EasyChair Preprint

№ 6263

IT Risk Management Based on ISO 31000 in the BRImo Application (BRI Mobile) as an E-Banking Transaction Information System

Fatma Wati, Sarmila Sari and Joy Nashar Utamajaya

August 9, 2021

IT Risk Management based on ISO 31000 in the BRImo Application(BRI Mobile) as an E-Banking Transaction Information System

Fatma Wati[1] , Sarmila Sari[2] , Joy Nashar Utamajaya S.Kom.,M.M.S.I [3]
[1,2,3] Sistem Informasi , STMIK Borneo Internasional Balikpapan
Jl. AW. Syahranie No.04, RT.32, Batu Ampar, Kec. Balikpapan Utara, Kota Balikpapan, Kalimantan Timur 76136
Fatmawati.18@stmik-borneo.ac.id[1],sarmila_sari.18@stmik-borneo.ac.id[2],Joy.nashar@stmik-borneo.ac.id[3]

Abstrak– BRImo application is a software support system owned by Bank bri in order to increase profits and provide maximum service to customers. With the BRImo application, it can make it easier for customers to register for new account openings and e-banking transactions anywhere without being limited by space and time. However, implementing information technology is not without risk, because banks are a highly regulated industry and must be carried out prudently. With the growing complexity of BRI's business activities and operations, the risks faced are also getting bigger. Threats that arise to operational activities can be triggered by various factors, both internal and external. Therefore, there is a need for risk management analysis on the BRImo Application using the ISO 31000 framework so that the possible risks that will occur can be minimized or eliminated by carrying out Risk Assessment and Risk Treatment. The results of this study are various possible risks in the identified application using a probability and impact matrix as well as the handling of the possible risks that exist. So that the results of this risk analysis can be used to help companies prevent, minimize risks and treat these risks according to their priorities before the possibility of these risks hampering the company's performance.

Keyword: BRI Bank, BRImo Application, IT Risk Management, ISO 31000 Framework, Risk Assessment, and Risk Treatment.

PRELIMINARY

The use of smartphones today is a very important need for society. The high number of public interest in the use of applications to facilitate human activities both in transactions and shopping online has made agencies, both government and private, compete to innovate to continue to improve their services through digital services. Based on data from the Ministry of Communication and Information (Kemenkominfo) states that internet or smartphone users in Indonesia reach 167 million people or about 89% of the total population of Indonesia [1].

The rapid growth of smartphone users in Indonesia has a positive impact on the business world, including the banking sector where the use of technology can make it easier for banks to provide better services to their customers by launching information technology-based banking transaction services, namely mobile banking. The m-banking service opens up opportunities for customers to conduct banking transactions via mobile devices or Personal Data Assistants (PDA)[2].

Mobile banking is a banking service facility provided by the bank to customers to carry out various banking transactions through various features available on smartphones. The services contained in mobile banking consist of payments, history, transfers, and others. The use of mobile banking services on cellular phones allows customers to more easily carry out their banking activities without the limitations of space and time. With the mobile banking service, it is expected to provide convenience and benefits for customers in accessing the bank without having to come directly to the bank [3].

The current digital era has changed conventional services to digital. Digitization services not only facilitate customers with machines, but also make customers transact quickly, frictionless, and provide satisfaction (customer experience). One of the Indonesian banks that has implemented mobile banking-based digital services is Bank Bri. Bank Bri realizes that the role of information technology is very important and if they don't keep up with the times, they will be displaced by other banks that first implement digital m-banking services, especially considering that the pattern of people's life needs has also changed.

Bank Rakyat Indonesia (BRI) as one of the state-owned banks is very concerned about the times in improving the quality of banking services to customers. this is proven by presenting the latest

service technology innovation, namely BRImo or BRI Mobile which has a security system that is better than BRI Mobile because this application applies user interface (UI) and user experience (UX) technology. BRImo is the latest mobile application development from the previous BRI Mobile application and has been used by 2.2 million customers in just 8 months since it was launched in February 2019 ago[4]. BRImo is a media for finding new customers, especially millennials who use smartphones a lot.

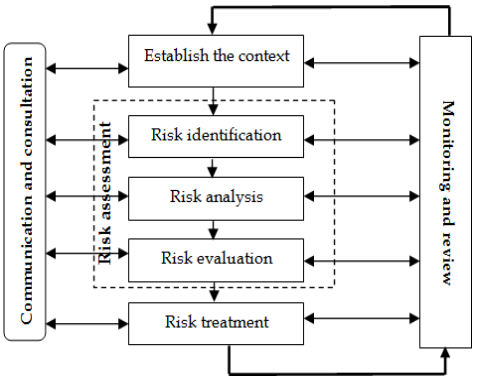
The BRImo or Bri Mobile application has several advantages that are offered to customers in facilitating e-banking transactions such as BRImo providing convenience in opening new accounts with the application, customers can view account mutations without using a passbook for the last 1 year of use which can be saved via PDF file and can be shared via Whatsapp chat, login with finger print/face recognition, and have access to promo info. The BRImo application has also combined the functions of mobile banking, internet banking, and electronic money (Tbank) in one application with a more complete and attractive transaction menu.

However, every application that is an important asset for the company must have the possibility of risks that can interfere and make the application not run optimally, and the BRImo application is no exception. Risk is the possibility of an event occurring that can result in a loss for the company. Tugiman (2009), defines risk as an adverse event or not achieving the expected goals [5]. Risk is related to uncertainty. This uncertainty occurs because of the lack or unavailability of information regarding what will happen. In a company, adverse uncertainty is called risk. The risk that is often an obstacle in the BRImo application can be triggered by various factors, both internal and external.

In identifying risk management in the BRImo application at BRI Indonesia, the appropriate guideline to be used in this research is to use ISO 31000. ISO 31000 is a standard related to risk management issued on November 13, 2009 by the International Organization for Standardization (ISO) [6]. This standard is intended to be applicable and adapted for all types of organizations by providing a generic structure and guidelines applicable to all operations related to risk management.

RESEARCH METHODS

A. Risk Management



Picture 1. Risk Management (ISO 31000)

International Organization for Standardization (ISO) 31000 as shown in figure 1 below, is a standard that was developed with the aim of providing universal risk management principles and guidelines. In the International Organization for Standardization (ISO 31000:2009) there are 2 stages in the risk management process. The first stage is risk assessment, which is the process of determining the risks that have the potential to prevent the company from achieving its business goals. In the risk assessment stage, there are 3 processes, namely risk identification, risk analysis, and risk evaluation.

1) Risk Identification: At this stage includes identification of risks that may occur in an activity. Identification carried out accurately and completely is vital in risk management. It is an important aspect of risk management. Techniques that can be used are interviews, surveys, historical information and others.
2) Risk Analysis (Risk Analyst): This stage looks at the potential risk, how much damage occurs in the risk. The probability of an event is very subjective and is based more on experience and reason
3) Risk Evaluation: At this stage, it is carried out to determine risk management by comparing the level of risk to a predetermined standard. The purpose of risk evaluation is to know the priority level from high to low and to know which level of risk must be followed up and which are monitored

The next stage is Risk Treatment. This stage is an effort to complete options that can reduce or even eliminate the possibility and impact of the risks that occur and apply treatment.

B. Research Method

The method used in this study uses a qualitative method which is carried out by identifying risks to determine the potential risks that exist in the BRImo application. The qualitative method chosen aims to explore and understand the meaning that comes from social or humanitarian problems. In the qualitative research process, things are done such as asking questions to resource persons, collecting specific data from the field and resource persons, then analyzing the data that has been obtained inductively.

The research was conducted by conducting interviews with IT staff or BRI bank employees at the North Penajam Paser Branch by asking various questions about the function of the BRImo system, what data and features are in the BRImo system, what possible risks can occur in the BRImo application, how to do it. overcome the risks that arise in the BRImo application, then the data needed focuses on the BRImo system used by the company to run its business.

RESULTS AND DISCUSSION

A. Risk Assessment

The risk assessment stage is the first stage carried out in research in accordance with the ISO 31000 risk management analysis guidelines. This stage is used in assessing the BRImo application which consists of 3 processes carried out namely risk identification, risk analysis, and risk evaluation. These three processes must be passed to go to the next stage.

1. Risk Identification

   a. Identify BRImo Application Assets

   The first process in the risk assessment stage is the process of risk identification or asset identification related to the BRImo application which is carried out through an interview process with IT Operation Support, Staff Manager, and employees at the BRI Bank Penajam Paser Utara Branch. At this stage, identification of assets from data, software to hardware related to the BRImo application is carried out.

Table 1. Identification of Assets in the BRImo Application

Information System Components	BRImo Application Assets
Data	Customer Data, Asset Data
Software	BRImo app
Hardware	Personal Computer (PC), Server Database, Server Web Service

b. BRImo Application Risk Identification

After identifying the assets associated with the BRImo application, the next thing that needs to be identified is the possible risks surrounding the BRImo application. The causes of risk can arise from several factors, these factors include the environment or nature, humans, systems and infrastructure. And don't forget to be given an identity for every possible risk found. The following is Table 2 identification of possible risks

Table 2 identification of possible risks

Source of Risk	**Risk Code**	**Possible Risk**
Nature or Environment	R01	Flood
	R02	Fire
	R03	Earthquake
	R04	Lightning
Human	R05	Application can't run
	R06	Damage caused by human activities (cybercrime and vandalism)
	R07	Information accessed by unauthorized parties
	R08	Error Input data in the application
	R09	Device or data theft
	R10	The appearance of the application is not user friendly

System and infrastructure	R11	Server Down
	R12	Full Memory
	R13	Bug In System or Application
	R14	Hacking against the network
	R15	Virus Attack
	R16	Slow response system performance
	R17	Error when inputting data in the application
	R18	No periodic maintenance Maintenance
	R19	Logout system automatically
	R20	Hardware Damage

From the results of the risk identification process, it was found that there were 20 possible risks originating from natural/environmental factors, humans, systems and infrastructure that could potentially affect the delay in the use of the BRImo application. Then the possible risks that have been identified are identified their impact on the company.

c. Identification of BRImo Application Risk Impacts

Table 3. Identification of risk impacts

Risk Code	**Possible Risk**	**Risk Impact**
R01	Flood	The company's business activities are hampered.
R02	Fire	The company's infrastructure is damaged and the company's business activities are stopped
R03	Earthquake	Damage to the Company's infrastructure and hampered business activities
R04	Lightning	Damage to Company infrastructure, lost network connection
R05	Application can't run	Slow down business performance, targets are not met
R06	Damage caused by human activities (cybercrime and vandalism)	Financial loss/company data information
R07	Information accessed by unauthorized parties	Data can be manipulated and then disseminated to the public but does not match the existing real data.
R08	Error Input data in the application	The inputted data becomes invalid
R09	Device or data theft	The company lost in terms of information and financial terms.
R10	The appearance of the application is not user friendly	Application users or Bri customers have difficulty operating the BRImo application
R11	Server Down	Unable to access BRImo and database.
R12	Full Memory	New customer incident failed to be accommodated.
R13	Bug In System or Application	Errors in system performance, causing system crashes
R14	Hacking against the network	Business activities are disrupted and hamper the business performance of the Company
R15	Virus Attack	Resulting in corrupt data or bugs in the BRIMO application
R16	Slow response system performance	Performance is not optimal, the achievement of the Company's targets is not met
R17	Error when inputting data	Targets are not met, hindering the business

	in the application	performance of the company
R18	No periodic maintenance Maintenance	Unable to determine the cause of the hardware failure.
R19	Logout system automatically	Re-entering unsaved data, slowing down the business workflow of the Company
R20	Hardware Damage	Inhibiting the process of operating the BRImo application

2. Risk analysis

The Risk Analysis is the second process or process after the completion of risk identification, which is the risk analysis process. The risk analysis process is the process of measuring risk by looking at two aspects, namely the possibility of how much damage occurs (impact) and how often the risk occurs (likelihood). The results of the risk analysis process can be used as suggestions in the risk evaluation process and in the process of managing existing risks. In this process there are two tables, namely the impact table and the likelihood table. Table . Likelihood criteria are in "Table 4" while the Impact table is in "Table 5"

Table 4. Likelihood Criteria

Likelihood		Information	Frequency of occurrence
Value	Criteria		
1	Rare	This risk almost never occurs	> 2 tahun year
2	Unlikely	This risk is rare	1 – 2 year
3	Possible	This risk happens sometimes	7 – 12 months
4	Likely	This risk often occurs	4 – 6 Months
5	Certain	The risk is bound to happen	1 – 3 Months

The probability value in Table 4. has 5 values, namely the first is Rare, Unlikely, Possible, Likely, and Certain. Rare is the smallest possible value and almost never occurs. The highest possible value is Certain, which is the risk that occurs most often.

Table 5. Risk Impact

Impact		Information
Value	Criteria	
1	Insignificant	Risk Does not interfere with company activities
2	Minor	The company's activities were slightly hampered but the company's core activities were not disrupted.
3	Moderate	Causing disruption to business processes so that part of the company's activities are hampered.
4	Major	Inhibits almost all company activities
5	Catastrophic	The company's activities stopped because the business processes experienced total disruption

The Impact Value table above also has 5 values, namely Insignficant, Minor, Moderate Major and Catastrophic. Insignficant is the lowest impact value and Catastrophic is the highest impact value because it greatly disrupts existing business activities. Risk does not interfere with company activities.

After the probability and impact values have been determined, the next step is to conduct a one-by-one assessment of the possible risks that exist in the BRImo application. Of the 20 possible risks, the likelihood and impact values are determined one by one based on the table reference made previously which can be seen in detail in table 6.

Table 6 Assessment of possible risks with likelihood and impact

Risk Code	**Possible Risk**	**Likelihood**	**Impact**
R01	Flood	1	2
R02	Fire	1	2
R03	Earthquake	1	5
R04	Lightning	2	1
R05	Application can't run	3	3
R06	Damage caused by human activities	4	3

	(cybercrime and vandalism)		
R07	Information accessed by unauthorized parties	3	2
R08	Error Input data in the application	4	1
R09	Device or data theft	2	3
R10	The appearance of the application is not user friendly	2	1
R11	Server Down	5	5
R12	Full Memory	2	3
R13	Bug In System or Application	4	3
R14	Hacking against the network	1	2
R15	Virus Attack	3	5
R16	Slow response system performance	5	3
R17	Error when inputting data in the application	4	2
R18	No periodic maintenance Maintenance	3	5
R19	Logout system automatically	4	2
R20	Hardware Damage	3	4

3. Risk evaluation

The last process to complete the risk assessment stage is the risk evaluation process. In this process, a reference is used in the form of a risk evaluation matrix. Where in the matrix is divided into 3 risk levels, namely low, medium and high. Possible risks that have been determined by the likelihood value and impact value in the previous process will be differentiated again according to the existing matrix. Table 7 has mapped risk levels based on likelihood and impact

Table 7. Risk Evaluation Matrix

Likelihood	**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
Impact			**1**	**2**	**3**	**4**	**5**
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**

Each possible risk based on likelihood and impact will be entered into the risk evaluation matrix by looking at the mapping in the previous risk evaluation matrix table. In the identity risk evaluation matrix table, each possible risk is entered into parameters according to the likelihood criteria and impact criteria that were carried out previously.

Table 8. Risk evaluation matrix based on likelihood and impact

Likelihood	**Certain**	5			R16		R11
	Likely	4	R08	R17 R19	R06 R13		

	Possible	3		R07	R05	R20	R15 R18
	Unlikely	2	R04 R10		R09 R12		
	Rare	1			R01 R02 R14		R03
Impact			**1** **Insignificant**	**2** **Minor**	**3** **Moderate**	**4** **Major**	**5** **Catastrophic**

Then after all the possible risks are entered into the risk evaluation matrix in table 9, it will be described from the 20 possible risks that exist in the BRImo application whether they are included in the level of risk with high, medium or low levels based on likelihood and impact criteria.

Table 9. Risk level of possible risks

Risk Code	Possible Risk	Likelihood	Impact	Risk Level
R01	Flood	1	2	Low
R02	Fire	1	2	Low
R03	Earthquake	1	5	Medium
R04	Lightning	2	1	Low
R05	Application can't run	3	3	Medium
R06	Damage caused by human activities (cybercrime and vandalism)	4	3	Medium
R07	Information accessed by unauthorized parties	3	2	Medium
R08	Error Input data in the application	4	1	Medium
R09	Device or data theft	2	3	Medium
R10	The appearance of the application is not user friendly	2	1	Low
R11	Server Down	5	5	High
R12	Full Memory	2	3	Medium
R13	Bug In System or Application	4	3	Medium
R14	Hacking against the network	1	2	Low
R15	Virus Attack	3	5	High
R16	Slow response system performance	5	3	High
R17	Error when inputting data in the application	4	2	Medium
R18	No periodic maintenance Maintenance	3	5	High
R19	Logout system automatically	4	2	Medium
R20	Hardware Damage	3	4	Medium

Based on Table 8 above, it can be seen that from the 20 possible risks identified, there are 4 out of 20 possible risks that have a high level, namely, Server Down, Virus Attacks, Slow system performance responding, and no periodic maintenance Then there are 11 possibilities that have a medium level, namely Earthquakes, Applications cannot be run, Damage caused by human activities (cybercrime and vandalism), Information accessed by unauthorized parties, Data input errors in applications, Device or data theft, Memory Full, System or Application Bugs, Errors when inputting data on applications, System Logout automatically, and Hardware Damage. While the possibility of risk at the Low level has 5 possibilities, namely floods, fires, lightning, the appearance of the application is not user friendly, and network hacking.

B. Risk Treatment

The stage after risk identification is the risk treatment stage. At this stage, what will be done is to provide suggestions regarding treatment for all possible risks that exist in the BRImo application. The treatment suggestions given are expected to

reduce or minimize the possible risks that exist. It can also be used by BRI Bank to prevent possible risks in the BRImo application. Risk treatment is arranged based on the level of risk that has been previously identified, from a high level of risk to a low level of risk, the details of the proposal can be seen in table 10 below.

Table 10. Risk Treatment

Risk Code	Possible Risk	Level	Risk Treatment
R11	Server Down	High	Check in the database and Refresh BRImo application.
R15	Virus Attack	High	Install a good and reliable antivirus, limit access so that not just anyone can access the application's Main Database and Server
R16	Slow response system performance	High	Refresh the system, check the system regularly
R18	No periodic maintenance Maintenance	High	There is a need for a regular hardware maintenance schedule, with a hardware maintenance schedule, technicians can monitor which hardware needs to be repaired and replaced with new hardware.
R03	Earthquake	Medium	Provide a backup server in another place / location that is more secure
R05	Application can't run	Medium	Immediately make repairs when the application dies / service and immediately provide announcements to customers.
R06	Damage caused by human activities (cybercrime and vandalism)	Medium	Change server passwords periodically.
R07	Information accessed by unauthorized parties	Medium	Conduct regular password maintenance in case of suspicious things.
R08	Error Input data in the application	Medium	Correcting errors, providing data editing features on the system, checking before running
R09	Device or data theft	Medium	Passwords are changed periodically. Do not tell other people important data such as ATM PINs to avoid irresponsible users.
R12	Full Memory	Medium	Check memory usage periodically and Increase memory capacity before it is full.
R13	Bug In System or Application	Medium	Checking the system, conducting periodic system testing, there is an IT staff in the customer service department who handles bugs in the system
R17	Error when inputting data in the application	Medium	Refresh the system if an error occurs when inputting
R19	Logout system automatically	Medium	Perform repairs and perform system performance tests
R20	Hardware Damage	Medium	Clean the hardware and immediately report to the technician if a problematic hardware is found

R01	Flood	Low	Put the server in a place that is difficult to reach by flooding (at higher ground), Have a backup server in a different place
R02	Fire	Low	Installing a backup server in a different location
R04	Lightning	Low	Installing a lightning rod, Automatically backing up the main server into the backup server
R10	The appearance of the application is not user friendly	Low	Make improvements by changing the user interface of the application that is easy to understand with the right color selection
R14	Hacking against the network	Low	Set complex passwords for every important part of the app

CONCLUSIONS

The stages of risk management analysis on the BRImo application at BRI banks based on the International Organization for Standardization (ISO 31000:2009) have been carried out. The risk analysis process is carried out from the risk assessment stage through 3 steps, namely risk identification, risk analysis, and risk evaluation. And the risk treatment stage is to make suggestions for risk treatment for the possible risks that exist in the BRImo application.

From the results of the risk analysis, it can be seen that there are 20 possible risks that have the potential to disrupt the performance of the BRImo application. There are 4 possible risks that are included in the level of risk high out of 20 possibilities, namely, Server Down, Virus Attacks, System performance that is slow to respond, and No periodic maintenance. Then there are 11 possibilities that are included in the medium level of risk, namely Earthquakes, Applications cannot be run, Damage due to human activities (cybercrime and vandalism), Information accessed by unauthorized parties, Errors in data input in applications, Theft of devices or data, Full Memory, System or Application Bugs, Errors when inputting data on applications, System Logout automatically, and Hardware Errors. And there are 5 possible risks that are included in the low level of risk, namely floods, fires, lightning, the appearance of the application is not user friendly, and network hacking.

From the results obtained, it can be seen that in overcoming the possible risks that exist in Bank BRI, BRI has implemented steps to minimize the impact of possible risks that often occur, but for system error problems, Bank BRI can monitor and perform regular maintenance on the BRImo application so that system error problems and possible risks can be minimized and business processes can run well.

SUGGESTION

After the researchers have completed the research on information technology risk management analysis using ISO 31000 on the BRImo application at BRI Bank, future researchers can conduct research with a wider scope so that the existing findings can be used by policy makers to compile documentation related to corporate risk management.

Because risk analysis is a part of IS/IT Governance, so if you only focus on risk management it will certainly not have an impact on the company, it is hoped that further studies will be carried out thoroughly so that the company truly aligns information technology with the company's strategy and realizes the benefits. IT (Benefit Realisation), maximizing IT resources (Resource Optimization) and risk management that is carried out appropriately and measurably (Risk Optimisation).

THANK-YOU NOTE

The author would like to thank God Almighty for the inclusion and strength that has been given so that the author can complete this journal. The authors also thank the supervisors and the BRI who are willing to take the time to conduct interviews and their closest friends. Once again,

thank you profusely to all those involved in writing who always provide support to the author.

REFERENCES

[1] BRI BANK, www.bri.co.id diakses pada 1 Februari 2012 Pukul 20.30

[2] Ayani, D. H. (2019). Berapa Pengguna Internet di Indonesia? Retrieved January 2, 2020, from https: // databoks. katadata. co.id /datapublish/2019/09/09/berapa-pengguna-internet-di-indonesia

[3] T. Ramdhany and R. A. Krisdiawan. 2018, Analisis Risiko Sistem Informasi Penjualan Berbasis Iso 31000 - Risk Management di PT. Remaja Rosdakarya, Teknol. dan Manaj. Inform., Vol. 3, No. 1, pp. 1–7

[4] G. W. Lantang, A. D. Cahyono, and N. Ngalumsine, 2019, Analisis Risiko Teknologi Informasi pada Aplikasi SAP di PT Serasi Autoraya Menggunakan ISO 31000, Sebatik 2621-069X, Vol. 23 No. 1, pp. 36–43

[5] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi ITOP," J. SITECH Sist. Inf. dan Teknol., Vol. 2, No. 1, pp. 13–20, 2019, doi: 10.24176/sitech.v2i1.3122

[6] A. N. Rilyani, Y. AW Firdaus, and D. D. Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000," e-Proceeding Eng., Vol. 2, No. 2, pp. 1–8, 2015.