ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 3, pp. 181-199
DOI:10.33168/JSMS.2022.0310

Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001

Nilo Legowo, Yoyo Juhartoyo

Information Systems Management Department, Binus Graduate Program
Master Of Information Systems Management, Bina Nusantara University, Jakarta
Indonesia 11480

nlegowo@binus.edu ; yoyo.juhartoyo@binus.ac.id

Abstract: In the era of information technology-based electronic banking services, there are a number of security vulnerabilities, including those in information technology systems, hardware vulnerabilities, software vulnerabilities, and human resource carelessness. The objectives of this research were to conduct a risk assessment, determine the level of maturity of the information technology security system using a checklist from Annex A of ISO 27001, which contains 11 domains and 39 control objectives, and conduct a risk assessment of information technology assets, as well as provide recommendations for controlling the risk level. On average, 75% of information security systems are now fully developed. The domain that is still lacking is business continuity management, which has a maturity level of only 55%, whereas domain compliance is the highest at 93%. Three (3) assets have a very high basic value risk (inherent risk), while seven (7) assets have a high basic value risk. There are 19 recommendations for controls that should be put in place to control the level of risk. In practice, assets with a very high level of risk can be prioritized by figuring out the costs, benefits, and risks of not putting in place the control recommendation.

Keywords: risk management, information technology, security systems, risk assessment, maturity level

1. Introduction

Bank Indonesia, in its capacity as the Central Bank, is committed to achieving and maintaining the value stability of the rupiah through the management of the Monetary, Payment System, and Financial System Stability domains.

The primary functions of Indonesian banking are to collect and distribute public funds and to support the implementation of national development so as to increase the equitable distribution of development and its results, economic growth and national stability, and enhance the living standards of the populace.

In this age of information technology-based electronic banking services, there are many holes in information technology security, including operational procedures and banking information technology, hardware, software, and human resources.

Every type of banking business must always comply with Bank Indonesia's rules and policies when conducting all business process activities and utilizing information technology resources to provide banking product services to customers. including provisions in the application of standard risk management for information system security.

Risk management in banking can increase the value of the bank's shares, give the bank's management an idea of how likely it is that the bank will lose money in the future, and help set up a system for making decisions based on the availability of information that can be used to measure performance more accurately.

The theft of banking customer data can be carried out by both internal and external parties. An external company uses the following methods to steal customer data: skimming (using a tape recorder), phishing (via the internet and social media), malware (viruses), sniffers (intercepting data packets on network communication), keyloggers (recording/copying data via the keyboard), and typo-sites (updating fake sites that have names similar to the official website). Even though a company employee is taking advantage of holes or flaws in the way things are done to steal or destroy customer data, it is happening right now.

In addition to the theft of customer data, the problem of the availability of information technology systems must be addressed, as it can foster mistrust, harm the company's image and reputation, and even pose a legal risk to customers. Information technology systems are available in the form of software, hardware, databases, data communication, supplies, and services.

As associated with the risk management information technology system, Bank Indonesia issued Bank Indonesia Regulation (PBI) 9/15/PBI/2007 dated November 30, 2007 on the Implementation of Risk Management of Information Technology by Commercial Banks.

Implementation of the provisions of PBI No.9/15/PBI/2007 listed in Bank Indonesia Circular Letter (SEBI) 9/30/DPNP dated December 12, 2007 on Risk Management of Information Technology by Commercial Banks

Given the importance of information security systems, then the policy on the security of information systems should include at least these: procedures for asset management; procedures for human resource management; procedures for physical security and the environment; security procedures; logical security; security procedures for operational information technology; and procedures for handling incidents in securing information (Directorate of Banking Research and Regulation, 2007: 52).

The issues to be discussed in this study are as follows: what are the current conditions of risk management in information technology system security? and what are the risks that currently exist in information technology systems? and how to control and minimize the risks' impact?

The purpose of this study is as follows: to perform a measurement of the maturity level of information technology system security risk management that is currently applied; to evaluate the risk management of information technology security systems; and to provide recommendations to control the risk impact.

2. Literatur Review

2.1. IS/IT risk management in banking

According to (Yousef Tabsh and Vida Davidaviien, 2016), governments in developing countries should adopt a high level of information and communication technology (ICT) implementation and attempt to implement it. The implementation of ICT has produced promising results. This new system must be adapted by the government in order to achieve a higher level of sustainable development. For the government to improve the economic and social situation in developing countries, there needs to be good coordination between governments so that they can get the most out of ICT's national applications.

In the field of risk management, different experts and professional organizations have come to the same conclusion: failure can be caused by the risk of informational ambiguity that comes from different risk assessments from different points of view (McCuaig, 2008, s. 3; Ernst, 2009, s. 4).

In a brief discussion of the risk management specifications for financial institutions, the similarities and differences between IS/IT risk management and operational risk management are described. It is possible to incorporate multiple IT/IS risk management tools and methods into operational risk management, along with a summary of the benefits and difficulties of the various frameworks. (Vlasta Svatá and Martin Fleischmann, 2011) acknowledged that information systems and technology have a significant impact on banking industry business processes. IS/value IT is highly dependent on its implementation and integration with banking activities. Thus, IS/IT is an important factor that can contribute to a bank or financial institution's competitiveness and commercial success (Vlasta Svatá and Martin Fleischmann, 2011).

The role of IS/IT is very important in business because weaknesses in IS/IT risk control can cause not only financial losses and failures in financial institutions or threats to client deposits but also have a negative impact on the overall economy both nationally and globally (Martin Fleischmann and Vlasta Svatá, 2011).

Operational risk is caused by failure or insufficient (inadequate) internal processes, people, or systems, or by external events. This risk will have an impact on the entire business because of the daily operational risks. Operational risk can arise, among others, due to insufficient or malfunctioning internal processes. (Kountur, R.,2008)

2.2. Information system

The notion of a system is a series of two or more components that are interconnected that interact to achieve a goal. (Romney, 2004) Meanwhile, ref. According to (Sutanto, 2000), the definition of a system is a collection or group of subsystems/parts/components of any kind, either physical or non-physical, that are interconnected with each other and work together in harmony to achieve a particular purpose.

Information is the result of data processing that provides meaning and benefits. (Sutanto, 2000). In addition, information is defined as the output of data processing that is organized and useful for the people who receive it. (Midzan Sutanto and Barry L. Cushing, 2000).

An information system is a collection of subsystems, both physical and non-physical, that are interconnected with each other and work together in harmony to achieve one goal of processing data into useful information. (Sutanto, 2000), citing (John F. Nash and Midzan Sutanto, 2000) An information system is a collection of components that, when combined, are intended to configure a network, provide important communication, processing of certain transactions and routines, assist management and users of other internal and external parties, and provide a basis for a decision right (Intelligent).

The components of the information system are as follows: hardware; software; brainwaves; procedures; databases; and networking. (Sutanto, 2000).

2.3. Information security

The definition of information security is an effort to secure information assets against threats that may arise (Sarno and Iffano, 2009). Ref. ISO/IEC 27001 (2005).

regarding the management of information security systems, says that information security is an effort to protect against various kinds of threats to ensure business continuity, minimize business risks, and increase investment and business opportunities.

Information security is an effort to prevent fraud (cheating) or, at least, detect fraud in the application of information systems where the information itself is not physically visible. Information security must contain three important aspects, namely: firstly, the confidentiality aspect, which ensures the confidentiality of data or information, ensures that information can only be accessed by authorized persons and ensures the confidentiality of data sent, received and stored; the second aspect of integrity, which ensures that data is not changed without the permission of the authorities (authorize); the third aspect of availability, which ensures that data will be available when needed, ensuring that authorized users can use the information and related tools if needed (Supradono, 2009).

The scope of information security is 4, namely ISACA (2010): (a) An organization is a network of people, assets, and the process by which they interact with one another, defining the role and work of collaborating to achieve a common goal. People are human resources and security information; processes are all formal and informal mechanisms (large, small, simple, complex) for resolving everything. (d) Technology is the combined/aggregate of all the equipment, applications, and infrastructure that can make the process more efficient.

Some definitions of risk are as follows: (1) risk is the possibility of loss (risk is the possibility of a loss), (2) risk is the possibility of loss (risk is the possibility of a loss), (3) risk is the possibility of loss (risk is the possibility of a loss), (4) risk is uncertainty (risk is the uncertainty). (Darmawi, 2010), Subjective uncertainty is an individual's assessment of the risk situation.

(Lokobal dkk, 2014) is a reference According to this source, there are several causes of risk that can be distinguished as follows: (1) internal risk, namely risks that arise from within the company itself; (2) external risks, namely risks originating from outside the company or from the company's environment; (3) financial risk, namely risk caused by economic and financial factors of the company; (4) Operational risk encompasses all risks, including financial risks and risks caused by human factors, nature, and technology.

Operational risk is the potential deviation from expected results due to a system malfunction, human resources (HR), technological or other factors, Putro, Djohan (2008). Operational risk can occur at two levels, namely technical and organizational. At the technical level, operational risks could occur if the information system contains the errors noted above, inadequate information and risk measurement is inaccurate and inadequate. At the organizational level, operational risks can arise due to system monitoring and reporting, systems and procedures, and policies not running as they should.

2.4. Risk information technology

The risk category of information technology by (Hughes,2006) At the use of information technology at risk of information loss and recovery was included in six categories, namely: (1) security; (2) availability; (3) recovery; (4) performance; (4) power scale; (5) compliance.

While the cause of the risk of information technology by (Napitupulu S.J., 2009) is (1) change control, inadequate data, or (2) data that is incomplete.

Risk management consists of three main processes, namely (1) risk assessment (risk assessment), (2) mitigation of risk (risk mitigation), and (3) evaluation and assessment (evaluation and assessment). (Stoneburner, Gary, 2002). Evaluation and assessment is the final process in risk management, which is a step further evaluation to implement a successful risk management program. (Iswari, 2011).

According to (ITGI, 2009), information technology risk is also a business risk, such as two sides of the same coin; in particular, the business risks associated with the use, ownership, operation, involvement, influence, and adoption of IT in an enterprise do not need to make a difference between business risk and IS/IT risk.

2.5. Risk assessment

The definition of risk assessment is explained as the identification, evaluation, and estimation of the level of risk involved in a situation, its comparison with benchmarks or standards, and determining the level of acceptable risk. (ISF, IR AM., 2010).

Different approaches to risk assessment in the area of information risk; in this case, the risk assessment of information systems and/or information technology plays a very important role in every organization. There are two reasons for the assertion of a risk assessment approach. First, IS/IT integrates all the different functional areas within an organization and has the potential to integrate risk assessment. Second, IS/IT is concerned with processing data and information, which makes it less likely that information will be of poor quality, (Vlasta Svatá and Martin Fleischmann, 2011).

Risk assessment is part of risk management. It is a process to assess how often the risk occurs or how large the impact of the risk is. Ref. According to (Jakaria, D.A, Dirgahayu, R.T., Hendrik, 2013), the purpose of risk assessment is to (a) identify the threat; (b) identify the vulnerability; (c) the possible impact caused by vulnerability exploitation (impact analysis); and (d) the possibility of danger or damage (likelihood).

In risk management, there are several things that need to be done sequentially, starting from identifying risks that exist in the field with an assessment of emerging risks, determining priorities for risk mitigation, evaluating the results of risk mitigation, implementing and maintaining efforts to mitigate the impact of risks on company operations, based on identification during the risk assessment stage. Risk mitigation is carried out not only to reduce risk but also to reduce the negative impact on the sustainability of the company's operations.

The next step The strategy that will be carried out at the risk mitigation stage, the efforts to be made are as follows: (a) risk elimination (risk elimination/avoidance), (b) risk reduction, (c) risk reduction. transfer), (d) risk acceptance. a policy of accepting risk and an attitude of acceptance, especially the residual risk remaining after risk mitigation measures from the possible impacts that may arise, (Al Bone, 2008).

In addition, to mitigate risk, there are six main processes that must be prepared and need to be carried out by the company to minimize risk, with the following steps, among others: Prioritize action; evaluate recommended controls; conduct a cost-benefit analysis; select control; assign responsibility; and develop a safeguards implementation plan.

This activity is a process to determine the security control implementation plan has been The control process in risk management will be carried out to get the result of this process, which is the implementation plan for the protection effort. Meanwhile, when implementing the selected control, it is the process to implement risk control from the possibility of a risk occurring or not being able to eliminate the risk that occurs, according to (Al Bone, 2008).

Team Mentoring and Consulting in Risk Management The Ministry of Finance stated that the evaluation of the risk involves assessing risks in order of priority risk by the way through the process according to the rules systematically. Meanwhile, according to e-learning UI, risk evaluation is to compare the level of risk that has been estimated at this stage of risk analysis with standard criteria used. A risk assessment is: (a) a description of how important risks are; (b) a description of the priority risks to be addressed; (c) a description of losses that might occur well within the parameters of cost or other parameters; and (d) putting the control information for the consideration stage.

According to Tim Mentoring and Risk Management Consulting Finance Ministry, the purpose of risk assessment is as follows: (a) determine who has the highest to the lowest priority level; (b) determine which risks are followed up with treatment; and any risks that only need to be monitored.

To perform the evaluation process, we need a clear parameter to measure the impact of a risk appropriately. (Loosemore, Reilly, & Higgon, 2006).

ISO/IEC 27001 was issued in October 2005 in order to replace the standard BS7792-2. ISO 27001, which is the Indonesian version of ISO/IEC 27001, contains clauses and clauses of specifications or requirements that must be met in building an Information Security Management System (SMKI). In implementing the standard, it must be independent from the use of information technology products, require a risk-based management approach, and be designed to ensure that information security controls are able to protect information assets from various risks that occur and provide a level of security confidence for interested parties (Communications, 2011, p10).

In the ISO Standard, there are many clauses that list the main requirements that must be met. These include: (1) information security management system (framework, processes, and documentation); (2) management responsibilities; (3) internal audit of the ISMS; (4) management reviews of the ISMS; and (5) continuous improvement.

In addition to the important requirements contained in this standard, it requires setting objectives, controlling and controlling information security, which includes several domain areas, namely 11 security domains as follows: (1) information security policy, (2) information security organization, (3) asset management, (4) information security human resources, (5) physical and environmental security, (6) communication and operations management, (7) access control, (8) procurement/acquisition, development, and maintenance of information systems, (9) information security incident management, (10) business continuity management (business continuity management), (11) Compliance (Kominfo, 2011).

3. Research Methodology

Researchers conducted direct observation of the object from the literature and collected relevant data for later analysis in order to provide recommendations to improve the system in place to do research, in particular the information security risk management system with a scope that is predetermined.

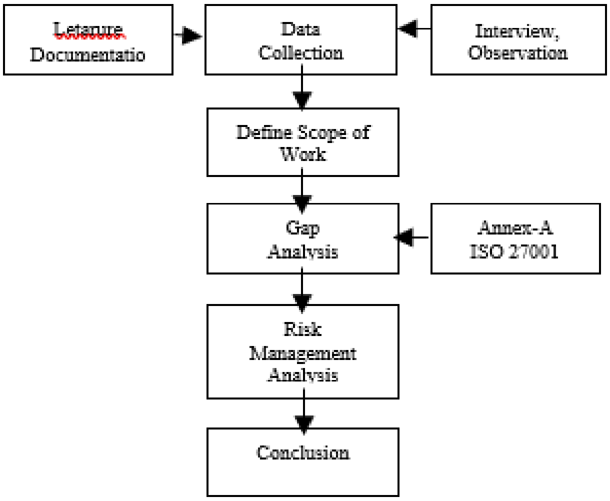


Fig.1: Frameworks

In the process of data collection, the researchers divided into two groups: primary data (obtained directly) and secondary data (obtained from the documentation) that will be used as a management evaluation of the risks of security of information systems.

The next process that determines the scope of the study is the first step of the assessment exercise for the management of the information technology system. In this study, the scope of which will be examined is the application of Core Banking System companies. The scope includes the organization, assets and technology relating to the core banking system and the location. Here is an explanation of the scope in question: (a) The organization is a division related to existing information technology activities under the Operations and IT Directorate, (b) Asset and technology, namely: Core Banking System application, servers, load balancers, core switches, routers, antivirus, network, source code, procedures, UPS, generators, and others,(c) location, the room is the primary server (data center) located in Jakarta and the space is the server backup (Data Recovery Center).

The next step is the process of analyzing the gap (gap analysis). It was conducted to determine the condition of the maturity level of the information security system that has been run by the company today. For analysis, we used the domain and control ektive from Annex-A standard ISO 27001:2005.

In the analysis process of risk management, risk identification is carried out, and the evaluation of risks, risk mitigation, and control of information technology security systems is carried out.

Activities undertaken in the risk identification process are (a) the identification of all assets relating to the scope of the research; (b) identifying threats to assets; (c) identifying vulnerabilities/weaknesses that may be exploited; (d) identifying the impact if the weaknesses/weaknesses are exploited;

While in the process of risk evaluation, (a) assessing trends (likelihood) and (b) measuring the risks based on inherent risk

In evaluating the controls to determine (a) whether controls need to be implemented to reduce the risk and (b) to provide recommendations for improving procedures to improve the risk management processes of information technology security systems.

4. Result and Discussion

The purpose of this subchapter is to determine the maturity level of the information technology security system that has been implemented by the organization, beginning with the analysis process by identifying current and targeted gaps. In line with Annex A of ISO 27001: 2005, data is collected through observation and interviews based on questionnaires.

Inquiries will determine if a policy or procedure exists and if it is followed, as well as if safety-related control systems information technology is utilized. For each answer, you'll get a score in the form of a percentage (%) that shows how close the current information security system is to what it should be.

Considered conformity parameters are (a) whether existing policies and procedures are executed, (b) whether existing controls are executed, and (c) the conformity between policy and control exercised. The table below contains six parameters to be used in the evaluation of conformity weights. This article was released on August 1, 2010.

Table 1 Maturity scale

Scale (%)	Description
0	Procedure = No; Control = No
25	Procedure = No; Control = Yes
50	Procedure = Yes;Control = No
75	Procedure = Yes; Control = Yes, but do not accordance to procedure
100	Procedure = Yes; Control = Yes

A division of Information Technology Systems and Operations is responsible for completing this questionnaire via direct interviews with the relevant work units. This interview's staff is currently responsible for system security and policy, data center operations and recovery, and software development. In addition to information about the state of information technology security systems, we will investigate and receive data about an incident involving information technology systems that occurred during this time period.

After obtaining all of the responses from respondents through interviews and questionnaires, the responses were categorized according to domain control and ISO 27001: 2005. Then, the responses are assigned a weight/value proportional to the data. To calculate the weight/value of per-domain, the value per control will be averaged and then used to calculate the weight/value. The conformity/maturity scale ranges from 0 to 100 percent, with 0 indicating that no procedures or controls are currently in operation and 100 indicating that all existing procedures and controls are in accordance with the current state of operations. The outcomes of domain-based calculations are displayed in Table 2.

Table 2: Current maturity level

Clause	Domain / Control	Current Condition (%)
A5	Security Policy	75
A6	Organization of Information Security	83
A7	**Asset Management**	**60**
A8	Human Resources Security	78
A9	**Physical and Environmental Security**	**69**
A10	Communications and Operations Management	84
A11	Access Control	74
A12	Information System Acquisition, Development and Maintaining	77
A13	Information Security Incident Management	75
A14	**Business Continuity Management**	**55**
A15	**Compliance**	**93**

As shown by the data presented above, multiple domains, including asset management (60%), physical and Environment security (69%), and business continuity management (55%), have a low level of compliance or maturity, as shown by the data presented above (55 percent). Currently, compliance has reached 93 percent, which is close to the desired level of conformity. The level of compliance and maturity of the enterprise IT security system is currently 75%.

The risk management analysis process has included identification (assets, vulnerabilities, and threats), impact analysis, risk assessment, and risk treatment and mitigation, as depicted in Fig. 2.

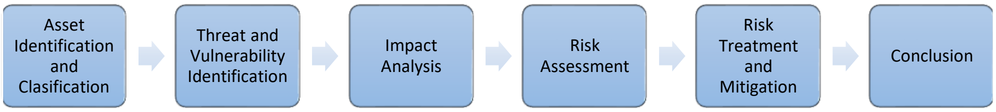
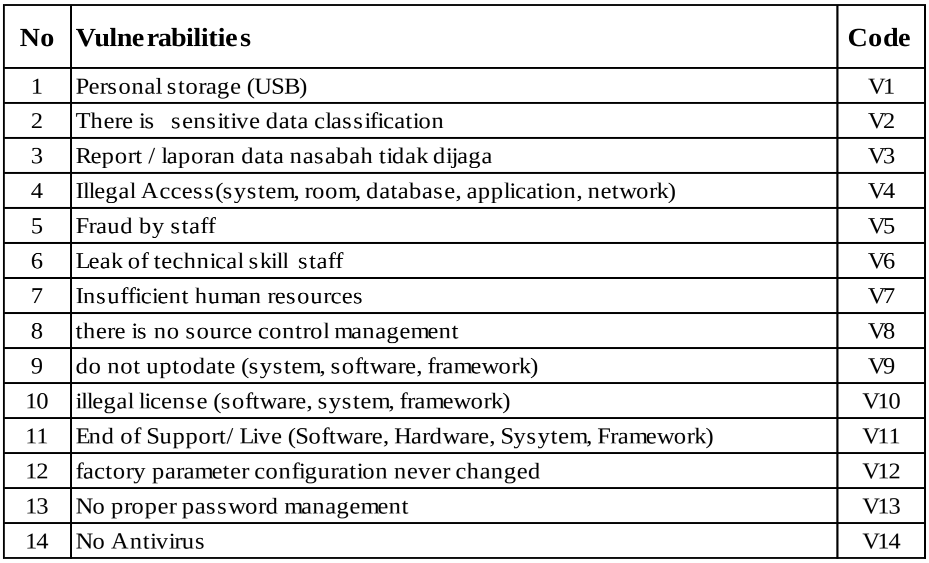

Asset Identification and Clasification
Threat and Vulnerability Identification
Impact Analysis
Risk Assessment
Risk Treatment and Mitigation
Conclusion

Fig. 2: The Risk management analysis process

Vulnerability identification is performed to determine the vulnerability of what could occur and the source of these vulnerabilities, as they can originate from the asset itself or anything else that can be exploited by internal or external parties. The enterprise information system could be endangered by the absence of security procedures, technical controls, physical controls, or other controls that could be exploited by threats. The vulnerabilities that currently exist in information security systems are detailed in Table 3.

Table 3 Vulnerability Identification



No	Vulnerabilities	Code
1	Personal storage (USB)	V1
2	There is sensitive data classification	V2
3	Report / laporan data nasabah tidak dijaga	V3
4	Illegal Access(system, room, database, application, network)	V4
5	Fraud by staff	V5
6	Leak of technical skill staff	V6
7	Insufficient human resources	V7
8	there is no source control management	V8
9	do not uptodate (system, software, framework)	V9
10	illegal license (software, system, framework)	V10
11	End of Support/ Live (Software, Hardware, Sysytem, Framework)	V11
12	factory parameter configuration never changed	V12
13	No proper password management	V13
14	No Antivirus	V14

The identification of threats was conducted in order to determine all potential threats that could compromise vital company assets by exploiting a weakness. If threats are made by exploiting existing vulnerabilities, it will have a negative impact on operational, reputational, and even business firms.

Table 4: Threat identification

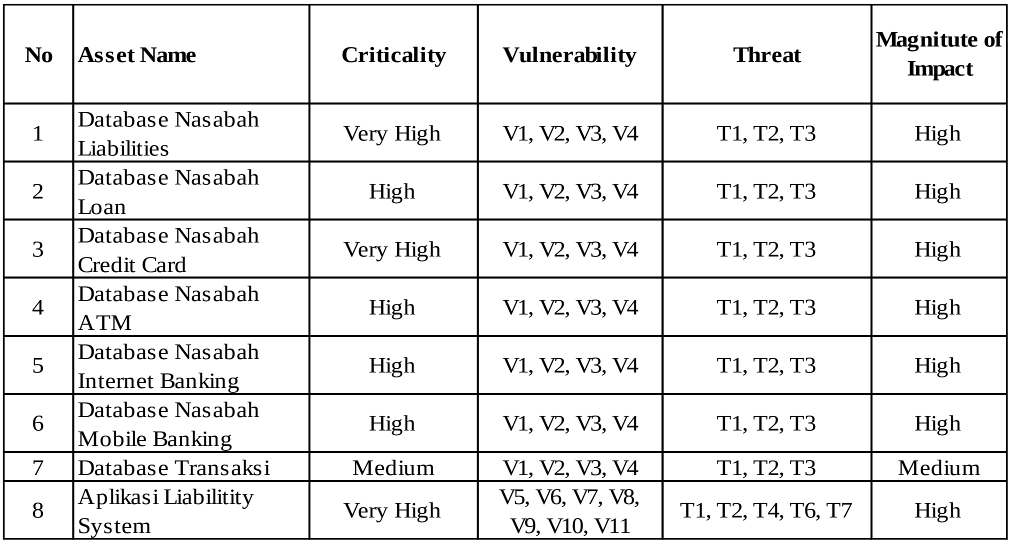
No	Threat (Ancaman)	Code
1	Malfuction or failure (system, software, database, storage, hardware, etc.)	T1
2	Illegal use of user-id (illegal access and authorized)	T2
3	Stolen (data, hardware)	T3
4	Malicious Software (Virus, Trojan, time bomb, etc.)	T4
5	Stolen of customer funds	T5
6	Error program logic	T6
7	Back-door access	T7
8	Phising	T8
9	Hardwaredestruction	T9
10	Parameter setting error	T10
11	Sniffer	T11
12	Insufficient staff	T12
13	Sabotage (Power Supply, AC, Genset, UPS, Cable, Network)	T13

14	Supplies Malfunction (AC, Genset, UPS, Network Device & Cable)	T14
15	System Capacity Overload (Database, Network, CPU, Storage)	T15
16	Data Center Building destruction	T16
17	Natural disaster	T17

The subsequent step is to analyze the impact of an incident, issue, or problem caused by the successful exploitation of a vulnerability by external and internal parties. Our operations, business, and company's reputation will be affected by the occurrence of the aforementioned. To conduct the impact analysis, the following steps were taken: (a) using identified data assets; (b) analyzing each asset's vulnerability; (c) analyzing any potential threat to assets; and (d) providing an assessment of the impact if the threat materialized.

The following are the outcomes of the asset impact analysis:

Table 5: Impact analysis



No	Asset Name	Criticality	Vulnerability	Threat	Magnitute of Impact
1	Database Nasabah Liabilities	Very High	V1, V2, V3, V4	T1, T2, T3	High
2	Database Nasabah Loan	High	V1, V2, V3, V4	T1, T2, T3	High
3	Database Nasabah Credit Card	Very High	V1, V2, V3, V4	T1, T2, T3	High
4	Database Nasabah ATM	High	V1, V2, V3, V4	T1, T2, T3	High
5	Database Nasabah Internet Banking	High	V1, V2, V3, V4	T1, T2, T3	High
6	Database Nasabah Mobile Banking	High	V1, V2, V3, V4	T1, T2, T3	High
7	Database Transaksi	Medium	V1, V2, V3, V4	T1, T2, T3	Medium
8	Aplikasi Liabilitity System	Very High	V5, V6, V7, V8, V9, V10, V11	T1, T2, T4, T6, T7	High

The next step in the risk management analysis process is to conduct a risk assessment after analysing the impact assessment on assets. Risk assessment is a method for determining the frequency (likelihood) and severity (impact) of a risk, which is then utilized to calculate the basic risk/value of the current risk (Inherent Risk). Before we do the risk assessment, we need to figure out the risk criteria for impact scale, likelihood scale (the higher the scale, the more likely it is that this will happen), and risk level. The impact scale measures how much the above things will affect the company's operations, business, and reputation.

This risk level matrix is necessary for determining or assessing the risk level of an asset. The scale of possibility/likelihood will have a value between 0.1 and 1, whereas the scale of impact will have a value between 10 and 100. The risk of a basic value is determined by the product of the likelihood function and the impact function. This is done by multiplying the likelihood value by the value's impact (inherent risk).

The following are the outcomes of the Impact Scale :

Table 6: Impact scale

Magnitute of Impact	Impact Definition
Low	Downtime < 5 hours
	No impact to organization business
	Impact to operational organization
Medium	Downtime 6 - 12 hours
	Impact to business and reputation organization
	Impact to operational organization
High	Downtime > 12 hours
	Very Bad impact to business and reputation organization
	Operational damage

The following are the outcomes of the Likelihood scale :

Table 7: Likelihood scale

Magnitute of Impact	Impact Definition
Low	Probably 0 – 5 times per year
Medium	Probably 6 – 10 times per year
High	Probably can more than 10 times per year

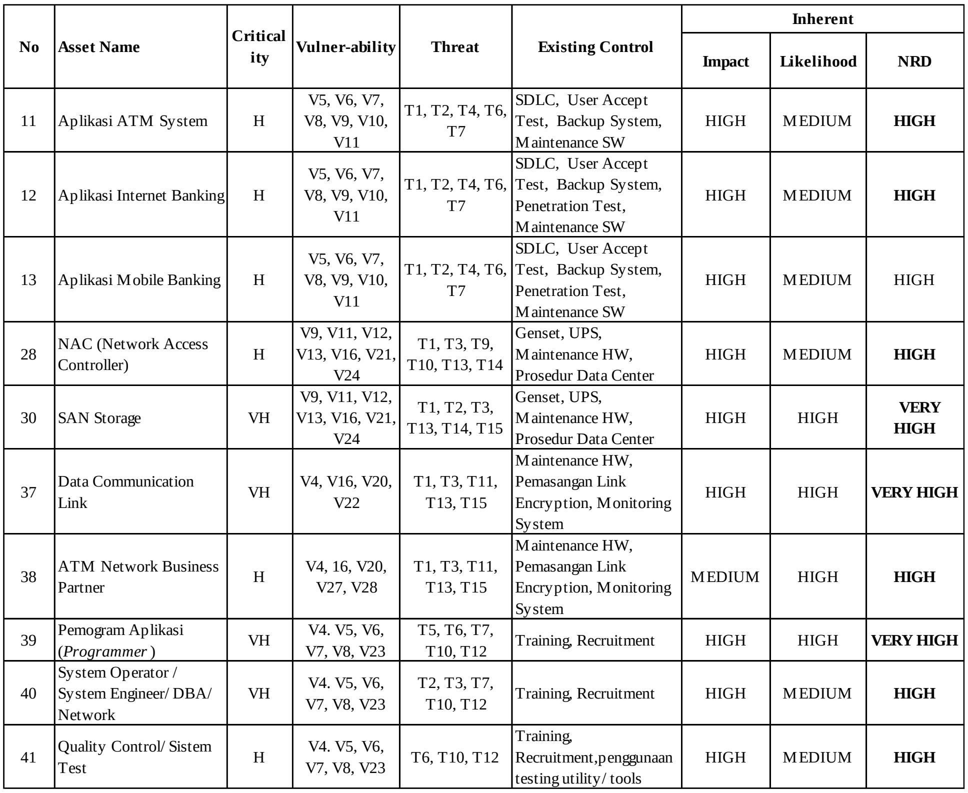
The following are the outcomes of the Risk Level Matrix:

Table 8 Risk Level Matrix

Threat Likelihood	Impact Level		
	Low (10)	Medium (50)	High (100)
Low (0.1)	Low (1)	Low (5)	Medium (10)
Medium (0.5)	Low (5)	Medium (25)	High (50)
High (1.0)	Medium (10)	High (50)	Very High

Below are the results of an assessment of the risks that exist today along with controls what is already run by the company to minimize the threats that result in business risks.

Table 9 Inherent Risk Result



No	Asset Name	Criticality	Vulner-ability	Threat	Existing Control	Inherent		
						Impact	Likelihood	NRD
11	Aplikasi ATM System	H	V5, V6, V7, V8, V9, V10, V11	T1, T2, T4, T6, T7	SDLC, User Accept Test, Backup System, Maintenance SW	HIGH	MEDIUM	**HIGH**
12	Aplikasi Internet Banking	H	V5, V6, V7, V8, V9, V10, V11	T1, T2, T4, T6, T7	SDLC, User Accept Test, Backup System, Penetration Test, Maintenance SW	HIGH	MEDIUM	**HIGH**
13	Aplikasi Mobile Banking	H	V5, V6, V7, V8, V9, V10, V11	T1, T2, T4, T6, T7	SDLC, User Accept Test, Backup System, Penetration Test, Maintenance SW	HIGH	MEDIUM	HIGH
28	NAC (Network Access Controller)	H	V9, V11, V12, V13, V16, V21, V24	T1, T3, T9, T10, T13, T14	Genset, UPS, Maintenance HW, Prosedur Data Center	HIGH	MEDIUM	**HIGH**
30	SAN Storage	VH	V9, V11, V12, V13, V16, V21, V24	T1, T2, T3, T13, T14, T15	Genset, UPS, Maintenance HW, Prosedur Data Center	HIGH	HIGH	**VERY HIGH**
37	Data Communication Link	VH	V4, V16, V20, V22	T1, T3, T11, T13, T15	Maintenance HW, Pemasangan Link Encryption, Monitoring System	HIGH	HIGH	**VERY HIGH**
38	ATM Network Business Partner	H	V4, 16, V20, V27, V28	T1, T3, T11, T13, T15	Maintenance HW, Pemasangan Link Encryption, Monitoring System	MEDIUM	HIGH	**HIGH**
39	Pemogram Aplikasi (*Programmer*)	VH	V4. V5, V6, V7, V8, V23	T5, T6, T7, T10, T12	Training, Recruitment	HIGH	HIGH	**VERY HIGH**
40	System Operator / System Engineer/ DBA/ Network	VH	V4. V5, V6, V7, V8, V23	T2, T3, T7, T10, T12	Training, Recruitment	HIGH	MEDIUM	**HIGH**
41	Quality Control/ Sistem Test	H	V4. V5, V6, V7, V8, V23	T6, T10, T12	Training, Recruitment,penggunaan testing utility/ tools	HIGH	MEDIUM	**HIGH**

Based on the outcomes of measurements of residual value risk, no assets with a value of high or extremely high risk have been downgraded to medium.

A business plan must include a control recommendation in order to reduce the level of risk to an acceptable level. The company will be advised to implement certain objective controls from Annex A of ISO/IEC 27001:2005.

The following is a list of control objectives that will be recommended for implementation based on the results of the implementation of the gap analysis, which indicates that the current conditions are low and critical.

Table 11: Control recommendation

No	Clause	Control Recommedation	Justification
1	A.7.1	Responsibility for assets	To identify the assets of the organization and determine the proper protection responsibilities

2	A.7.2	Information classification	Ensuring that the information belongs to the organization had received an adequate level of security
3	A.8.2	During employment	Ensuring that that employees, contractors / vendors and third parties to understand the threats and information security related rules, responsibilities and able to support the information security policies of the organization in order to reduce the risk of human error in carrying out their daily work.
4	A.9.1	Secure areas	Prevent unauthorized physical access, damage and disruption to the territories and information organization
5	A.9.2	Equipment security	efforts to prevent asset theft, loss, damage and disruption to organizational activities
6	A.10.1	Operational procedures and responsibilities	Guaranteeing operational information processing facilities appropriately and safely
7	A.10.2	Third party service delivery management	Guarantee the level of information security and the delivery of services according dengen agreements with third parties
8	A.10.3	System planning and acceptance	plans to minimize the risk of system failure
9	A.10.4	Protection against malicious and mobile	Protect the integrity of software and information from threats.
10	A.10.5	Back-Up	Maintaining the integrity of the availability of data, information and application facilities to generate information
11	A.10.6	Network security management	Ensure the protection of information exchange on computer networks and infrastructure facilities
12	A.10.10	Monitoring	Detecting access to unauthorized data and information processing activities.
13	A.11.2	User access management	Ensure that only users have permission to access and to prevent unauthorized users from accessing company information systems
14	A.11.3	User responsibility	Ensure that only users have permission to access the information system and prevent unauthorized user access to systems.
15	A.11.5	Operating system access control	Avoid unauthorized access to the operating system
16	A.11.6	Application and information access control	Avoid unauthorized access to the information on the application system
17	A.12.5	Security in development and support processes	Maintaining the security of application software support and information system development

18	A.12.6	Technical vulnerability management	Reducing the occurrence of risks caused by technical vulnerability exploits published.
19	A.15.1	Compliance with legal requirement	Preventing breach of duty to the law, legislation, regulations and contractual obligations as well as other security requirements applicable

To control that is not recommended because it is not within the scope of the security system is considered to be included in the Statement of Applicability (SOA).

5. Conclusion

There are some of the findings and recommendations from studies conducted:

1. The results of the condition of the security system technology's gap analysis.
2. The current maturity level has reached 75%, according to information gathered using a checklist based on Annex A of ISO standard 27001:2005. Business continuity management, which has reached a maturity level of 55%, requires a revision or improvement of business continuity management procedures at this time. While domains with a high level of maturity have achieved 93 percent compliance,
3. Based on the results of the risk assessment (risk assessment), there are three (3) information technology asset value basis risks (inherent risks) that are extremely high (extremely high) and seven (7) asset value basis risks that are high, and it is recommended to perform repair procedures in order to reduce the risk level of the enterprise information technology security system.
4. Priority application that repairs to the control procedure to maintain the availability of SAN Storage and Data Communication and to improve human resource capacity, particularly application programmers with training, to enhance application programmers' skills.

To continue the research, it is necessary to conduct a cost-benefit analysis of the impact of whether a control will be implemented or not. This is done to ensure that the control that will be implemented provides the greatest benefit at the lowest cost while also taking into account the level of risk that would exist if no controls were implemented.

Based on the results of the risk assessment, the recommendation to perform implementation of the recommendation based on prioritization of information technology assets with the highest risk or very high risk in advance (Table 11).

At the moment, the organization doesn't have a raw information security system framework. To manage the risk management system of information technology security, the organization needs to choose a implementation or security of information systems framework, such as ISO 27001.

Acknowledgement

This research can be completed with the support of all parties who have assisted in data collection at the assets software, hardware, computer network and infrastructure in Banking companies area case which was used as the object of research, I am thank to Yoyo Juhartoyo as the author, and also to Bina Nusantara University who has provided the means and support facilities in research funding and publications.

References

Al Bone (2008). Rancangan sistem Jaringan Perusahaan, *MTI*, 2008.

Barry L Cushing dan Midzan Sutanto (2000). *Sistem Informasi Akuntansi 1*. Bandung: Lembaga Informasi Akuntansi, 2000.

Darmawi (2010). *Manajemen Risiko*. Jakarta: Bumi Aksara, 2010.

Djohan putro (2008). *Manajemen Risiko Korporat*. Jakarta: PPM, 2008.

Hughes (2006). Five to IT risk management best practice. *Risk Manag*, 53(18), 7-14.

ISACA (2010). *Certified Information Security Manager*: Review Manual 2011.

ISF, IR AM. (2010) https:// www.securityforum.org/?page=Documen tView& itemid=4414.June 2010.

ISO IEC 27001 (2005). Information Technology – Security Techniques – Information Security Management System – Requirment.

Iswari (2011). Penggunaan Teknik Data Mining untuk Manajemen Resiko Sistem Informasi Rumah Sakit. Bandung: ITB.

ITGI. (2009). Enterprise risk: Identify, govern and manage IT risk, the risk IT framework. Exposure Draft.

Jakaria, D. A., Dirgahayu, R.T., & Hendrik. (2013). Manajemen risiko sistem informasi akademik pada perguruan tinggi menggunakan metoda octave allegro. *Pada Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 15 Juni*, Yogyakarta.

John F Nash dan Midzan Sutanto. (2000). Sistem Informasi Akuntansi 1. Bandung: Lembaga Informasi Akuntansi, 2000.

Kominfo. (2011). Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Jakarta: Tim Direktorat Keamanan Informasi.

Kountur, R. (2008). Manajemen risiko operasional perusahaan. Pendidikan Pembinaan Manajemen. Jakarta.

Lokobal dkk (2014). Manajemen risiko pada perusahaan jasa pelaksana konstruksi di propinsi papua (Study Kasus di Kabupaten Sarmi). *J. Ilm. Media Eng.*, 109–118.

Loosemore, Reilly & Higgon (2006). Risk Management in Projects. USA: Tailor & Francis.

Mc Cuaig, B. (2008). Fundamentals of GRC: Mastering risk assessment [White Paper]. Thomson Reuters.

Napitupulu S. J. (2009). Pengukuran risiko operasional dengan metode agregating value at risk. Skripsi pada FMIPA Universitas Sumatera Utara:Tidak diterbitkan.

Peraturan Bank Indonesia Nomor : 9/15/PBI/2007. Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum. Retrieve June 1, 2016 from http://www.bi.go.id/id/peraturan/perbankan/Pages/PBI9_17_2007.aspx.

Romney, (2004). Accounting Information System. Jakarta: Salemba Empat.

Sarno dan Iffano. (2009). Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.

Stoneburner, G. (2002). Risk Management Guide for Information Technology Systems: Recomendations of the National Institute of Standards and Technology. U.S. Departement of Commerce.

Supradono, (2009). Manajemen risiko keamanan informasi dengan menggunakan metode octave (operationally critical threat, asset, and vulnerability evaluation. *Media Elektr,* 4-8.

Sutanto, (2000). Sistem Informasi Akuntansi 1. Bandung: Lembaga Informasi Akuntansi.

Vlasta S. & Fleischmann, M. (2011). IS/IT risk management in banking industry. *AOP*, ISSN 0572-3043, 19(3).

Youssef T. & Vida, D. (2016). Information and communication technologies in energy management. *Journal of System and Management Sciences*, 6(4), 67-81. ISSN 1816-6075 (Print), 1818-0523 (Online).