Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 938-946
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Information Security Risk Analysis of State-Owned Bank Information Technology (IT) Assets Using the Octave Allegro Method

Muhammad Azel Tasya[1], Dawam Dwi Jatmiko Suwawi[2], Rio Guntur Utomo[3]
[1,2,3]Telkom University, Jawa Barat, Indonesia
e-mail: azeltasha@student.telkomuniversity.ac.id[1], dawamdjs@telkomuniversity.ac.id[2], riogunturutomo@telkomuniversity.ac.id[3]

Abstract

Utilization of Information Technology (IT) in companies today is an important element to support the effectiveness & efficiency of business processes. This research set PT ABC as a case study place. In utilizing its IT assets, the company has a division that is responsible for managing and managing the company's IT assets, namely the IT Asset division. The IT Asset Division of the Company has never conducted a security risk analysis on its IT assets. In helping companies to determine the level of information security of their IT assets, an analysis of the information security risks of these assets will be carried out. This study uses the OCTAVE Allegro method in analyzing the company's IT assets. OCTAVE Allegro consists of eight stages and is grouped into four phases. The research resulted in 5 risks from 7 IT assets which were analyzed and made into a Risk Register document. Furthermore, the researcher recommends ISO 27002:2014 control of the IT asset risk as a mitigation measure.

Keywords*: IT Assets, Risk, Risk Analysis, OCTAVE Allegro, ISO 27002:2014*

Abstrak

Pemanfaatan Teknologi Informasi (TI) pada perusahaan saat ini menjadi suatu elemen penting untuk menunjang efektivitas & efisiensi proses bisnis. Penelitian kali ini menetapkan PT ABC sebagai tempat studi kasus. Pada pemanfaatan aset TI-nya, perusahaan tersebut memiliki divisi yang bertanggung jawab dalam mengelola dan memelihara aset TI perusahaan, yakni divisi IT Asset. Divisi IT Asset perusahaan tersebut belum pernah melakukan analisis risiko keamanan informasi terhadap aset TI-nya. Untuk membantu perusahaan untuk mengetahui tingkat keamanan informasi aset TI-nya, akan dilakukan analisis risiko keamanan informasi dari aset tersebut. Penelitian menggunakan metode OCTAVE Allegro dalam menganalisis aset TI perusahaan. OCTAVE Allegro terdiri atas delapan tahapan dan dikelompokan menjadi empat fase. Penelitian menghasilkan 5 risiko dari 7 aset TI yang dianalisis dan dijadikan suatu dokumen Risk Register. Selanjutnya peneliti memberi rekomendasi kontrol ISO 27002:2014 terhadap risiko aset TI tersebut sebagai suatu langkah mitigasi.

Kata kunci*: Aset IT, Risiko, Analisis Risiko, OCTAVE Allegro, ISO 27002:2014*

1. INTRODUCTION

Utilization of Information Technology (IT) in companies (agencies) is currently an important element to support the effectiveness & efficiency of business processes [1]. The role of IT can improve the quality of services to achieve business goals [1]. Utilization of IT must be accompanied by appropriate and relevant management to minimize the risks that may arise [1]. The benefits of IT are not only as the main support facility but also the main key in effective service for the company [1], especially in the utilization of IT assets of PT ABC. Based on the green book of the PT ABC Regional Office, the company currently has around 200 employees. In utilizing IT assets, the division responsible for managing and maintaining the company's IT assets is the IT Asset division.

IT assets are goods that are valued by a company or company that can provide benefits to the company's operational activities [2]. Tangible and intangible assets can be used as company tools [2]. In the utilization of IT assets, risk management is needed [3]. According to Arthur J. Keown [3], risk is the prospect of an unfavorable outcome, where the actual result may differ from the expected result. IT asset risk management is expected to reduce the impact of risk on the company's business areas [4].

Based on the results of interviews with PIC related divisions PT ABC has never conducted an information security risk analysis on its IT assets. This is certainly a problem, because the company is one of the largest banking service companies in Indonesia. Business areas that have an impact on PT ABC can be in the form of a decline in reputation due to an unsafe and frequently disturbed system, decreased productivity due to many employees coming in and out, financial losses due to reduced productivity, fines and penalties due to lawsuits, as well as employee health and safety conditions that are not considered because the financial area is disrupted. Therefore, so that the service quality of the company is well maintained, the author will conduct an information security risk analysis on its IT assets and provide control recommendations as a mitigation measure against the risk of these assets.

The method used in the analysis of IT asset information security risk is the OCTAVE Allegro method. As a compared to other methods, OCTAVE Allegro method can identify IT assets, vulnerabilities, and threats to IT assets quickly, precisely, and accurately without the need for extensive knowledge of risk management [5]. This method is widely applied to companies with more than 100 employees [5]. The OCTAVE Allegro method is considered suiTable and can be applied according to the conditions of PT ABC. Furthermore, providing control recommendations, the standard used is ISO 27002:2014. Selection of ISO 27002:2014 because ISO 27002 provides guidance on information security control practices and is a standardization of information security management, commonly called ISMS (Information Security Management System) [6]. This research produces a Risk Register document. Therefore, the findings of the IT asset analysis using the OCTAVE Allegro method are the contents of the Risk Register document.

2. RESEARCH METHODOLOGY

2.1. Data Collection Techniques

The study was conducted at PT ABC from March to April 2022. The data was collected through interviews and observations. Interviews were conducted by asking for data related to IT assets and risks from those IT assets to the PIC of the IT Asset division. The data generated is in the form of primary/qualitative data by generating data that will be used for the risk analysis process with the OCTAVE Allegro method.

Table 1. Research Data Needs

Data source	Data Name	Data Benefit
PT ABC	IT Asset List	Knowing what IT Assets Division's IT assets are
	Risk Measurement Criteria	Knowing the level of risk for several aspects of the company
	Information Asset Container	Knowing the IT asset wrapper
	Enterprise IT Asset Vulnerabilities	Knowing the vulnerabilities of IT assets
	IT Asset Threat Scenarios	Knowing how IT assets can be threatened/disrupted
	Risks that may occur	Knowing the risks that may occur in IT assets

2.2. Data Analysis Using OCTAVE Allegro Method

Each stage of the eight stages of OCTAVE Allegro is further broken down into several risk assessment activities that will be carried out. In this process, findings will be produced in the form of a Risk Register. In facilitating its implementation, OCTAVE Allegro provides guidelines in the form of worksheets 1 to 10.

Table 2. Step of OCTAVE Allegro Method

No	Activity	*Output*	*Worksheet*
1	Establish Risk Measurement Criteria	Company risk measurement criteria from the lowest to the highest	*Allegro Worksheet 1-6 and 7*
2	Developing Information Asset Profile	Profile of critical information assets	*Allegro Worksheet 8*
3	Identifying Containers of Information Assets	Mapping the risky asset environment	*Worksheets 9a, 9b, and 9c*
4	Identifying Area of Concern	Information asset vulnerabilities	*Worksheet 10*

No	Activity	*Output*	*Worksheet*
5	Identifying Threat Scenarios	Matrix value as a reference for assessment in risk analysis	*Output 4 (Information Asset Risk Environment Maps) Worksheet 10 Information Asset Risk Worksheets Column (6) worksheets aset information and container*
6	Identifying Risk	Nilai Matriks sebagai acuan penilaian dalam analisis risiko	*Information Asset Risk Worksheet*
7	Risk Assessment	Impact area value Table, relative risk score Table is obtained based on the specified matrix value	*Risk Measurement Criteria Step 1 • Information Asset Risk Worksheets 10*
8	Mitigation Considerations	Mitigation action decisions based on risk assessment matrix	

2.3. Giving Control Using ISO 27002:2014

The provision of control recommendations for ISO 27002:2014 is carried out by the author and the company qualitatively. The author summarizes the entire control of ISO 27002:2014 into several parts that are suiTable and appropriate for the findings. The author will provide recommendations to the IT Asset PIC in the selection of controls, if the PIC agrees to the recommendations, then it is certain that the controls provided are suiTable and appropriate.

3. RESULT AND DISCUSSION

3.1. Establish Risk Measurement Criteria

In the first step in OCTAVE Allegro, the researcher held a discussion with PIC IT Asset regarding the identification of the consequences of a risk on several areas that have an impact on the company's business. The researcher asked about the risk measurement criteria that will be used to evaluate the impact on each area and prioritize them. In the risk measurement criteria, there are qualitative measures that will form the basis of the risk assessment of information technology assets. These measures have low, medium, and high values. Risk measurement Criteria can be seen on Table 3. Risk Measurement Criteria.

Table 3. Risk Measurement Criteria

***Allegro Worksheet* 1**	**Risk Measurement Criteria – Reputation and Trust in Employees**		
Aspect	Low	Medium	High
Reputation	The loss of consumer confidence is marked by a decrease in product use by <5%.	Loss of Consumer Confidence is marked by a reduction in product usage by >5% - <10%	Loss of Consumer Confidence is marked by a decrease in product use by >10%

3.2. Developing Information Asset Profile

The next step is to build a profile of the company's information assets. An information asset profile is different from a risk profile. Information asset profile is a representation of information assets that describe unique features, qualities, characteristics, and values [10]. This method is useful for ensuring that these assets are clearly and consistently described to avoid ambiguous definitions of asset boundaries, commonly referred to as rational selection [10]. The list of information asset profiles was obtained through interviews with PIC IT Asset. The information asset profile can be seen in Table III. Information Asset Profile. Information Asset Profile can be seen on Table 4. Information Asset Profile.

Table 4. Information Asset Profile

***Allegro Worksheet* 7**	**Critical Asset Information**
Critical Assets	**Rational Selection**
Server	Serve and take full responsibility for data requests from client computers. In addition, the server function is also to set access rights to the network that can be used by client computers

3.3. Identifying Containers of Information Assets

After the information asset profile is generated in section 3.2, the third step is to identify the information asset container. Containers are places where information assets are stored, shipped, and processed. There is only one activity in this step, which is to identify three main points regarding security and the concept of asset information containers. The three main points consist of a technical information asset container, a physical information asset container, and a human resource information asset container. The list of information asset containers was obtained through an interview with PIC IT Asset. Asset Information Container can be seen on Table 5. Asset Information Container.

Table 5. Asset Information Container

***Allegro Worksheet* 8b**	**Identification (Mapping) Environmental Risk Critical Assets (Physical)**
Internal	
Container Description	Owner
Cable of Internet	PIC IT Asset
Server	PIC IT Asset
Laptop	PIC IT Asset
Computer	PIC IT Asset
Router	PIC IT Asset

3.4. Identifying Area of Concern

The fourth step is identification of Area of Concern. Area of Concern is an area that is vulnerable to risk or threat by reviewing each asset container to see and determine potential areas [9]. Furthermore, the Area of Concern is expanded to obtain threat scenarios. The list of Area of Concern was obtained through an interview with PIC IT Asset. The area of concern identification can be seen in Table 6. Area of Concern.

Table 6. Area of Concern

No	**Area of Concern**	**Related Asset**
1	Employees are less careful in inputting program code and High server workload	Server

3.5. Identifying Threat Scenarios

In this fifth step, the Areas of Concern previously identified in sub-chapter 3.4 are expanded into threat scenarios. This threat scenario means a detailed description of the attributes of a threat. in it there are actors, means, consequences, risk, and security requirements. This step is useful for considering the possibilities in a threat scenario. Asset threat scenarios were obtained through interviews with PIC IT Asset. The threat scenarios can be seen in Table 7. Threat Scenarios

Table 7. Threat Scenarios

No	**Area of Concern**	**Threat Scenario**	
1	Employees are less careful in inputting program code High server workload	Actor	IT Manager
		Mean	The employees made a mistake in scripting
		Consequences	Destruction

		Risk	Software Failure
		Security Requirement	Perform data backup in accordance with control policies

3.6. Identifying Risk

In the sixth step, the consequences for several areas impacting the company if a threat occurs are noted. A threat has potential consequences for each of the affected areas of the company. The relationship between the threat and the impact area is written in the form of a value. This impact value is obtained from the results of interviews with PIC IT Asset using OCTAVE Allegro. The risk identification can be seen in Table 8. Risk Identification.

Table 8. Risk Identification

Impact Area	Priority	Value	Impact Value		
			Low (1)	Medium (2)	High (3)
Reputation and Trust in Employees	1	5	5	10	15
Productivity	2	4	4	8	12
Financial	3	3	3	6	9
Fine dan Penalty	4	2	2	4	6
Safety and Health	5	1	1	2	3
TOTAL (POOL)			15	30	45

3.7. Risk Assessment

In the seventh step, a quantitative assessment of the extent to which the firm is affected by the risk is calculated. The value obtained from a risk assessment is called the relative risk value. The relative risk value refers to the risk identification criteria that have been made in sub-chapter 3.6. The relative risk value is obtained by considering the extent of the consequences of the risk on the various impact areas that have been made in sub-chapter 3.1. The risk assessment can be seen in Table 9. Risk Assessment

Table 9. Risk Assessment

No	Risk	Criteria			
1	Software Failure	Consequences	Destruction		
		Severity	Impact Area	Value	Score
			Reputation and Trust in Employees	High	15
			Productivity	High	12
			Financial	High	9
			Fine dan Penalty	Low	2
			Safety and Health	Low	1
		Relative Risk Score			39

3.8. Mitigation Considerations

The last or eighth step of the OCTAVE Allegro method is for the author and the PIC of the relevant division to determine the risks that require mitigation and develop strategies to reduce the impact of these risks. This is done by looking at which risks have a relatively high value. Furthermore, risks that are relatively high in value are recommended for control according to security needs, containers for assets, and the company's operational environment. Mitigation Consideration can be seen on Table 10. Pool Mitigation.

Table 10. Pool Mitigation

Pool	Area of Concern	Action
31 – 45	1. Software Failure 2. Network failure 3. Abuse of Access Rights 4. Human Error	Mitigation
16 – 30	5. Hardware failure	Mitigation or Pending
0 – 15	Nothing	Accepted

3.9. Result of Risk

The result based on the information security risk analysis of IT assets using the OCTAVE Allegro method in sub chapter 4.9 is 4 out of 5 risks have been obtained because they have a risk value that must be mitigated. The 4 risks are:

a) Software Failure.
b) Network Failure.
c) Abuse of Access Rights.
d) Human Error

One risk that is of moderate value is Hardware Failure. The result of the mitigation consideration according to the pool value of the risk is either mitigation or deferred. Due to the use of the device having a major effect on the company's operations, the author will still mitigate these risks so that in the end the risks that must be mitigated are five. Here are the results of the five risks that were mitigated:

a) Software Failure.
b) Network Failure.
c) Hardware Failure.
d) Abuse of Access Rights.
e) Human Error

3.10. Determination of the Risk Register

The Risk Register can be used in decision making to determine the right asset allocation for the company.

3.11. Control Recommendations Using ISO 27002:2014

The next step is to provide control over the risks contained in the Risk Register in sub-chapter 3.10. The granting of control uses the ISO 27002:2014 standard.

4. CONCLUSION

Based on the discussion related to the analysis of information security risks on IT assets of PT ABC, it can be concluded that 5 risks resulted from the 7 IT assets analyzed. Development steps are needed to mitigate it. The 5 risks are Software Failure, Network Failure, Hardware Failure, Abuse of access rights, and Human Error. The use of the OCTAVE Allegro method should be carried out by PT ABC twice a year. With this, analysis to risk mitigation, the losses incurred by the company can be reduced or generated. In addition, the results of the OCTAVE Allegro analysis in this study can be used as a reference for analyzing the risk of IT assets in other banking companies with the same company criteria.

REFERENCES

[1] Isro Mukti., Yogi. 2018., "As Management Information System Web-Based Pagar alam College of Technology". National Seminar on Information Technology (IT) and Communication (SEMNASTIK) X, Palembang-Indonesia, 19 October 2018.

[2] Tan, Ding. 2002. Quantitative risk analysis step-by-step, SANS Institute 2003.Retrievedfrom http://www.sans.org/readingroom/whitepapers/auditing/quantitativerisk-analysis-step-by-step-849. 2003.

[3] Arthur J. Keown, DF (2005). Financial Management Principles and Applications, 10th edition. Prentice – Hall (I), 9th edition. 2005.

[4] MM Maulana and SH Supangkat. (2006). Information Technology Risk Management Framework Modeling for Companies in Developing Countries. Proceedings of the National Conference on Information & Communication Technology for Indonesia, 121-126. 2006.

[5] Keating, CG (2014). Validating the Octave Allegro Information Systems Risk Assessment Methodology: A case Study. https://nsuworks.nova.edu/gscisetd 2014.

[6] SNI ISO/IEC 27002:2014 Telkom Education Foundation. "Information Technology - Security Engineering - Information Security Management System - Requirements. 2014.

[7] Sarno, & Riyanarto. (2009). ISO 27001 Based Information Security Management System. Retrieved from http://katalog.librar.unand.ac.id//index.php?p=show_detail&id=56429 Surabaya ITS Press, 2009.

[8] Tracy Whipple & Robin Pitblado. "Applied Risk-Based Process Safety: A Consolidated Risk Register and Focus on Risk Communication", Retrieved.