Journal of Theoretical and Applied Information Technology
31st May 2019. Vol.97. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE IMPLEMENTATION OF SYSTEM ENTERPRISE RISK MANAGEMENT USING FRAMEWORK ISO 31000

[1]GEDE WISNU ARTA SUYASA, [2]NILO LEGOWO
Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University, Jakarta Indonesia
E-mail: [1]gede.suyasa@binus.ac.id, [2]nlegowo@binus.edu

ABSTRACT

Enterprise Risk Management is very important in a company because it can have a very important impact on information systems in the company. The purpose of this study is to analyze the risk of risk management information systems especially on financial technology which is based on the level of risk that is happening and also measure the level of maturity that has been applied whether it is in line with the expected target of one of the state-owned banks. this research uses ISO 31000 standard, observations, audit check lists, and interviews. In this risk management information system analysis will focus on 7 domains. The results of this study indicate that the level of risk faced by Bank XYZ is at the highest risk level. so that Bank XYZ must take control to overcome these risks. Information system maturity level at Bank XYZ has an average value of 3.00 which explains that it is still in the defined stage. While the target expected by Bank XYZ is 4.00. The gap of 1.00 must be a concern, because the level of risk arises due to the maturity level of the Bank XYZ system that has not been fulfilled.

Keywords: *Information System Risk Management, Financial Technology, Enterprise Risk Management, ISO 31000, Maturity Level.*

1. INTRODUCTION

Every company will always face risks in its business processes. Both actions taken and decisions taken by managers or company leaders will contain or bring risks [1]. Risks will arise with uncertainty. If everything can be ascertained with a hundred percent accuracy rate then it is very unlikely. Therefore the possibility of risk will always arise [2].

Responding to this risk management is a very important thing to be realized so that risk can be mitigated. The use of technology will be able to reduce the risks that occur [3] but this does not guarantee because technology is also not independent of the risks that will be caused [4]. The essence of the use of technology that is the main technology is to be efficient and effective in its business processes [5].

The existence of technology provides an important role in facing competition and is important in improving the economy of a country. The application of technology in banking to serve financial services is called financial technology [6]. According to the financial stability board, financial technology is a technology that enables financial innovation that can produce new business models, applications, processes, or products related to financial markets and institutions and financial service provision [7]. The purpose of applying technology can increase productivity and efficiency in the banking itself. In line with developing a banking, the more data.

The application of technology affects the level of productivity in the banking sector [8]. The effect of applying technology to the banking sector can be seen from the use of internet banking, credit cards, cash deposit machines and electronic fund transfers.

One of the banks that applies financial technology is Bank XYZ as the bank that has the largest number of branches, units and the number of Automated Teller Machines (ATMs) in Indonesia. This was evidenced by the data of the Financial Services Authority (OJK) in 2016, with 466 Bank XYZ branch offices, 5964 sub-branch offices and 23,587 units of Bank X ATM in Indonesia. Bank XYZ innovates in the form of E-Banking.

To support E-banking, in 2017, Bank XYZ has realized an IT investment budget of around 666.2 billion Rupiah. This budget amount is 53% of Bank XYZ's 2017 capital expenditure. Therefore,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

this IT investment will be able to develop E-banking at Bank XYZ.

Adoption of digital-banking services has increased rapidly throughout Asia [9]. Customers switch to computers, smartphones and tablets in their interactions with banks making activities to visit branch offices and communicate via telephone lines to enjoy banking services, much reduced. Because of the large number of customers using online banking services, the risk aspect must be a priority considering that Financial technology will depend on digital networks (e-channels).

The high number of users and E-banking transactions there are risks faced by Bank XYZ, because the Bank increasingly relies on information technology and the internet to operate and market interactions. Bank XYZ innovates where it develops a service system in the form of E-Banking in launching all forms of banking transactions, but increasing transactions have the potential to increase the risk of technology, both for individuals and the banking financial industry. Threats in banking will be related to threats in the financial transaction side of the E-banking system can be seen in the following figure 1.

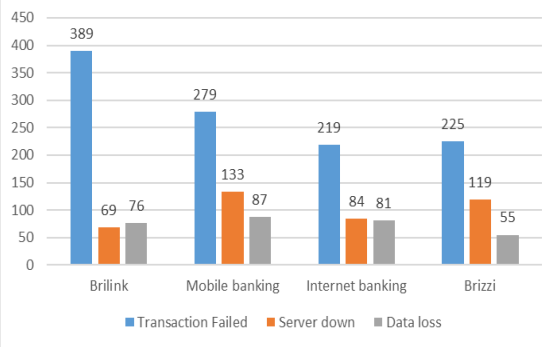

Figure 1. E-banking risks faced by Bank XYZ Branch Offices, 2017

Figure. 1 shows the many risks faced by Bank XYZ as financial service providers and providers of E-banking systems there are risk threats in transactions throughout 2017 in addition to the risks from the transaction side, there are risks from the side of the workers in the use of the system. To see how much risk is faced, see the following figure 2:

Figure 2. E-banking risks faced by Bank XYZ Branch Offices, 2017

Figure. 2 shows that throughout 2017, internal risks such as the infrastructure network have 4 cases, for the database there are cases, there are 6 power failures, there are 12 cases of viruses and hardware problems there are 12 cases. The existence of risks from the transaction and internal side must be mitigated and prevented from risk.

The existence of the concept of Enterprise Risk Management (ERM), then risk management must be implemented at all levels of the company and there is a clear structure in risk management in the company. Various companies in Indonesia, both private and state-owned enterprises, are trying to start implementing ERM by developing risk management policies and forming a risk management unit that is responsible for ensuring the implementation of risk management in the company in accordance with the established policies.

Based on the background of the problem, the formulation of the problem in the study identifies the risks that affect Bank XYZ's financial technology performance as follows: How to identify the risk factors that occur, and how to evaluate the risk based on maturity levels that can affect Bank XYZ's financial technology performance. The purpose of this study are as follows: Knowing in identifying any risk factors that affect Bank XYZ's financial technology performance, and risk evaluation based on maturity levels that can affect the performance of Bank XYZ's financial technology.

The limitations of the problems to be discussed in this study are as follows:

1. This research will be conducted on the IT system at the branch office at XYZ Bank.

2. This research is to collect data by distributing questionnaires with operational managers, IT officers.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. This research was conducted on the performance of XYZ Bank fintech which has been implemented since the beginning of January 2017.

2. RELATED WORK

This research requires an understanding of a number of theories to support or be the basis and references in the study. These theories are the results of various sources and literature.

2.1 Risk Management

Risk management is an activity that is directed to assess, reduce (to an acceptable level) and monitor risks associated with information [10]. The main purpose of the risk management process in the organization is to protect the organization and its ability to carry out their mission, not just IT assets. The emergence of risk management is not merely to avoid the danger of loss but also to seize opportunities [11].

According to the Regulation of the Minister of Finance of the Republic of Indonesia (OJK) number 12 / PMK.09 / 2016 article 1 number 3 is explained that the risk management process is the application of systematic management policies, procedures and practices on communication and consultation activities, context setting, risk identification, risk analysis, risk evaluation, risk mitigation, and monitoring and review [12].

The existence of objectives, benefits and principles of risk management implementation which are described through the Regulation of the Minister of Finance of the Republic of Indonesia (OJK) number 12 / PMK.09 / 2016 article 2 [12], namely:

a. increase the likelihood of achieving goals and improving performance.
b. encourage proactive management.
c. provide a solid foundation in decision making and planning.
d. improve allocation effectiveness and efficient use of organizational resources.
e. increase compliance with provisions.
f. increase stakeholder trust.
g. increase organizational resilience.

According Banasiewicz (2017) explain the Risk Management Standards ISO 31000 framework, and clarifies the concept of risk management of the company remains an exclusive target [13]. Business organizations continue to hope to change risk management efforts that focus on controlling historical costs as a source of true competitive advantage, but obstacles remain. The key between these obstacles is the continuous fragmentation of attempts to distort organizational difficulties, where known risks are focused on risk management, unknown threats oriented towards organizational resilience and self-imposed transformation, mindful change management continues to function as three independent research disciplines and organizational practice fields [13].

2.2 Enterprise Risk Management

The concept of Enterprise Risk Management (ERM) is the most effective way in an organization to manage a risk [14]. To see how much the benefits of ERM for the company can be seen from the explanation as follows:

1. Avoid the risk of financial difficulties
2. Increase risk management and level of awareness in choosing strategies and in decision making.
3. Reducing losses and increasing shareholder return capital and value.
4. Strengthening the level of trust in management towards operations, efficient governance, enhancing the company's reputation, and clarifying organizational decision making.

Enterprise Risk Management (ERM) is increasingly becoming an option as an organizational approach or framework to treat risk [15]. There are two ERM references, namely the COSO ERM framework and serial ISO 31000 [15]. COSO ERM is issued by the Committee of sponsorship of the Organization of the Trade Commission (COSO) while the ISO 31000 series is published by the International Organization for Standardization (ISO).

.

2.3 ISO 31000 Implementation Process

The process of implementing using ISO 31000 there are several stages of the process to get the desired results [11]. To see the process can be seen as follows:

2.3.1 *Determination of Context*

Basically the sequence of activities in this risk management process illustrates some basic concepts as follows:

1. The sequence of risk management stages describes the 'problem solving' cycle.
2. Risk management is preventive.
3. Risk management is in line with the concept of 'continuous improvement'.
4. Risk management focuses on the scope of the problem to be managed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.3.2 *Risk Identification*

The target of the risk identification stage is to make a comprehensive and broad list of risks that can affect the achievement of targets, both increasing, blocking, slowing or even frustrating the achievement of organizational goals [16]. At this stage, identification of risks to be managed is carried out. Identification must be carried out on all risks, both inside and outside the organization.

2.3.3 *Risk Analysis*

After risk identification is complete, the next step is processing data in the form of risk analysis. Risk analysis is an attempt to understand deeper risks. The results of this risk analysis will be input for risk evaluation and for the decision-making process regarding the treatment of these risks. Risk analysis includes activities that analyze the sources of risk and trigger the occurrence of risks, their positive and negative impacts, and the likelihood of their occurrence [17].

2.3.4 *Risk Evaluation*

Risk Evaluation aims to help the decision making process based on the results of the risk analysis that has been carried out [18]. The risk evaluation process will determine which risks require treatment and how the treatment priorities for those risks are risk allocation, risk mitigation, risk sharing or risk acceptance.

In evaluating the need for an assessment of the maturity level that explains the maturity of the information system process maturity that takes place in the company (in form / numbers) [19]. The overall maturity level is obtained from the identification of each maturity level in all the control objectives involved. For this reason, it is necessary to assess the score of each respondent, the writer uses a Likert scale that reflects the answer patterns 1, 2, 3, and 4 [20]. Then the data is obtained through distributing the questionnaire by means of each answer given a Likert scale. For the purposes of answers can be given a score with data as shown in the following Table 1.

Table 1. Applications in each class

Value	Description
1	Very bad
2	Not good
3	Good
4	Very good

In measuring the Bank XYZ maturity level, a questionnaire was used as a method of data collection that would have index values of each criterion on the measurements carried out using the following formula:

$$x = \frac{\sum \text{statements complience values}}{\sum number\ of\ maturity\ level\ complience\ value}$$

According to the research that has been implemented by Djatmiko, the scale of making the index has a mapping of the level of maturity models [21]:

- 0.00 - 0.49 is at the level of 0 (Non-Existent) There is nothing, incomplete every known process.
- 0.50 - 1.49 is at level 1 Initialization, there is evidence that the organization is aware of a problem that requires handling.
- 1.50 - 2.49 is at level 2 Repetition, the same procedure has been developed in the process - the process to handle a task, and followed by everyone involved in it. There is no training and communication from the standard procedure.
- 2.50 - 3.49 at level 3 Defined, procedures have been standardized, documented, and communicated through training. However, the implementation is handed over to each individual, so it is likely that irregularities cannot be detected.
- 3.50 - 4.49 is at level 4 Managed, measurement and monitoring of compliance with procedures, as well as taking action if the process does not work effectively, can be done. Process improvements are carried out constantly.
- 4.50 - 5.00 is at level 5 Optimized, the implementation of the process is carried out satisfactorily. This is the result of continuous process improvement and measurement of organizational maturity. Information technology is integrated with the work flow, and serves as a tool that improves quality and effectiveness. The organization is more renponsive in facing business competition.

2.3.5 *Risk Control*

Risk control involves identifying alternatives to risk control, analyzing existing options, controlling plans and implementing controls. Control alternatives that can be done Risk aversion, reduce probability, reduce consequences, risk transfer.

This alternative transfer of risk is carried out after calculating the benefits and losses. This risk transfer can be a risk transfer to the contractor. Therefore, in the contract agreement with the contractor, the scope of work must be clearly stated and also the risk to be transferred. In addition, the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

consequences that may occur can also be in transferring the risk with the insurance.

2.4 Risk Management in E-Banking

According to the International Standard for Organization risk management is the process of identifying risks, to information assets and organizational infrastructure, and taking steps to reduce risk so as to reduce the risk received [22]. When an organization relies on IT-based systems to stay afloat, information security and risk management must be part of an economy to make business decisions [23]. This decision is based on a trade-off between the cost of implementing an information system control and the benefits realized from the safe and available operation of the system.

According to BCBS, the management principles for electronic banking (e-banking) are divided into three components, namely Board Management, Security Control, Legal and Reputational Risk Management [24]. In this study will focus more on the Oversight Board Management because in this section will explain the strategies in risk taking faced by managers and IT officers who are responsible for the business strategy of the bank and the IT system in the future.

2.5 Risk Analysis using the Risk Matrix Method

According to Hyatt, one of the most popular and widely used risk analysis methods is the Risk Matrix Method [25]. In this method, two basic factors that influence the estimated value of risk are considered: the probability of bad events (predetermined event scenarios) and their consequences. Probability events occur in a conventional scale (usually 5 levels): from 1 that is the least likely event, to 5 that is the probability of a very high event, and the effect: from A that is a minor (very little) effect, to E is a large effect, disaster. To see this can be seen through the following table 2:

Table 2. Risk Matrix Scheme

	A	B	C	D	E
5	M	M	H	H	H
4	M	M	M	H	H
3	L	M	M	M	H
2	L	L	M	M	M
1	L	L	L	M	M

The letters refer to the risk area: small (L), medium (M), high (H). By using the risk matrix method, it is important to identify the expected opportunity categories and categories of losses in relation to the scale of the hazard analyzed (events) [26]. Keep in mind that the subjective selection of risk categories can be one of the weaknesses of this method. When using a three-level risk scale, a small risk is equivalent to the area of activity taken in the existing procedures, intermediate risk is de facto the same as the area under crisis / risk management (to reduce risk to an acceptable level), high risk equal with the area, where immediate evacuation of people at risk is recommended.

2.6 Risk Management Standards

Because risk management still has a very important role in supporting organizational activities, we need standards or references that govern governance of security information. There are several standards for risk management that lead to risk management such as COSO ERM, ISO 31000: 2009. To find out the comparison of standardization can be seen in the following:

Table 3 ISO 31000

Key Term	**ISO 31000:2009**
Scope	This International Standard provides principles and general guidelines on risk management that can be used by public, private or community companies, associations, groups or individuals. Therefore, this International Standard is not specific to any industry or sector.
Define risk management	Coordinated activities to direct and control the organization related to risk.
Risk management	Continue and repeat: • Set the context

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

process	• Identification • Analysis • Evaluation • Risk care • Monitor and review
Risk appetite	The amount and type of risk that the organization wants to manage or maintain.
Risk Assessment	The whole process of risk identification, risk analysis and risk evaluation.

Tablel 4 COSO ERM

Key Term	**COSO ERM**
Scope	concepts that are fundamental to how companies and other organizations manage risk, provide the basis for applications across organizations, industries and sectors. It focuses directly on achieving the objectives set by a particular entity and provides a basis for defining the effectiveness of a company's risk management.
Define risk management	influenced by the entity's board of directors, management, and other personnel, which are applied in strategic and company-wide settings, designed to identify potential events that can affect the entity, and manage risks to be within the risk appetite.
Risk management process	Internal environment Destination setting Event identification Risky task Risk response Control activities Info & communication Monitoring
Risk appetite	A large number of risks that an entity can accept in pursuing its mission or vision.
Risk Assessment	Risk is analyzed, considering possibilities and impacts, as a basis for determining how they should be managed. Risk is assessed inherently and residual based.

In Tables 3 and 4 explain the differences between ISO 31000 and COSO ERM as standardization in risk management. The comparison of this standardization will illustrate the main differences between ISO 31000 and the COSO ERM Framework.

According to Gjerdrum, D., & Peter, M. (2011) The COSO ERM framework is a complex, multi-layered, and complex directive that is difficult for many organizations to find [17]. ISO provides a leaner approach that is easier to digest. ISO is based on the management process, and through process adjustments for each organization, it is integrated into existing management and strategic initiatives. The COSO model is control and compliance based, and it contributes to it being difficult for traditional risk managers to embrace. If COSO is carried out by the organization's internal audit team, there is a problem having the program audited by the same person who applied it; ISO allows for independent audit functions to occur during the monitoring and review phase. COSO is written by auditors, accountants and financial experts; ISO is written by risk management practitioners and international standard experts.

Reviewing ISO and COSO together can provide opportunities for risk management practitioners and auditors to integrate and strengthen their activities. Depending on the views and success of your organization with COSO, it may be useful to review how ISO can provide an approach to designing a path that will be more effective in accelerating growth and profitability throughout the company.

2.7 Previous research

This previous research became one of the reference material for the author in conducting research so that researchers can enrich the theory used in reviewing the research conducted. The material used from several studies conducted by previous research as a reference in enriching the study material in the author's research. Many author describe using ISO 3100 and The results the framework described in ISO 31000 can also be adjusted and applied to manage risks associated with the project. Although projects often require specific time frames and criteria [16].

Other researchers found that The ISO 31000 model can explain the structure and consistency better in making decisions about risk management in the bank. It is possible to coordinate the direction of risk management with the overall strategy of developing and operating the bank of Kazakhstan. The adaptive model ISO 31000 aims to promote an integrated risk management system that can be the basis for increasing competitiveness and increasing the security of national banks [27].

In respect to determinants of ERM implementation, previous empirical studies [28] have found that the majority of sample companies Among the top 300 companies in Australia that implement ERM and use the ISO 31000 or AS / NZS 4360: 2004 framework. In addition, companies with complete ERM implementations apply ERM more broadly than companies with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

partial implementations. Overall, it can be concluded that the extent to which ERM implementation among Australian sample companies seems better than other countries as reported in previous studies. However, because of the small sample size of the study and the focus on large companies, the generalization of the findings above may not be possible.

For the impact implementation of the integrated system of risk management in the Banks [30] they found The results of this study produce a new risk management culture in the overall bank management system, not limited by one component of the managerial mechanism. This led to an increase in bank competitiveness and also helped to increase the level of security of their economy. This shows that the implementation of ISO 3100 can provide very good benefits for the company.

in the use of ERM, it must be large scale because if it is applied in small and medium scale enterprises, the desired results will not be appropriate, as proven by the results of the research by Liuksiala & Ruuskanen (2012). in papapran, the appropriate in explaining risk management in Finland does not meet the standards set especially in small and medium scale companies.

3. Methodology

This study conducts a study by looking for data and information from related books and journals as well as studying theories related to the topics and problems to be studied. In additions researchers determine the population and the number of samples that will be used in the study. Next, the researcher gave questionnaires to IT workers at Bank XYZ which contained questions related to research which would then be processed and analyzed through the ISO 31000 framework, to see the steps of this research can be seen as follows figure 3:

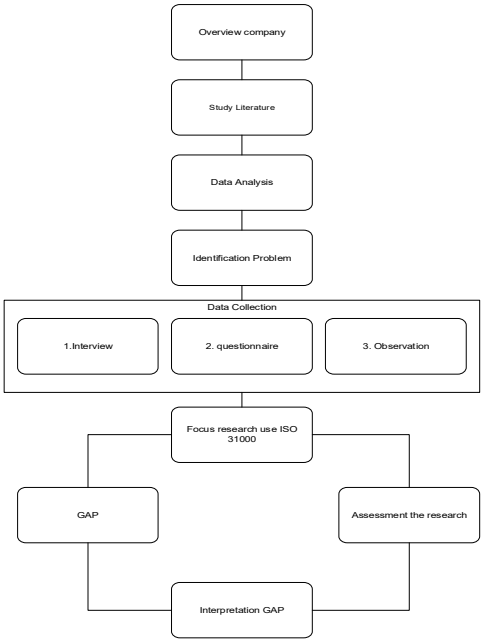

Figure. 3. Research Steps

Explanation of figure 3:

1. In the first stage, it provides general information about the company that will be researched.
2. Describe relevant theories and literature studies based on the results of previous studies.
3. Analyzing data and preserving data in the field.
4. Identify the problems faced by the company being studied.
5. Collect relevant data based on interviews, questionnaires and company documents.
6. Using ISO 31000 standardization and comparing real conditions in the company.
7. Compare whether there are gaps that occur so that they can provide recommendations

4. Results and Analysis

Determination of context is the first stage in the implementation of the ISO 31000 model in terms of the Strategic Context, Organizational Context, Risk Management Context. To see the process at the stage of determining the context can be seen as follows:

4.1 Strategy Context

Bank XYZ establishes a risk management framework that is the basis for implementing all risk management activities at all levels of the organization. The Bank XYZ Risk Management Framework assists organizations in managing risks effectively and will ensure that complete &

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

adequate risk information obtained from the risk management process can be used as a basis for decision making.

4.2 Organizational Context

Annual Report released by Bank XYZ in the world of banking, the implementation of Good Corporate Governance is a mandatory thing in day to day operations, both in terms of Governance Structure, Governance Process, and Governance Outcome. In addition to protecting the company from existing risks, the implementation of good governance will also lead to public trust in the company.

4.2 Risk Identification

Risk identification obtained in the XYZ Bank is based on the business processes that run in the company. In this study focused on the risks of IT operations because some of the problems that have occurred originated from the company's operations where the risks that occur in the company consist of the risk of access to unwanted access, data tracing, network communication work, work unit, power and environment in the work unit, infrastructure on servers and storage, and the risk of viruses and malware

4.3 Risk Analysis

After identifying risks, the next step is risk measurement by looking at the potential occurrence of how much severity (damage) and the probability of the occurrence of the risk. To be able to analyze the risk can be done through a check list containing a list of questions. For check lists have different objectives depending on the risk side that will be discussed. In this study the check list was divided into seven categories. Eight categories are explained as follows:

1. See if there is unwanted access on critical devices by unauthorized parties. The domain code is PAS1.
2. Ensure there are no difficulties in tracing data. For the domain code is PDT3.
3. Ensuring the failure of the IT infrastructure to meet business needs in this case is the Work Unit Communication Network. For the domain code is the PKL8 Communication Network.
4. Ensure that there is no IT infrastructure failure (PC, Passbook Printer, Dotmatrix Printer, Laserjet, Scanner) in meeting business needs in this case is a Peripheral / IT Device Work Unit. For the domain code is PKL 8 Peripheral // IT Unit Work Unit.
5. Ensuring that there is no failure of the IT infrastructure in meeting business needs in this case is the Work & Energy Unit. For the domain code is the Power Environment PKL 8.
6. Ensure there is no failure of IT infrastructure (Server & Storage BDS) in meeting business needs. PKL 8 Storage Server
7. Ensure that there are no IT devices that are vulnerable to attacks by malicious programs (for example: viruses, malware, etc.). For the domain code is POK1.

These seven points are of particular concern because if one of the points is not met, the banking institution will experience the impact and impact directly on the business process and worker productivity. To see further the check list results that have been obtained through interviews and check directly.

4.4 Risk Evaluation

Risk Evaluation aims to help the decision making process based on the results of the risk analysis that has been carried out. The risk evaluation process will determine which risks require treatment and how the treatment priorities for those risks are risk allocation, risk mitigation, risk sharing or risk acceptance. To see this can be seen in the table as follows table 5.

Table 5. Risk Evaluation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Risk Type	Code	Risk	Severity	Occurance	Risk Scoring
access rights	A1	Data theft occurs	4	1	8
	A2	Misuse of access rights	2	3	11
	A3	Password security features are not maintained	5	2	17
	A4	lack of care	5	1	10
	A5	Lack of sausages	2	1	3
	A6	lack of training on data security	2	1	3
	A7	Incomplete documentation	5	1	10
tracing data	B1	Less effective in tracing data	5	4	24
	B2	data is often not stored data	4	1	8
	B3	Absence of data history	5	2	17
	B4	lack of care	5	1	10
	B5	The absence of a thorough examination	5	1	10
Communication Network	C1	Lack of Effectiveness in work communication	5	1	10
	C2	late in solving the problem	3	3	15
	C3	Lack of maintance on work communication	4	1	8
	C4	Unmanaged working units	5	1	10
Peripheral	D1	the failure of IT infrastructure	2	3	11
	D2	Lack of maintance on work communication	5	1	10
	D3	late in overcoming the problem	5	1	10
	D4	Unattended peripherals / IT Devices Work Units	5	1	10
Power & Environment	E1	The occurrence of a power outage	1	3	4
	E2	lack of supervision	5	1	10
	E3	late in overcoming the problem	5	3	21
	E4	Lack of maintance on work communication	5	2	17
Server & Storage	F1	Slow system on server	5	1	10
	F2	The occurrence of a power outage	5	1	10
	F3	Lack of maintance on Server & Storage Work Units	4	1	8
	F4	late in overcoming the problem	5	1	10
IT security	G1	Attacked by viruses and malware	3	3	15
	G2	Slow operating system on PC	4	2	14
	G3	The absence of socialization to avoid unwanted events	5	1	10
	G4	Lack of supervision	5	1	10
	G5	the pc becomes vulnerable to virus attacks	5	1	10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From table 5 shows each category can be seen how much the frequency of the occurrence of risk and how much the impact caused. After knowing the many frequencies and how much impact they can take a risk assessment. This risk assessment is based on the risk matrix table where the frequency is linked to the impact it will get a middle value so that it gets the value of a risk. Based on the results obtained shows that there are still high risks faced. The results obtained must reflect the effectiveness of the response measures that will be faced and the level of residual risk reported makes sense [29]. The results of the risk value can be used as a reference whether each risk category faced can still be received or not. To see this can be seen in the table as follows Table 6:

Table 6. Risk Response for each category

Risk Type	Code	Risk	Risk Scoring	Criteria for Risk Management
access rights	A1	Data theft occurs	8	Monitored
	A2	Misuse of access rights	11	Management Control
	A3	Password security features are not maintained	17	Management Control
	A4	lack of care	10	Management Control
	A5	Lack of sausages	3	Acceptable
	A6	lack of training on data security	3	Acceptable
	A7	Incomplete documentation	10	Management Control
tracing data	B1	Less effective in tracing data	24	Unacceptable
	B2	data is often not stored data	8	Monitored
	B3	Absence of data history	17	Management Control
	B4	lack of care	10	Management Control
	B5	The absence of a thorough examination	10	Management Control
Communication Network	C1	Lack of Effectiveness in work communication	10	Management Control
	C2	late in overcoming the problem	15	Management Control
	C3	Lack of maintance on work communication	8	Monitored
	C4	Unmanaged working units	10	Management Control
Peripheral	D1	the failure of IT infrastructure	11	Management Control
	D2	Lack of maintance on work communication	10	Management Control
	D3	late in overcoming the problem	10	Management Control
	D4	Unattended peripherals / IT Devices Work Units	10	Management Control
Power & Environment	E1	The occurrence of a power outage	4	Monitored
	E2	lack of supervision	10	Management Control
	E3	late in overcoming the problem	21	Management attention (urgent)
	E4	Lack of maintance on work communication	17	Management Control
Server & Storage	F1	Slow system on server	10	Management Control
	F2	The occurrence of a power outage	10	Management Control
	F3	Lack of maintance on Server & Storage Work Units	8	Monitored
	F4	late in overcoming the problem	10	Management Control
IT security	G1	Attacked by viruses and malware	15	Management Control
	G2	Slow operating system on PC	14	Management Control
	G3	The absence of socialization to avoid unwanted events	10	Management Control
	G4	Lack of supervision	10	Management Control
	G5	the pc becomes vulnerable to virus attacks	10	Management Control

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From table 6 explains that there are management criteria that are not acceptable, namely in category two with the risk of being less effective in tracing data. This indicates that this sub-category must be a concern because the highest risk level occurs. Criteria for risk management aim to monitor and measure risk. Managing and benchmarking risk must be done because it will relate to risk management policies [30].

4.5 Information System Maturity Level

From table 6 explains that there are management criteria that are not acceptable, namely in category two with the risk of being less effective in tracing data. This indicates that this sub-category must be a concern because the highest risk level occurs.

The maturity level as a whole is obtained from the identification of each maturity level in all the control objectives involved based on seven categories. For that, it is necessary to assess the score (value) of each respondent, the writer uses a Likert scale. After knowing the next step is the distribution of questionnaires. Where the questionnaire is divided into 2 divisions, namely the IT and non-IT divisions in which the intended users are.

Questionnaires used amounted to eight people in which two people came from the IT / E-channel division and six people were workers from operational management totaling one person, Account Officer numbered three, HR division numbered one person and Teller numbered one person. To find out more, it can be seen in the table as follows Table 7.

Table 7. Questionnaire Value

	High Level Objective							
Questionnaire Value	Respondents based on division	PAS1	PDT3	PKL 8 Communication	PKL 8 Peripheral	PKL 8 Power Environment	PKL 8 Server Storage	POK1
	Manager operasional	21	15	13	12	12	12	15
	Acc Officer 1	21	9	12	11	12	6	15
	Acc Officer 2	21	9	12	12	12	6	15
	Acc Officer 3	21	9	12	12	12	6	15
	SDM	19	9	12	11	12	6	13
	Telle	21	9	12	12	12	6	15
	IT/E-channel 1	21	15	12	12	12	12	15
	IT/E-channel 2	21	15	12	12	12	12	15
Amount	8	166	90	97	94	96	66	118

In table 7 After the questionnaire calculation process is carried out, the results of the calculation of each number of questionnaires are obtained from the total questions that have been filled by 8 respondents. Here's how to calculate in determining the index of each domain process that has been managed, it can be seen in the table as follows table 8.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 8. Maturity Level

Maturity Level									
Category	Total Questions		Number of Respondents		Total Questions * Number of Respondents		Total Questionnaire Value	Number of Answers	Indeks
	IT Section	User	IT Section	User	IT Section	User			
PAS1	7	7	2	6	14	42	56	166	2.96
PDT3	5	3	2	6	10	18	28	87	3.11
PKL8 Jaringan Komunikasi	4	4	2	6	8	24	32	97	3.03
PKL 8 Peripheral	4	4	2	6	8	24	32	94	2.94
PKL 8 Power Environment	4	4	2	6	8	24	32	96	3
PKL 8 Server Storage	4	2	2	6	8	12	20	60	3
POK1	5	5	2	6	10	30	40	118	2.95

Table 8 describes the index value of each category in which the category in PAS1 describes the access rights as having an index of 2.96, in the PDT3 category which explains the data tracing has an index of 3.21, then the PKL 8 category which describes the work unit communication has an index of 3.03, in the PKL 8 category which describes the peripherals / IT devices the work unit has an index of 2.94, then in the PKL 8 category which describes the power environment has an index of 3.00 then PKL 8 which explains the storage server has an index of 3.30 and the last in the POK1 category which describes IT security work units have an index of 2.95.

The purpose of this maturity level is because each level of maturity consists of the main characteristics of Project Management, factors, and processes. This model shows sequential steps that outline the organizational improvement of the Project Management process [31]. After knowing the index value in each category, it will then compare the conditions that currently occur with the expectations that you want to achieve. The Index target expected by Bank XYZ is level four maturity. To see the comparison of maturity levels between user respondents and the IT part that occurs at this time with the target set can be seen as follows figure 4.

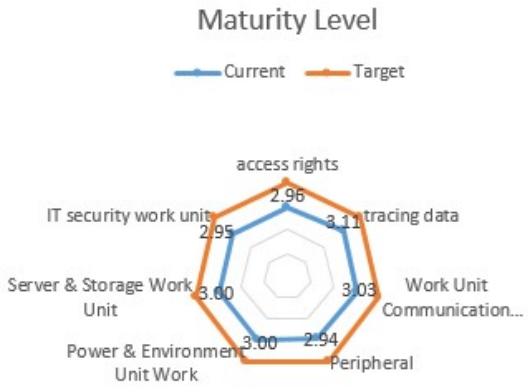

Figure. 4. Maturity Level at Bank XYZ

Figure 4 shows that what is the target and the conditions that are happening the value of system maturity at Bank XYZ is not fulfilled in 7 domain categories. The maturity level that is expected by the Bank XYZ is four while for domains on access rights only has a value of 2.96, for tracing data has a value of 3.11, for network communication work units have a value of 3.03, for peripheral domains / IT devices work units have the value is 2.94, for the power and environment domain the work unit has a value of 3.00, for the domain server and work unit has a value of 3.00, and for the domicile of IT security the work unit has a value of 2.95.

4.6 Risk control

Risk control is a recommended step to avoid risk, reduce risk, transfer risk and even accept risks with controls adjusted for each risk. Risk control in this study is only focused on very high, high and medium which are prioritized to be avoided and reduced. Focusing on the high,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

moderate level has the aim that the risks faced can be broken down in more detail in the table as follows Table 9:

Risk Analysis Matrix 5 x 5			Impact Level				
			1	2	3	4	5
			Not Significant	Minor	Moderate	Significant	Very Significant
Possible Level	5	Almost certainly happened					
	4	Often occur		A2,			B1
	3	Sometimes happens	E1	D1	C2,G1		E3
	2	Rarely happening				G2	A3,B3,E4
	1	Almost nothing happens		A5,A6		A1,B2,C3, F3,	A4,A7,B4, B5,C1,C4, D2,D3,D4, E2,F1,F2,F 4,G3,G4,G5

Table 9 Explains that risks occur in each domain and the details shown in the activity code. From table 9 shows that the risk that occurs a lot is the risk at the intermediate stage, it should be aware that this risk will deter from productivity at Bank XYZ. The intermediate mean the risk can be acceptable for this service, but for each threat the development of the risk must be monitored on a regular basis, with a following consideration whether necessary measures have to be implemented [32].

5. CONCLUSION

The application of the ISO 31000 standard as an alternative standardization system solution provides several recommendations. The recommendation is based on the results of a questionnaire that covers seven domains. The seven domains are broken down based on control objectives that have risks based on the level of risk. The following risks occur: First Based on a very high level of risk, there is only one control objective that has a very high risk of objectivity control: Less effective in tracing data. The second is based on high risk, one is found in the control objective: late in overcoming the problem in the Power & Environment Unit.

Third, based on the middle risk, there are several parts as follows: There are two access rights domains found, namely: The occurrence of misuse of access rights, password security features are not maintained, lack of security. For data tracing domains: absence of data history, lack of guarding, absence of a thorough inspection. For the work unit communication domain, there are three problems, namely the absence of data history, lack of guarding, lack of thorough inspection.

In the work unit peripheral domains, three problems are found, namely lack of maintenance in work communication, delays in dealing with problems, poor maintenance of peripherals / IT units of work units. For the Domain power environment, two problems are found, namely: lack of supervision, lack of maintenance on work communication. For Domain servers and storage, two problems are found, namely the slow system on the server, the occurrence of a power outage. Work unit security domain there are five problems, namely attacked by viruses and malware, the slow operating system on the PC, the absence of socialization to avoid unwanted events, lack of supervision, delays in solving problems so that the PC becomes vulnerable to virus attacks.

In addition to the level of risk found, researchers also found maturity levels on the information system at XYZ banks. Maturity level is important to explain because it can see how mature the information system in the XYZ bank is. From the research results obtained is the value of system maturity at Bank XYZ is not fulfilled in 7 category domains. The maturity level expected by the Bank XYZ is four.

To see the current condition of the 7 domains can be seen as follows: In the Domain the access rights only have a value of 2.96. Tracing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

domain data has a value of 3.11. The work unit's communication network domain has a value of 3.03. Peripheral domains / IT devices work units have a value of 2.94. The power domain and work unit environment have a value of 3.00. The server domain and work unit have a value of 3.00. The IT security domain in the work unit has a value of 2.95. After knowing the comparison between the maturity level of the current condition and the expected conditions, there is a gap that the average maturity level of the information system at Bank XYZ is 3.00 at the Defined level, while the maturity level target that Bank XYZ wants to achieve is level 4. From this comparison can be obtained by a gap of 1.00 this indicates that the maturity level target has not been achieved as expected.

Along with this study there are several studies that find the same thing Svatá & Fleischmann (2011) found the risk of IS / IT in the banking sector. In this study explained that the number of banks failed due to the non-fulfillment of the ISO 31000 standard so that the occurrence of many cases starting from its governance, the system failed to meet business objectives. This is due to failed supervisory boards and senior managers in the risk management system's responsibilities and controls [33].

Suggestions that can be given by researchers based on the results of the research are as follows: First in general, the IT operational process has proceeded well, but still there must be improvements, both technical and non-technical, still being improved. Bank XYZ must pay attention to the level of risk where the most common risk level is medium status risk where the advice given is: A routine procedure that is sufficient to bear the impact. Need effective internal control and monitoring. In addition, strategies focus on monitoring and reviewing existing control procedures.

Second, the level of maturity in the Financial technology system at Bank XYZ also needs to be noticed because the current condition of the system maturity level is 3.00 and for the target that is expected is 4.00, there is a gap of 1.00. to realize the value of the maturity level at XYZ banks, it is recommended that there be socialization between the IT team for each individual employee, so that the possibility of deviation can be detected. In addition, Managed and monitoring of compliance with procedures, and taking action if the process does not work effectively, can be done. Process improvements are carried out constantly. Lastly, adding workers who are tasked to carry out prevention is carried out routinely so that it can mitigate a problem so that it will eventually accelerate the existing business processes.
work.

REFRENCES:

[1] W. Bennis, “Why Leaders Can’t Lead.,” *Train. Dev. J.*, vol. 43, p. 35, 1989.

[2] S. P. D’Arcy and S. P. D’Arcy, “Enterprise Risk Management,” *J. Risk Manag. Korea*, vol. 12, no. 1, 2001.

[3] S. Hass, M. J. Abdolmohammadi, and P. Burnaby, “The Americas literature review on internal auditing,” *Manag. Audit. J.*, vol. 21, no. 8, pp. 835–844, 2006.

[4] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, “How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits,” *Policy Sci.*, vol. 9, no. 2, pp. 127–152, 1978.

[5] M. E. Bakos, J. Y., & Treacy, “nformation technology and corporate strategy: a research perspective. MIS quarterly,” 1986.

[6] Y. A. Au and R. J. Kauffman, “The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application,” *Electron. Commer. Res. Appl.*, vol. 7, no. 2, pp. 141–164, 2008.

[7] Financial Stability Board, “Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities’ Attention,” no. June, p. 65, 2017.

[8] T. Oliveira and M. Martins, “Literature review of Information Technology Adoption Models at Firm Level,” *Electron. J. Inf. ...*, vol. 14, no. 1, pp. 110–121, 2011.

[9] McKinsey and Company, “Global Media Report 2015. Global Industry Overview,” pp. 1–24, 2015.

[10] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology,” *Nist Spec. Publ.*, vol. 800–30, p. 55, 2002.

[11] BSN, *Manajemen Risiko Prinsip dan Pedoman*. 2016.

[12] OJK, *Jaringan Kantor Perbankan*. 2016.

[13] A. D. Banasiewicz, “Total Exposure Management: Enterprise Risk Management,Organizational Resilience and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Change Management," vol. 1, no. 2, pp. 24–34, 2017.

[14] L. Bates, "Avoiding the pitfalls of enterprise risk management," *J. Risk Manag. Financ. Institutions*, vol. 4, no. 1, pp. 23–28, 2010.

[15] A. Alijoyo, "Majalah SNI Valuasi Manajemen Risiko Berbasis SNI ISO 31000.PDF." p. 51, 2016.

[16] G. Purdy, "ISO 31000:2009 - Setting a new standard for risk management: Perspective," *Risk Anal.*, vol. 30, no. 6, pp. 881–886, 2010.

[17] D. Gjerdrum and M. Peter, "The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework," *Risk Manag.*, no. 21, pp. 8–12, 2011.

[18] C. Lalonde and O. Boiral, "Managing risks through ISO 31000: A critical analysis," *Risk Manag.*, vol. 14, no. 4, pp. 272–300, 2012.

[19] M. C. Paulk, B. Curtis, M. B. Chrissis, and C. V Weber, "for Software , Version 1 . 1 Software Engineering Institute," no. February, 1993.

[20] P. Fraser, J. Moultrie, and M. Gregory, "The use of maturity models/grids as a tool in assessing product development capability," in *Engineering Management Conference, 2002. IEMC'02. 2002 IEEE International*, 2002, vol. 1, pp. 244–249.

[21] B. Djatmiko, "Audit Sistem Informasi untuk Menilai Proses Penyampaian dan Dukungan (Delivery and Support) dalam Pelayanan Informasi dengan Menggunakan framework CobiT (Studi Kasus: PT Telekomunikasi Indonesia, Tbk. R&D Center)," 2007.

[22] International Standard for Organization, "Risk Management – Principles and Guidelines," 2009.

[23] E. Avanesov, "Risk Management in Iso 9000 Series Standards Risk Management in Iso 9000 Series Standards," *Int. Conf. Risk Assess. Manag.*, pp. 2–11, 2009.

[24] B. C. on B. S. BCBS, "Risk Management Principles for Electronic Banking," *Weatherwise*, vol. 56, no. 6, pp. 53–56, 2003.

[25] N. Hyatt, *Guidelines for process hazards analysis (PHA, HAZOP), hazards identification, and risk analysis*. CRC press, 2003.

[26] P. R. Garvey and Z. F. Lansdowne, "Risk matrix: an approach for identifying, assessing, and ranking program risks," *Air Force J. Logist.*, vol. 22, no. 1, pp. 18–21, 1998.

[27] O. S. Tumenbayeva and G. N. Zhaksybekova, "Implementation of the integrated system of risk management in the banks of Kazakhstan," *Indian J. Sci. Technol.*, vol. 9, no. 5, 2016.

[28] S. Ahmad, C. Ng, and L. A. McManus, "Enterprise Risk Management (ERM) Implementation: Some Empirical Evidence from Large Australian Companies," *Procedia - Soc. Behav. Sci.*, vol. 164, no. August, pp. 541–547, 2014.

[29] D. Brodie, "Enterprise risk," *Enterp. Liabil. Common Law*, no. September, pp. 27–44, 2011.

[30] Insitute of Risks Management, "A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 Contents," *Risk Manag.*, vol. 7, no. 1, p. 20, 2010.

[31] Y. H. Kwak and C. W. Ibbs, "Project Management Process Maturity (PM)2 Model," *J. Manag. Eng.*, vol. 18, no. 3, pp. 150–155, 2002.

[32] A. S. Markowski and M. S. Mannan, "Fuzzy risk matrix," *J. Hazard. Mater.*, vol. 159, no. 1, pp. 152–157, 2008.

[33] V. Svatá and M. Fleischmann, "IS/IT Risk Management in the Banking Industry," *Acta oeconomica pragensia*, vol. 19, no. 3, pp. 42–60, 2011.