedback or requests for E-banking application development

IV. CONCLUSION

However, to see the overall risk that may not be seen by the organization, risk management is carried out based on industry, Based on the results of the risk assessment using the ISO 31000 framework[14]. The risk analysis process is carried out using the risk assessment stage through 3 processes, namely, risk identification, risk analysis, and risk evaluation. and the stages of risk treatment where the results are useful as suggestions for risk treatment for possible risks that occur in Bank XYZ application services[15]. 20 risks may occur in Bank XYZ, and after being categorized the risks are divided into internal risks and external risks. After mapping the risk, it is now possible to determine the priority level based on the impact and probability of occurrence.

The prioritized risks in Bank XYZ's E-banking service are R3, R4, R9, R13, R15, R17, R18, and R20. where this risk must be handled as quickly as possible so that nothing detrimental happens to Bank XYZ because this risk has a very large risk for Bank XYZ.

But in this study, the results obtained are not perfect because there may still be other possible risks in the same scope or a different scope. So there is a need for further research that looks at it from a different point of view to get better results than before.

REFERENCES

[1] M. Miftakhatun, “Analisis Manajemen Risiko Teknologi Informasi Pada website Ecofo Menggunakan ISO 31000,” Journal of Computer Science and Engineering (JCSE), vol. 1, no. 2, 2020.
[2] J. Simarmata et al., Pengantar Teknologi Informasi. Yayasan Kita Menulis, 2021.
[3] A. Rahmawati and A. F. Wijaya, “Analisis Risiko Teknologi informasi menggunakan ISO 31000 pada aplikasi ITOP,” Jurnal SITECH : Sistem Informasi dan Teknologi, vol. 2, no. 1, 2019
[4] H. W. Apriyanti, “Model Inovasi Produk perbankan syariah di Indonesia,” Economica: Jurnal Ekonomi Islam, vol. 9, no. 1, 2018.
[5] Kholis, N., 2020. Perbankan Dalam era Baru Digital. Economicus, 12(1)
[6] Masin, M. et al., 2022. Risiko Perkembangan teknologi perbankan syariah era millenial. Al-Azhar Journal of Islamic Economics, 4(1).
[7] Agustinus, Stefan., 2017, Analisis Risiko Tek¬nologi Informasi Menggunakan ISO 31000 pada Program HRMS, Jurnal RESTI Vol. 1 No.3,2017
[8] Leitch, M., 2010. ISO 31000:2009-The New International Standard on Risk Management. Risk Analysis, 30(6), pp.887-892.
[9] Rahmawati, A. and Wijaya, A., 2019. Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP. Jurnal SITECH : Sistem Informasi dan Teknologi, 2(1), pp.13-20.
[10] Gunawan, Imam. (2017). Metode Penelitian Kualitatif. Edisi Pertama. Cetakan Kelima. Jakarta:Bumi Aksara.
[11] W. O. Norlita and A. D. Rarasati, “Risk analysis of microfinance conversion based on ISO 31000 Pt. Bank Bri Syariah. Tbk Aceh,” RSF Conference Series: Business, Management and Social Sciences, vol. 1, no. 5, 2021.
[12] B. Barafort, A.-L. Mesquida, and A. Mas, “Integrated Risk Management Process Assessment Model for IT organizations based on ISO 31000 in an ISO multi-standards context,” Computer Standards & Interfaces, vol. 60, 2018.
[13] B. Barafort, A.-L. Mesquida, and A. Mas, “ISO 31000-based Integrated Risk Management Process Assessment Model for IT organizations,” Journal of Software: Evolution and Process, vol. 31, no. 1, 2018.
[14] Norlita, W. O., & Rarasati, A. D. (2021). Risk Analysis of Microfinance Conversion Based on ISO 31000 PT. Bank BRI Syariah. Tbk Aceh. RSF Conference Series: Business, Management, and Social Sciences, 1(5), 125–134.
[15] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, “Manajemen Risiko teknologi informasi Menggunakan ISO 31000 : 2018 (Studi Kasus: Cv. XY),” Sebatik, vol. 23, no. 1, 2019.