International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Risk Management Analysis of Public Services Information System Case Study: PT ABC

Robi Agusdinata[1], Rina Noviana[2]
[1]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424
[2]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424

***Abstract*—** *Information security is very necessary in the use of information system applications because in the process of storing and using data, threats that can affect the confidentiality, integrity and availability of information can attack the information assets. All industries require protection of their information assets especially in social security companies where there is a registered participant's personal information data, so they need more protection for their information assets. In protecting these information assets, companies must first know the risks that might occur and assess which risks have the most significant impact on their business processes and need to be addressed. This research aims to assess the risk of critical information assets owned by PT ABC, from the technical, physical, and human resources aspects, using the Octave Allegro framework. The Octave Allegro framework focuses valuations on critical information assets and is relatively easy to use because companies do not need a lot of resources to use them so they are suitable for application in small and medium-sized companies such as PT ABC. PT ABC's public service system was chosen as the object of the case study because it had not previously carried out a risk assessment. The results of this study, which used interviews and document analysis as a method of data collection showed that PT ABC needs to focus more on implementing their security controls on technical containers.*

***Keywords*—** *Risk assessment, System Information, technical, physical, people, Octave Allegro.*

I. INTRODUCTION

The rapid development of information technology that occurs very quickly makes information technology (IT) an important part of a company's success in realizing new innovations. Nowadays IT is not only a supporting unit in a company, but IT is seen as something of value for a company's operations in achieving the company's strategic business plan that is aligned with the company's vision and mission.

PT ABC is a public service delivery agency related to labor social security to address certain socioeconomic risks which is implemented using a social insurance mechanism. In serving PT ABC participants Using a website-based information system called Participant Reporting Information System (SIPP) where registered companies will register, add and subtract participants. Data stored by participants needs to be safeguarded from data leakage risks and other risk threats.

Applications that have been developed to facilitate and support operational work require good management to secure data and information in the application. Where these applications are integrated in one system connected to the internet network. The internet on the one hand helps facilitate the work of institutional work, but on the other hand the internet also opens opportunities for cybercrime to attack the internal systems of the organization. To avoid these criminal opportunities, in information system security management a firewall with configuration policies is needed to determine user access rights for certain applications. One of the policies used is to give access permissions to users through user ID and password authentication. Technological developments show that cyber crime is increasing, but the cybersecurity community also continues to develop knowledge about cybersecurity and applications to help sectors that implement information technology.

The next research manifests, Academic Information System Risk Management in Higher Education Using the Octave Allegro Method (Jakaria, Deni Ahmad, 2013) research uses the octave allegro method to be able to identify information assets, area impacts, and threat scenarios that can occur in academic information systems used at the research institution. The research produces risk assessments from external and internal parties which then proceed with making policies to make strategic planning to safeguard critical information assets as well as recovery steps if threat scenarios actually occur.

In order to improve security, the risk of cyber crime must be minimized and properly managed. Therefore, it does not only require the technology used but also conducts an assessment with the aim of managing security gaps as risks are discovered and reducing these risks to increase availability PT ABC operations. In risk management, the octave method is a method that can be used as a reference. Octave is a method developed by Carnegie Mellon university, this management is used to carry out risk management that combines analysis of organizational behavior, and technological weakness. In accordance with the above background, the risk management method that will be used for this research is the Allegro octave method

II. STUDI LITERATUR

A. Risk Management

According to Pardjo YAP (Pardjo, 2017) Risk management is an integrated part of the organizational process. Risk management is an inseparable part and is inseparable from the process of the company's activities in achieving the objectives so that risk management is not an additional task in the organization.

According to Whitman and Mattord (Whitman; et al, 2010) risk management is a process in the form of protection and control that is implemented. According to Djohanputro (Djohanputro, 2008) risk management is a structured and systematic process in identifying, measuring, mapping,

Robi Agusdinata and Rina Noviana, "Risk management analysis of public services information system case study: PT ABC," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 442-444, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

developing alternative risk management, and in monitoring and controlling the implementation of risk management. Risk management includes:

1. Reliable access to the latest risks.
2. The decision-making process is supported by a risk analysis framework and evaluation process.
3. Monitor risk.
4. Appropriate control to deal with risk.

Risk management is related, not only to the probabilities of negative risk aspects but also to positive risks, according to Hinsa Siahaan (Siahaan, 2009). A good risk management system should be able to provide confidence that by implementing risk management, organizations can reduce the uncertainty that looms in every decision making while still being able to innovate by their capabilities.

So it can be concluded risk management is a series of systematic processes to manage management implemented by individuals or in a corporate organization.

B. Risk Assessment Methods

The Technical Department of ENISA's Risk Management Section (ENISA, 2006) has listed the methods that can be used in risk management. The following are the usual methods used for risk assessment:

1. Austrian IT Security Handbook
2. CRAMM
3. Dutch A&K analysis
4. EBIOS
5. ISF methods for risk assessment and risk management
6. ISO / IEC IS 13335-2 (ISO / IEC IS 27005)
7. ISO / IEC IS 17799: 2005
8. ISO / IEC IS 27001 (BS7799-2: 2002)
9. IT-Grundschutz (IT Baseline Protection Manual)
10. MARION
11. MEHARI
12. OCTAVE
13. SP800-30 (NIST)

C. OCTAVE Allegro

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Allegro is a security framework that uses an octave approach and is designed to carry out risk assessments of an organization or company's operations to produce faster results without requiring in-depth knowledge of risk assessment. Octave Allegro is slightly different from other octave approaches because this framework focuses on information assets owned by organizations or companies in the context of how these assets are used, how they are stored, transferred and processed, as well as how threats, vulnerabilities, and disruption can occur to these assets.

Fig. 1. Steps to the Octave Allegro framework

III. RESEARCH METHODS

This study uses two methods, namely a qualitative approach and a quantitative approach. Data collection was carried out qualitatively in the form of observations, interviews, and analysis of documents held by companies relating to information security. The quantitative approach is carried out by scoring identified risks based on the results of qualitative data obtained to determine the appropriate mitigation approach for each risk. This research is a type of case study research. This case study was carried out to implement Octave Allegro's risk assessment framework on PT ABC's public service information system.

The instrument used by the study refers to The Octave allegro Guidebook, v1.0 made by Caralli, Stevens, Young, and Wilson which is used to assess risks in technical, physical, and people aspects related to critical information assets of PT ABC, determining the categories the risks of each identified risk, determine the approach needed by the company, and strategies for mitigating what can be done to reduce those risks.

IV. IMPLEMENTATION

A. Implementation of PT ABC's Public Service Information Management System

In managing public service information systems that can be accessed widely through the internet, PT ABC application uses a 3-tier infrastructure model where there is a separation between the database server and application server. To prevent data loss on the server, the system has a primary server and a backup server. The primary server is in a different location from the backup server. Availability of data is maintained by synchronizing data which is divided into two ways, namely daily backup with synchronization and incremental backup by doing data backup. Data backup is done by copying data from the server to the read-only backup server storage. Parties that often interact directly with company information assets are system administrators, database administrators, and administrative or operational departments. System administrators maintain information assets related to the application of PT ABC's information systems, database administrators monitor utilization and perform preventive and corrective maintenance of database servers, while the

Robi Agusdinata and Rina Noviana, "Risk management analysis of public services information system case study: PT ABC," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 3, pp. 442-444, 2019.

administration or operational department manages information assets related to business processes of the company obtained from participants.

Regarding the implementation of information security in the company, PT ABC does not yet have a written policy (standard operational procedure) related to security that governs this issue and specific information security training courses are held for company employees. PT ABC has also never conducted an audit or risk assessment from an independent outside party to assess the extent of the implementation of information security in the company.

B. Risk Profile

After carrying out the process of risk assessment stages from the Octave Allegro framework, a risk profile that has the potential to occur on critical information assets owned by the company is obtained.

Allegro Worksheet 7	**IMPACT AREA PRIORITIZATION WORKSHEET**
PRIORITY	**IMPACT AREAS**
5	**Reputation and Customer Confidence**
4	**Financial**
2	**Productivity**
1	**Safety and Health**
3	**Fines and Legal Penalties**

Based on the risk assessment carried out for all areas of concern, to facilitate companies in seeing which containers require more attention in their mitigation efforts, those risks can be classified based on the mitigation approach taken.

Relative Score Matrix		
Risk Score		
30-45	16-29	0-15
Pool 1 (*Mitigate*)	Pool 2 (*Defer*)	Pool 3 (*Accept*)

Risks in the Pool 1 group will be mitigated whose means for each of these risks will be controlled to reduce the impact or eliminate the threat. The risks in Pool 2 are still considered whether to be mitigated or accepted, the risks to be mitigated in Pool 2 are risks that have the characteristics of medium impact to high impact. While risks in the Pool 3 group will be accepted, which means the company will not take action because the impact is small on the company's business.

V. CONCLUSIONS AND RECOMMENDATIONS

This study was conducted to determine the compatibility of the Octave Allegro risk analysis framework implementation at PT ABC and other non-bank financial services companies. The results of this study are identified risks for each container of critical information assets and scores for each risk so that the company can determine effective and efficient mitigation strategies. Based on the results of the analysis that has been done, the conclusion that can be drawn from this study is that in general the Octave Allegro framework can be used in risk assessment on PT ABC's public service information system.

In the risk assessment conducted on PT ABC, there are 3 aspects of containers, namely technical, physical, people containers. From the results of the identification, PT ABC should focus more on the application of security controls on technical containers because based on the results of the identification of risks that have been carried out, these containers have the most risk so that various security controls need to be implemented as mitigation measures. Considering that the main business of PT ABC runs on a public service information system that is owned, the security holes in technical containers directly related to the system need to be addressed. Apart from technical containers that are the main focus, the application of information security controls also needs to be applied to people containers and physical containers because there are still risks that need to be mitigated in those containers.

REFERENCES

[1] Caralli, R. A. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Pittsburgh: Carnegie Mellon University. Retrieved March 2013, from www.cert.org/archive/pdf/07tr012.pdf

[2] National Institute of Standards and Technology (NIST). (2009). Recommended Security Controls for Federal Information Systems and Organizations. Gaithersburg: National Institute of Standards and Technology. Retrieved February 2013, from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated- errata_05-01-2010.pdf

[3] National Institute of Standards and Technology (NIST). (2011). Managing Information Security Risk. U.S. Department of Commerce. Gaithersburg: National Institute of Standards and Technology. Retrieved April 2013, from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[4] Christina, Diane. (2012). Assesmen Manajemen Risiko Berbasis ISO 31000:2009.

[5] Delamaire, Linda., Abdou, Hussein., and Pointon, John. (2009). Credit Card Fraud and Detection Techniques. Banks and Bank Systems. Volume, 4 Issue 2.