E-ISSN: 2476-9606
Abstract Proceedings International Scholars Conference
Volume 7 Issue 1, October 2019, pp. 1741-1750

https://doi.org/10.35974/isc.v7i1.1387

Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method

Elmor B. Wagiu[1], Raminson Siregar[2], Raymond Maulany[3]
Universitas Advent Indonesia
elmor@unai.edu

ABSTRACT

Universitas Advent Indonesia is one of the many universities that use information technology to support their business processes in the hope that information technology will provide significant benefits. The use of information technology in supporting a business can not be separated from the risks that might be faced. for that, good management of information technology will be the key to how much risk will be faced. In this case, the researcher will conduct an analysis of information system risk management at the Universitas Advent Indonesia. The method used by researchers is OCTAVE ALLEGRO. OCTAVE ALLEGRO is a method that is often used to carry out analysis in the field of risk management and risk assessment. The purpose of this study was to identify risks that could potentially threaten business processes at Universitas Advent Indonesia by first identifying the impact of the area, determining the scale of priorities etc. The results of the study using OCTAVE Allegro is a risk reduction approach for each area of concern of each UNAI critical information asset namely student financial information, lecturer financial information, student score information, student transcript information, and class attendance data. UNAI makes written rules regarding responsibilities in maintaining information security and sanctions for violators and do socialize about the rule well gradually to Universitas Advent Indonesia employees. Re-evaluate information security by using OCTAVE Allegro method periodically, for example, once every 2 years.

Keywords: Risk Management Analysis, Risk Assessment Analysis, Information System, OCTAVE Allegro.

INTRODUCTION

In the application of information technology in an organization, risk is one thing that must be anticipated. With the emergence of these risks, business processes in organizations have the potential to experience disruption. Universitas Advent Indonesia is one of the universities that uses information technology to support their daily activities. Almost all the main activities that are running already use information systems and information technology. The potential for the emergence of risks to information technology and information systems is also large. Besides

that, Universitas Advent Indonesia has never carried out risk measurement on information technology and has not implemented risk management. Therefore a research was made on the Analysis of Risk Management Information Systems at Universitas Advent Indonesia Using the Octave Allegro Method.

LITERATURE REVIEW

Christopher Alberts (2002) efines risk as the possibility of damage or loss. The definition above refers to a situation where someone can do something undesirable or natural events that can cause undesired results that have a negative impact on the organization.

Jake Koun (2010) said that risk is a quantitative measurement of the potential damage caused by threats, security holes, or from an event (having malicious intent or not) that affects a collection of information technology assets owned by a company.

According to Talabis and Martin (2013:28), OCTAVE is a collection of tools, techniques, and methods for risk based information security assessments. Currently OCTAVE has 3 different versions:

1. OCTAVE;
2. OCTAVE-S; and
3. OCTAVE-Allegro.

OCTAVE or (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is the original framework and is the basis for all OCTAVE types of frameworks. It is recommended for large organizations (according to SEI this typically means an organization with more than 300 employees) that have the ability and resources to conduct internal security evaluations and workshops across the organization. Among the three, this version is the most prescriptive and very closely resembles a methodology. It is very comprehensive and contains various templates such as surveys, meeting minutes, and guidelines on how to conduct workshops. This framework recommends the involvement of a wide variety of people, many of whom are not directly involved in the risk management function.

OCTAVE-S was developed for smaller organizations. According to SEI, OCTAVE-S was made for organization with less than 100 employees and would require a team of 3–5 people who are knowledgeable about the company in order to complete the evaluation. This framework assumes that the people doing the assessment know about the company's assets, security requirements, threats and security practices and thus do not require the company-wide workshops and meetings that are prescribed in the original OCTAVE framework. The

assumption that a company of only 100 employees could dedicate 3–5 people for the execution of a risk assessment is indicative of one of the major shortcomings of OCTAVE in general; an overall underestimation of the level of effort it takes to execute an assessment and the reasonable amount of resources that would have to be applied to be successful.

Finally, OCTAVE-Allegro is the most recent version of the framework. OCTAVEAllegro was specifically streamlined for information security risk assessments. Similar to OCTAVE-S, this framework does not require extensive organizational involvement. We will be focusing on the Allegro iteration of OCTAVE and all future references of OCTAVE in this book will be regarding OCTAVE-Allegro.

METHODS

The method used in this study is the Octave Allegro Method. Talabis and Martin (2013:30) explain the OCTAVE-Allegro framework describes eight steps and provides various worksheets and questionnaires as a guide and model on how to assess risk for the organization or more specifically the assets of the organization. What follows is a brief introduction to the eight steps of OCTAVE-Allegro.

1. Establish Risk Measurement Criteria

   Some of the areas that octave recommends evaluating are (the first 5 are prescribed by OCTAVE-Allegro, the Sixth is intended to be customized by your organization):

   a. Reputation/Customer Confidence.
   b. Financial.
   c. Productivity.
   d. Safety and Health.
   e. Fines and Legal Penalties.
   f. User-defined Impact Criteria.

The table below are the example of Risk Measurement Criteria.

Table 1. **Risk Measurement Criteria Allegro Worksheet – Financial**

Impact Area	Low	Moderate	High
Operating Costs	Increase of less than _____% in yearly operating costs	Yearly operating costs increase by to _____%.	Yearly operating costs increase by more than _____%.
Revenue Loss	*Less than %	*To %	*Greater than*

	yearly revenue loss	*yearly revenue loss*	*% yearly rev- enue loss*
One-Time Financial Loss	*One-time financial cost of less than $*	*One-time financial cost of $* *to $*	*One-time financial cost greater than $*
Other:			

2. Develop an Information Asset Profile

   Several important activities included in this step are:

   a. Documenting the owners.
   b. Providing a description of the critical assets.
   c. Identifying Confidentiality, Integrity, and Availability (CIA) requirements.
   d. Identifying which of the CIA requirements is most important.
   e. Rationale as to why the asset is important.

3. Identify Information Asset Container

   The information being collected here can be categorized into:

   a. Technical—Hardware, Processes, Type of Information, Vendor, Partner Information, etc.
   b. Physical—Location of the hardware/data, Data Centers, etc.
   c. People—Asset Owners, Technical Contacts, etc.

4. Identify Areas of Concern

   According to the OCTAVE-Allegro documentation, "Areas of Concern" are a descriptive statement that details a real-world condition or situation that could affect an information asset in your organization.

5. Identify Threat Scenarios

   This threat scenario consists of a statement that combines the following factors:

   a. Asset.
   b. Access/Means.
   c. Actor.
   d. Motive.
   e. Outcome.

6. Identify Risks

   This step identifies the risk for the asset by simply creating a table listing down the threat and the impact. This is represented in the following formula:

Risk = Threat (condition) + Impact (consequence)

7. Analyze Risk

   Going through this analysis helps establish a rationale to support the assignment of scores using Octave's impact scoring worksheets.

8. Select Mitigation Approach

   In OCTAVE, there are four pools:

   a. Pool 1—Mitigate.
   b. Pool 2—Mitigate or Defer.
   c. Pool 3—Defer or Accept.
   d. Pool 4—Accept.

RESULTS

Establish Risk Measurement Criteria

At this stage, the researcher conducted an interview with the head of the IT department. From the results of interviews and discussions conducted, the risk measurement criteria are determined. In this step there are 2 activities, namely the determination of the impact area and the determination of the priority scale in the predetermined impact area. The chosen impact area is the customer's reputation and trust, financial, productivity, safety and health, as well as fines and penalties.

Activity 1 – impact area determine

Table 2. **Impact area - Customer Reputation and Trust**

		LOW	***MODERATE***	***HIGH***
Customer Reputation and Trust	**Reputation**	Reputasi terkena dampak minimal; sedikit atau tidak ada upaya atau biaya yang diperlukan untuk pulih	Reputasi rusak, dan beberapa upaya dan biaya diperlukan untuk pulih	Reputasi rusak atau hancur hampir tidak bisa diperbaiki
	Customer Loss	Kurang dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	15% hingga 25% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 30% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

For the impact area of customer reputation and trust, there are 2 points that will be used as a reference, namely reputation (impact on company reputation) and customer loss (impact on decreasing number of customers).

At the point of reputation, the impact will be said to be low if the reputation is only slightly affected and almost no effort is needed to improve reputation. Impact on reputation will be said to be moderate if reputation is greatly affected and costs are needed to improve reputation. Impact on reputation will be said to be high if the impact caused is very bad and reputation can hardly be repaired.

At the customer loss point, customer participation caused by trust involvement is less than 10% for the low (small) category, between 15% - 25% for the medium (medium) category, and more than 30% for the high (high) category.

Develop an Information Asset Profile

In this step, we will determine what assets are critical to UNAI. In determining critical assets for UNAI, the assessment is carried out on the core process at UNAI. UNAI is an institution engaged in education, for that the core process at UNAI is a process that starts from registration until students graduate /wisuda.

Critical Information Assets

1. Students Financial Information
2. Staff Financial Information
3. Students Grade
4. Students Transcript
5. Class Attendance

The following is an explanation of the critical information assets that have been written above, related to rationale for selection, description, owner, security requirement, dan most important security requirement aspects. Security requirement divided into three parts, namely confidentiality, integrity, and availability.

The explanation below is the result of observations and discussions conducted by researchers with IT departments.

Students Financial Information

Table 3. **Information asset profiling – Students Financial Information**

Critical Asset	Informasi Keuangan Mahasiswa
Rationale for Selection	Informasi keuangan mahasiswa merupakan aset

		informasi yang kritikal karena berhubungan langsung dengan finansial UNAI dan merupakan salah satu penghasilan utama dari UNAI
Description		Aset ini terdiri dari kumpulan data terkait dengan transaksi pembayaran uang kuliah mahasiswa, data hasil kerja mahasiswa di UNAI, dan juga data beasiswa yang didapatkan oleh mahasiswa
Owner		UPT-Komputer, BO
Security Requirements	***Confidentiality***	Informasi mengenai keuangan mahasiswa harus dijaga tingkat kerahasiaannya dikarenakan informasi ini berkaitan langsung dengan finansial mahasiswa dan juga UNAI
	Integrity	Informasi ini harus terjaga selalu akurat karena informasi ini digunakan untuk tagihan dan informasi pelunasan pembayaran kepada orang tua dan mahasiswa itu sendiri.
	Availability	Informasi ini harus tersedia bagi dosen, mahasiswa, Biro Keuangan UNAI, dan juga orang tua mahasiswa
Most Important Security Requirement		***Integrity*** Alasan: Informasi mengenai keuangan mahasiswa harus akurat. Setelah mahasiswa melakukan pembayaran atau mendapat beasiswa, maka informasi keuangan mahasiswa tersebut harus di-*update*

Students Grade

Table 4. **Infomation asset profiling – Students Grade**

Critical Asset	Nilai Mahasiswa	
Rationale for Selection	Informasi mengenai nilai mahasiswa merupakan informasi yang berkaitan langsung dengan mata kuliah yang diambil oleh mahasiswa. Dan juga nilai ini akan mempengaruhi prestasi mahasiswa di dalam maupun di luar kampus saat sudah wisuda.	
Description	Aset informasi ini terdiri dari data mahasiswa, mata kuliah yang diambil dan juga nilai serta bobot penilaian yang didapatkan oleh mahasiswa	
Owner	UPT-Komputer, Biro Administrasi Akademik	
Security Requirements	Confidentiality	Informasi mengenai nilai mahasiswa harus dijaga privasinya oleh mahasiswa dan pihak UNAI agar tidak disalahgunakan oleh pihak – pihak yang tidak bertanggung jawab.
	Integrity	Informasi ini harus diisi dan juga harus dijaga keakuratan nilai mahasiswa tersebut.
	Availability	Informasi ini harus tersedia bagi dosen, mahasiswa yang bersangkutan, orang tua mahasiswa
Most Important Security Requirement	Integrity Alasan: Informasi nilai mahasiswa harus dijaga agar tetap akurat	

Identify Information Asset Container

Table 5. **Information Asset Containers – Students Financial Information**

Informasi Keuangan Mahasiswa	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	***Owner(s)***
Database: SunPlus Informasi keuangan mahasiswa disimpan, diambil, dan diproses dari database tersebut untuk aplikasi web	UPT-Komputer UNAI
Aplikasi: *Online System* (Modul BO) Informasi keuangan mahasiswa dapat diakses dari Modul BO untuk keperluan pencatatan pembayaran uang kuliah mahasiswa	Biro Keuangan
External	
Container Description	***Owner(s)***
Aplikasi: Modul Mahasiswa Informasi keuangan mahasiswa dapat dapat diakses oleh mahasiswa yang bersangkutan melalui aplikasi web khusus mahasiswa	Mahasiswa
Aplikasi: Modul Orang Tua Informasi keuangan mahasiswa dapat diakses oleh orang tua mahasiswa tersebut melalui *web*	Orangtua mahasiswa

Identify Areas of Concern

Students Financial Information

Table 6. **Area of Concern – Students Financial Information**

No	***Area of Concern***
1	Staff UPT-Komputer yang dapat memasukkan *malicious code*
2	Penyebaran hak akses (*password*) terhadap aplikasi *online system* (Modul BO) yang dapat mengakses dan memproses transaksi keuangan mahasiswa oleh staf BO
3	Modul BO dapat diakses oleh orang yang tidak memiliki otorisasi dari luar maupun dalam kampus
4	Pemanfaatan celah keamanan aplikasi *online system* (Modul BO) oleh pihak dalam/luar

DISCUSSION

Suggestions proposed by researchers in this study are as follows:

1. UNAI made written rules regarding responsibility in maintaining information security and sanctions for those who violated them and also conducted socialization regarding these regulations in stages to Universitas Advent Indonesia employees.

2. Re-evaluate information security using the OCTAVE Allegro method regularly, for example, every 2 years.
3. For subsequent research, the scope of research can use other departments or more specific to certain information systems.
4. In subsequent studies, the use of other methods in conducting risk assessments is highly recommended as a comparison with the research that has been done.

Conclusion

The conclusion of this research is:

1. The identified impact areas have the potential to threaten business processes at Advent University of Indonesia in order of priority scale from the highest to the lowest for the area impacts are safety and health, customer reputation and trust, productivity, financial or financial, and fines and penalties.
2. Risks that could have an impact on the institution are identified from critical information assets owned by the institution and determined areas that allow these critical information assets to have risks. Areas that allow this critical information asset in danger are staff who can enter malicious code into the system, spread access rights (passwords) of the information system at UNAI, and exploit security holes for each application that exists.
3. The priority that has been determined based on the relative value of the risk given is that the malicious code entered in the source code has the highest value because the resulting impact can cause severe damage to existing information systems and potentially damage business processes at UNAI. Then the second is the use of security holes in every information system by irresponsible parties that cause the information system to be accessed and can result in disclosure, interruption and modification of existing data.. Then the last is the distribution of access rights (passwords) to those who are not responsible.
4. Actions that can be taken to reduce risk for each area that has the potential to impact on the company are reducing malicious code that can be entered into the source code by conducting a quality assessment of the system before its use and providing training and seminars to staff about the need to safeguard information assets in company. Second, reducing the security holes in the information system by assessing the quality of the system before it is implemented to the user and providing training to system development staff in order to build a better system. Then, reducing the spread of access

rights (passwords), the way is to educate all staff how important it is to maintain the confidentiality of access rights to information systems because it can cause information systems to be accessed by people who are not responsible.

REFERENCES

Whitman, M. E. (2010). *Management of Information Security*. US: Thomson-Course Technology.

Christopher Alberts, A. D. (2002). *Managing Information Security Risks: the OCTAVE Approach (1st ed.)*. Boston, US: Addison-Wesley Professional.

Koun, J. (2010). *Information Technology Risk Management in Enterprise Environment*. New Jersey: John Willey & Sons.

Talabis, M., and Martin, J. (2013). *Information Security Risk Assessment Toolkit: Practical Assessment through Data Collection and Data Analysis*. Amsterdam, Netherlands: Elsevier.

Whitman, M. E. (2010). *Management of Information Security*. US: Thomson-Course Technology.