Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 135 (2018) 202–213

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Computer Science and Computational Intelligence 2018

Assessment Of Information System Risk Management with Octave Allegro At Education Institution

Jarot S. Suroso*, Muhammad A. Fakhrozi

Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management,

Bina Nusantara University Jakarta, Indonesia 11480

Abstract

Risk Management can reduce the risk of such as business processes that are not optimal, financial losses, declining reputation of the company, or the destruction of the company's business. To reduce damage to the information systems of the company's business process, there should be a risk management assessmentThe use of information systems required to support the company's business processes, especially in education institution, as well as the MH. Thamrin University. In the use of information systems, will appear risks that will give negative impact on the institution. To reduce the negative impact, need to do a risk assessment. The method used in this thesis is the OCTAVE Allegro. Data were analyzed using the 8 steps in the OCTAVE Allegro, and distributing questionnaires to users of information systems. The result, there are 34 areas of concern is mitigated, and the overall user feedback states agreed on mitigation steps. It was concluded that a risk assessment is useful for reducing the risks of information system

© 2018 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)
Selection and peer-review under responsibility of the 3rd International Conference on Computer Science and Computational Intelligence 2018.

*Keywords:*Assessment; Risk Management; Octave Allegro; Information System

* Corresponding author. Tel.: +62811852768; fax: +622153696969.
*E-mail address:*jsembodo@binus.edu

1877-0509 © 2018 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)
Selection and peer-review under responsibility of the 3rd International Conference on Computer Science and Computational Intelligence 2018.
10.1016/j.procs.2018.08.167

1. INTRODUCTION

Today, information technology is used as a base to support the company's business strategy, improve service quality and business processes. In use, information technology will bring risks. Management of risk are things that need attention. Management of risks can reduce the risk of such as business processes that are not optimal, financial losses, declining reputation of the company, or the destruction of the company's business. To reduce damage to the information systems of the company's business process, there should be a risk management assessment.
MH. Thamrin University is one of the educational institutions in Indonesia, located in East Jakarta, which consists of four faculties, namely the Faculty of health, computer science, economics, teacher training and science education. MH. Thamrin University has 2,307 students, 200 lecturers (permanent and non-permanent), and 165 employees. To support business processes as well as academic, of course, information system is being used to increase the value, promotion, strategy, communication, integration, and fluently of academic activities. Management and information technology risk assessment has not been done at the MH. Thamrin University, this is the basis for risk assessment at the MH. Thamrin University.

Things that underlie the need for risk assessment at the MH. Thamrin Universityis as follows:

1. The risk assessment has not been done at the MH. Thamrin Universityso it is difficult to assess how big the impact of emerging risks.
2. Lack of integrity of information systems at the MH. Thamrin University, and some departments are not fully functioning information system that makes coordination within the university becomes less accommodated process.
3. There is no formal policy on information technology security, causing the slow action taken to prevent risks that may occur as well as mitigation.
4. It is difficult to communicate the importance of the value of information assets held in the absence of documentation or supporting data.

The objective of the assessment of risk management information systems at the MH. Thamrin University:

1. Know the risks that affect the security of information assets.
2. Design some protection strategy for securing those risks.

The benefits to be achieved from the assessment of risk management information systems at the MH. Thamrin University:

1. Knowing things that affect the risk of information systems, in order to take the appropriate steps to minimize the risk of information systems.
2. Having a protection strategy designed to reduce the risk of information system security.
3. The management can communicate the importance value of information assets owned.

The scope of this discussion is:

1. The risk assessment carried out on the IT division and also on the daily operational, focusing on the protection of information assets.

Academic information system that is used by students, lectures, and employees of MH. Thamrin University.

2. LITERATURE REVIEW

The information system is a system within an organization that reconcile the needs of daily transaction processing, support the operation, managerial and strategic activities of an organization and provide certain outside parties with the reports required. Information systems are components that work together to collect, process, store and disseminate information to support decision-making, coordination, control, problem analysis and visualization in an organization [1].

Risk is the possibility of loss or damage caused by an act. Risk must be managed properly and thoroughly structured. Risk management is a structured approach to managing uncertainty that associated with the threat, or a series of human activities, including risk assessment, developing strategies to manage and mitigate risks by using empowerment / resource management. The adopted strategies, which is to transfer the risk to another party, avoiding the risk, reducing the negative effects of risk, and accommodate a part or all part of the consequences of a particular risk [2].

Risk management is a repetitive process that addresses the analysis, planning, implementation, control and supervision of the policies and measures of security policy implementation. In contrast, the risk assessment carried

out at a specific time and provides an interim figure of risk assessment and also provide measures of the risk management process [3].

With the risk management of information technology is expected to reduce the impact of the damage that could be the impact on the financial, reputation decrease due to unsafe system, a cessation of business operations, the failure of assets that can be assessed (system and data) and a delay in the decision-making process [4].

Organizations need to identify and implement appropriate controls to ensure adequate security of information [5]. Information security controls help organizations to provide the level of security needed for the organization of their information [6].

3. METHOD

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a methodology used to identify and evaluate information security risks. The use of OCTAVE itself is intended to help the company in terms of:

- Develop a qualitative risk evaluation criteria that describe the company's operational risk tolerance
- Identify the assets that are important to the company's mission
- Identify vulnerabilities and threats to those assets
- Determine and evaluate the possible consequences for the company if the threat occurred.

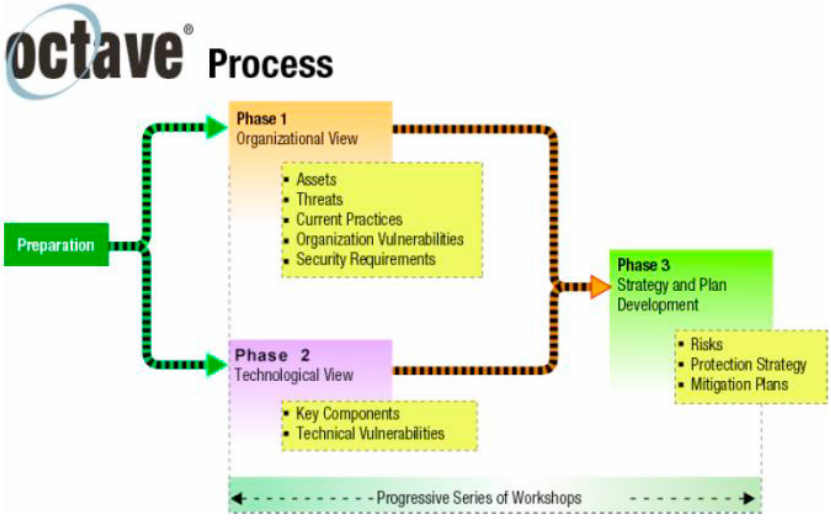

Fig 1. OCTAVE Steps [7]

Nowadays there are three variants of the OCTAVE can be used. The variants are OCTAVE method, OCTAVE-S, and OCTAVE Allegro. This three methodsare not a method that is complementary or substitute for one another. The use of these three methods are intended to meet the specific needs of the OCTAVE users who want to conduct a risk assessment.

Objectives to be achieved by the OCTAVE Allegro is a comprehensive assessment of the operational risk environment of an organization with the aim of producing better results without the need for extensive knowledge in terms of risk assessment. This approach differs from the OCTAVEapproach, which OCTAVE Allegro focus to information assets within the context of how they are used, where they are stored, transported and processed, and how they are affected by the threat, vulnerability, and disruption as a result [8].

The method used in this paper is a OCTAVE Allegromethod. OCTAVE Allegro approach aimed more specifically at information assets and data that support the information.

In the OCTAVE Allegromethod, there are four main stages, namely:

a. Establish Drivers
b. Assets Profile
c. Identify Threats

d. Identify And Mitigate Risks

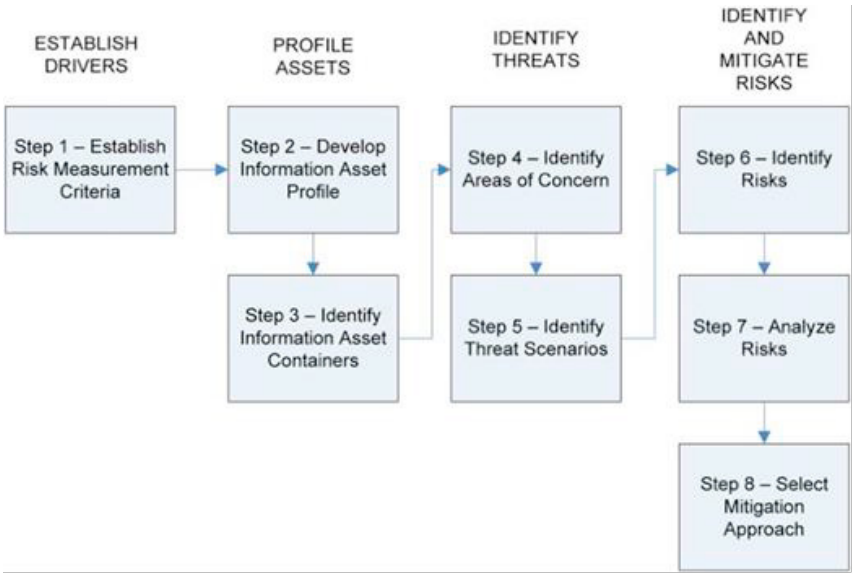

Fig2. The steps of OCTAVE Allegro [8]

4. RESULTS AND DISCUSSION

Risk assessment information systems at the MH. Thamrin University, conducted with the direct and met with the Head of IT, Head of Student Academic Administration Bureau, and Chief Financial Officer to explain the purpose of the assessment of risk information system, as well as obtaining the data that is required. Further detailed interviews were carried out to obtain critical information assets of course operational.
Once the preparation is ready and the data that required has been support, then performed a risk assessment of information systems at the MH. Thamrin University using the OCTAVE Allegro method consisting of eight steps.

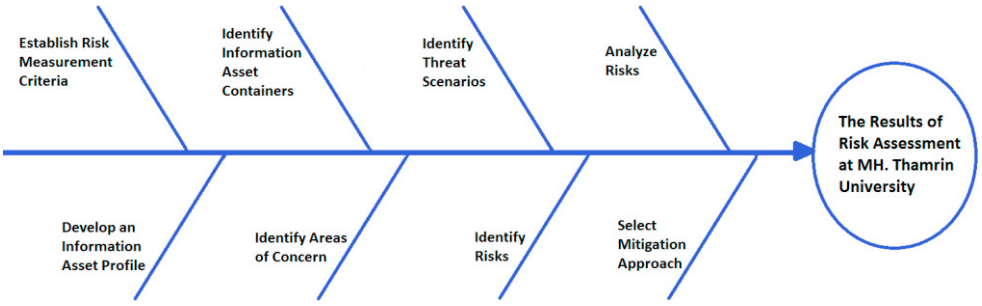

Fig 3. Framework

Step 1 : Establish Risk Measurement Criteria
At this step, the interview with the Head of IT, Head of Student Academic Administration Bureau, Chief Financial Officer, and staffs who are in the MH. Thamrin University. From the results of these interviews, criteria for risk measurement are determined. There are two activities undertaken in this step, namely the determination of the impact area, and setting priorities on the impact area. The things that being a consideration of the determination of the impact area is the mission and business objectives of the MH. Thamrin University. The selected impact area are reputation and customer confidence, financial, productivity, safety and health, as well as fines and penalties.

Table 1. Impact area prioritization

PRIORITY	IMPACT AREAS
5	Reputation And Customer Confidence
3	Financial
4	Productivity
1	Safety And Health
2	Fines And Penalties

Reputation and customer confidence is the biggest priority of the MH. Thamrin University because of the reputation and high customer confidence is indispensable in opportunities to get more students who enroll to MH. Thamrin University, as well as to facilitate the cooperation with external parties with the aim of improving the quality of students and academic activities of the MH. Thamrin University. Reputation and customer confidence certainly have direct impact on the financial, especially when the new academic year will run, making the considerations of the customer (in this case the prospective students) to enroll on MH. Thamrin University.
If there are serious problems in the area of reputation and customer confidence as well as financially, then the area of productivity will be affected, because of the decline in these two things will threaten the productivity of employees and customers MH. Thamrin University. Productivity decreases will lead to susceptibility to fines and lawsuits from related parties such *Kopertis* (Coordinator Of Private Colleges) and *Kemenristekdikti* (The Ministry Of Technology Research And Higher Education). This may have indirectly impact on health and safety area.

Step 2 : Develop an Information Asset Profile
Selected information assets is information that relating to or used in the core processes MH. Thamrin University. Critical information assets will be recorded on a worksheet critical informationasset that has been provided by OCTAVE Allegromethod. Things to be considered for selecting information assets are:
- Information asset that is important for the MH. Thamrin University
- Information asset used in the daily operations
- Information asset that if lost can interfere with the ability of the MH. Thamrin University in achieving its objectives and mission.

From the results of the above considerations, assetsthat classified as critical asset, namely:
1. Student Profile
2. Student Course Schedule
3. Student Attendance
4. Student Score
5. Payment of Tuition
6. Lecturer Profile
7. Lecturer Teaching Schedule
8. The Presence of Lecturer

Table 2. Example of Information Asset Profiling - Student Attendance

Critical Asset	Student Attendance
Rationale For Selection	Student attendance related to courses taken by the student, determine whether or not a student is entitled to follow Midterm Exam and Final Exam, as well as being one of the components of value to the final value of a course.

Description		These assets consist of courses, lecturers, study program, semester, class, and dates of attendance.
Owner		IT Division
Security Require-ment	***Confidentiality***	Student attendance information is not confidential, but it is important for students and the academic division.
	Integrity	Student attendance information should be in accordance with the actual conditions and time because related to the status of courses taken by the students.
	Availability	Student attendance information must be available for students, lecturer of the course, and the academic division.
Most Important Security Requirement		***Integrity*** Student attendance information must appropriate with the actual conditions, because in the students attendance, there is the attendance acount of each student, if it does not qualify, the student can not take the exam and affect the completion of a course taken by the student.

Step 3 : Identify Information Asset Containers

Information Asset Containers is the place where the informationasset stored, transmitted or processed. By using the worksheet Information Asset Risk Environment Map, the container was identified in which information assets are located that divided into three categories, namely:

- Technical
  Hardware, software or system that is under the control of the company (internal), and outside the control of the company (external).
- Physical
  The physical location or document that is under the control of the company (internal), and outside the control of the company (external).
- People
  Anyone who knows the information under the control of the company (internal), and outside the control of the company (external).

Table 3. Example of Information Asset Risk (Technical) - Student Attendance

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Web Server & Database : Attendance of students is stored in a database for web	IT Division

applications and desktop applications that synchronize each other	
AIS-UMHT : Attendance of students accessed through this application for collecting student attendance data	Student Academic Administration Bureau, Study Program
External	
Container Description	**Owner(s)**
Student-UMHT : Attendance of students accessed via this application to view student attendance data per course	Student

Table 4. Example of Information Asset Risk (Physical) - Student Attendance

Information Asset Risk Environment Map (Physical)	
Internal	
Container Description	**Owner(s)**
Printed student attendance files printed to be distributed during class	Study Program
External	
Container Description	**Owner(s)**

Table 5. Example of Information Asset Risk (People) - Student Attendance

Information Asset Risk Environment Map (People)	
Internal Personnel	
Name or Role / Responsibility	**Department / Unit**
Student Academic Administration Bureau Staff	Student Academic Administration Bureau
Study Program Staff	Study Program
IT Division Staff	IT Division
External Personnel	
Name or Role / Responsibility	**Department / Unit**
Student	Student

Step4 : Identify Areas of Concern

Activities conducted to identify areas of concern are as follows:

1. Conduct a review of each container to see potential areas of concern.
2. Record any areas of concern that have been identified in the Information Asset Risk Worksheet, record the name of information asset and recordthe areas of concern in detail.
3. Expand the area of concern to produce threat scenarios that being detailed explanation from the characteristics of a threat.
4. Record how threats affect the security requirements that set for information assets. Continue to any Information Asset Risk Worksheet until all areas of concern being detail.
5. Continue to any container on Information Asset Risk Environment Maps and record areas of concern as much as possible.

Table 6. Example of Area of Concern - Student Attendance

No	Area of Concern
1	There was an error in the management of student attendance data by Student Academic Administration Bureau staff because of vast amounts of data
2	Study Program staff disseminate AIS-UMHT access authorization that can provide access to student attendance
3	There is a third party that gain access to student attendance when students access the Student-UMHT through public computer
4	Exploiting security holes in Web Server & Database, AIS-UMHT, and Student-UMHT by parties inside or outside

Step5 : Identify Threat Scenarios

In this step, the area of concern extended to a threat scenario that detailing more about the properties of threat. Activities that must be addressed:

1. Completing the Information Asset Risk Worksheets for each identified threat scenarios.
2. Determine the probability into threat scenarios description that has been made on the Information Asset Risk Worksheets.

Table 7. Example of Properties of Threat - Student Attendance

1	***Area of Concern***	***Threat Properties***	
	There was an error in the management of student attendance data by Student Academic Administration Bureau staff because of vast amounts of data	***Actor***	Student Academic Administration Bureau staff
		Means	Staffusing AIS-UMHT
		Motives	Occurs by accidental (human error)
		Outcome	Interruption
		Security Require-ments	Adding validation function on the workpiece by staff, if necessary conduct a training in order to minimize errors
2	***Area of Concern***	***Threat Properties***	
	Study Program staff disseminate AIS-UMHT access authorization that can provide	***Actor***	Study Program staff
		Means	Access to AIS-UMHT
		Motives	The staff deliberately

	access to student attendance		disseminate access authorization to create student attendance vulnerable to modify
		Outcome	Disclosure, Modification
		Security Require-ments	Doing counseling about the importance of maintaining access authorization, and impose sanctions for staff who intentionally disseminate their access authorization
3	***Area of Concern***	***Threat Properties***	
	There is a third party that gain access to student attendance when students access the Student-UMHT through public computer	***Actor***	Not known
		Means	Students forget to log out after using Student-UMHT
		Motives	Third parties want to know the student attendance
		Outcome	Disclosure, Modification
		Security Require-ments	Shorten the login session, enforces password reset within a certain period
4	***Area of Concern***	***Threat Properties***	
	Exploiting security holes in Web Server & Database, AIS-UMHT, and Student-UMHT by parties inside or outside	***Actor***	Not known
		Means	Inside or outside parties identify and exploit vulnerabilities on the server, database, and application modules

		Motives	Inside or outside party wants to modify or damage the server, database, and application modules
		Outcome	Disclosure, Modification, Destruction, Interruption
		Security Require-ments	Enhance the security of hardware, software, and networks, as well as constantly monitor the security loopholes of the system, in order to avoid from parties that intend to infiltrate and destroy the system

Step6 : Identify Risks

In this step determined how threat scenario that has been recorded in Information Asset Risk Worksheet can make an impact to the company. Activities conducted in this step are:

1. Determine how MH. Thamrin University will be affected if the threat scenario really happens, seen from every threat scenario that is recorded on Information Asset Risk Worksheet.
2. Make a record of the consequences of the Information Asset Risk Worksheet, additional point also can be record if it is important. Consequences should be specifically recorded. Consider the impact areas of risk evaluation criteria when considering the consequences.

Step7 : Analyze Risks

In this step begins by reviewing the risk measurement criteria contained in the first step. Focusing on the impact of high, medium, and low for the company. Starting with the first worksheet risk and do a review of the consequences that have been recorded. Furthermore, relative risk score will be calculated and then used to analyze the risks and help the MH. Thamrin University to decide the best strategy for facing the risk.

Step 6 and Step 7 is interconnectedstep, which is considered the consequences that may occur in the area of concern each information asset that has been defined. The consequences have impact area assessed and given a score. Score obtained from multiplication priority with the value of the impact area. How to calculate the score can be seen in Table 8 as follows which could be Low (1), Moderate (2) and High (3).

Table 8. Calculating Score of Impact Area

Impact Areas	**Priority**	**Low (1)**	**Moderate (2)**	**High (3)**
Reputation And Customer Confidence	**5**	**5**	**10**	**15**

Financial	**3**	**3**	**6**	**9**
Productivity	**4**	**4**	**8**	**12**
Safety And Health	**1**	**1**	**2**	**3**
Fines And Penalties	**2**	**2**	**4**	**6**

Step8 : Select Mitigation Approach

In this step any risks that have been identified are sorted based on the value of risk. The risk categories into a particular order can aid decision-making in the status of mitigating such risks. The risks that have been identified are categorized based on the relative risk score that is owned, divided into:

Table 9. Relative Risk Matrix

Relative Risk Matrix		
Risk Score		
30 to 45	16 to 29	0 to 15
POOL 1	POOL 2	POOL 3

From the risk categories that exist, then take steps to mitigate those risks. The division mitigation steps are grouped into:

Table 10. Mitigation Approach

POOL	***Mitigation Approach***
1	Mitigate
2	Defer / Mitigate
3	Accept

Based on the evaluation result of information system risk management in the form of mitigation measures undertaken, are summarized into 12 statements made in the form of a questionnaire, and then distributed to the parties involved in the use of information systems at MH. ThamrinUniversity, to obtain feedback on the implementation of mitigation measures result.

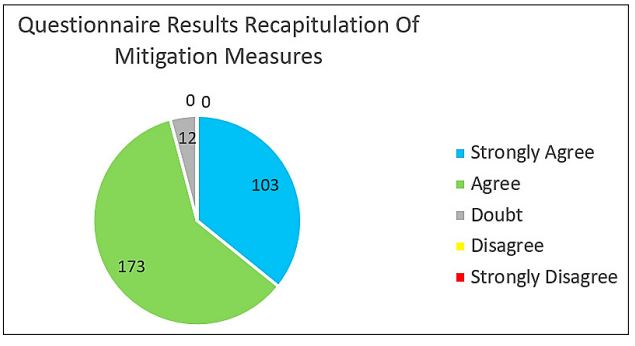

Fig 4. Questionnaire Results Recapitulation.

5. CONCLUSION

1. Using OCTAVE Allegro methods for assessing risks to information systems at Education Institution such as MH. Thamrin University, generating 8 critical information assets with 51 areas of concern, the 34 of them should be mitigated and 17 others can be defer / postponed. Mitigation measures had been determined based on threat scenarios.
2. Mitigation measures that have been determined then summarized into 12 statements in the form of questionnaires, and distributed to the parties involved in the use of information systems to obtain feedback regarding the application of such measures.
3. The results of the questionnaire stated that all parties involved agree and appreciate the mitigation measures resulting from the risk assessment, seen from the no one answer strongly disagree or disagree from 12 statements in the questionnaire, almost all the answers was very amenable and agree, only a few choose doubt.

References

[1] Laudon, Kenneth C., & Laudon, Jane P. (2010). *Management Information System : Managing the Digital Firm*. New Jersey: Prentice-Hall

[2] Suroso, J.S., Rahadi, B.. (2017). *Development of IT Risk Management Framework Using COBIT 4.1, Implementation In IT Governance For Support Business Strategy*. ACM International Conference Proceeding Series. Part F130654, pp. 92-96.

[3] Woody, C. (2006). *Applying OCTAVE: Practitioners Report.* Carnegie Mellon University.

[4] Hartawan, F., Suroso, J.S. (2017). *Information Technology Services Evaluation Based ITIL V3 2011 and COBIT 5 In Center For Data And Information*. Lecture Notes in Computer Science 10192 LNAI, pp. 44-51.

[5] Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *The Information Management Journal*, Vol. August 2005, p60-66.

[6] Van de Haar, H., & Von Solms, R. (2003). *Deriving Information Security Control Profiles for an Organization*. Computers & Security, 22 (3), p233-244.

[7] Woody, C. (2006). Applying OCTAVE: Practitioners Report. Carnegie Mellon University.

[8] Caralli, Richard A. et al. (2007). Introducing OCTAVE Allegro: Improving The Information Security Risk Asessment Process. Software Engineering Institute.