EasyChair Preprint

№ 6219

Information System Risk Management Using Octave Allegro Method

Ngakan Made Bayu Aditya and Susi Febiola

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

August 2, 2021

Information System Risk Management Using Octave Allegro Method

Ngakan Made Bayu Aditya[1], Susi Febiola[2]
Information System, STMIK Borneo International Balikpapan
Jl. AW. Syahranie No.04, RT.32, Batu Ampar, North Balikpapan District, Balikpapan City, East Kalimantan 26136
[1]ngakanmade_bayu.18@stmik-borneo.ac.id, [2]susi_febiola.18@stmik-borneo.ac.id,

Abstract

Awareness of the importance of security of information systems and their assets for an organization and the impact that may arise due to damage to information systems and their assets seems to have not received attention for most organizations. Risk assessment is part of information system risk management, carried out to assess how likely there are threats and vulnerabilities to information systems and their assets. This study aims to conduct a risk analysis on academic information systems in universities. The final result of the risk assessment is in the form of recommendations regarding the steps that must be taken to protect the information system and its assets.

Keywords – Information System, Risk Management, OCTAVE-S

1. PRELIMINARY

Information assets (hardware, software, systems, information and people) are important assets for an organization that need to be protected from security risks both from outside and within the organization. Information security cannot only rely on information security tools or technology, but it is necessary to have an understanding from the organization about what must be protected and determine appropriate solutions that can handle the problems of information security needs. For this reason, a systematic and comprehensive management of information security is needed. Aspects of information security needs must contain 3 important elements, namely:

1. *Confidentiality (confidentiality)* aspects that ensure the confidentiality of data or information, ensure that information can only be accessed by authorized persons and ensure the confidentiality of data sent, received and stored.
2. *Integrity (integrity)* aspects that ensure that the data is not changed without the permission of the authorized party, the accuracy and integrity of the information must be maintained and
3. *Availability (availability)* aspects that ensure that data will be available when needed, ensuring that authorized users can use the information and related tools when needed.

1.1 Information System Risk Security Management Framework

Activity evaluation considers what happens during the evaluation, when an organization conducting an information security risk evaluation, then to carry out the following activities:

a) Identification
   Identifying information security risks (recording risk profiles and organizational information)
b) Analysis
   Analyze risks to evaluate risks and determine priorities

c) Plan

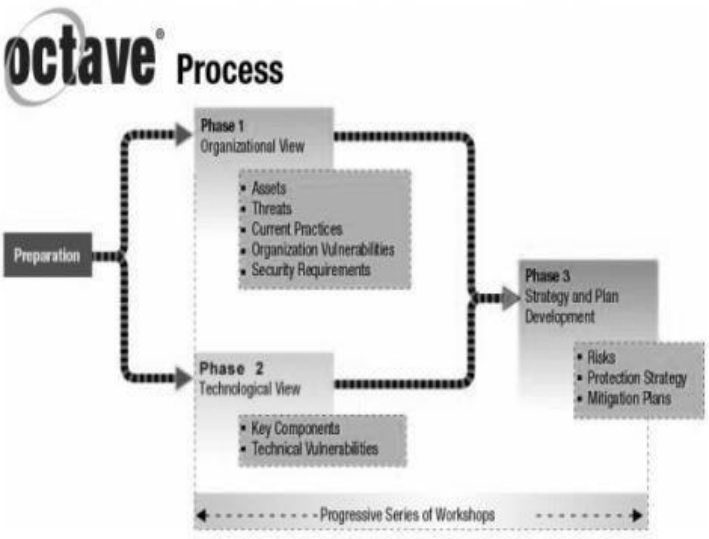
Plans for improved safeguards by developing strategies for organizational improvement and risk mitigation plans to reduce risks for critical organizational assets

d) Evaluation only provides an organizational direction for an information security activity; does not necessarily lead to improvement. After evaluation, the organization should take the following steps:
e) Monitor
   Monitoring progress and effectiveness, this activity includes risk monitoring for any changes.
f) Control
   corrective actions, by analyzing data, making decisions and executing the results of decisions made.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE-S) is a method that can be used to identify threats that may pose an information technology risk. The OCTAVE-S method will assess, analyze and conduct security risk-based strategic planning from various organizational perspectives.

OCTAVE-S

OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a technique or method used to conduct risk-based information security strategic planning and assessment. The OCTAVE framework can be used to identify, analyze and monitor information security risk management processes.



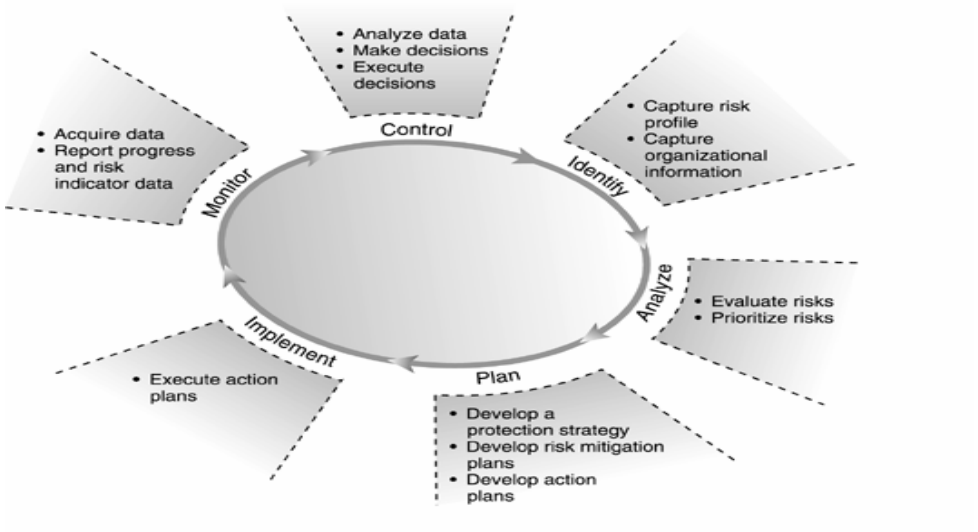
FMEA

Failure Mode and Effect Analysis (FMEA) is a method used to identify and analyze potential errors or failures in a system or process. The process of identifying potential failures is carried out
by assigning a value to each of these failure modes based on the severity of the impact (severity), the level of probability of occurrence (occurence), and the level of detection capability (detection). Furthermore, these three things will be calculated to find the value of the risk priority level (RPN). RPN can be calculated using the following equation:

RPN = Severity x Occurence x Detection

From the results of these calculations, the results will be obtained which are used to determine the level of risk.

This cycle is carried out continuously in connection with the increase and addition of risks that always appear to threaten information security. The General Accounting Office (GAO) makes guidelines in managing risk as shown below:



GAO-based Cycle Framework Drawing, 98

1. RESEARCH METHODS

To manage information security risk is to recognize what risk the organization is implementing it. Once risks are identified, the organization can make plans

overcoming and reducing/mitigating risks for each of the known risks. The OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) method developed by theSoftware Engineering Institute, Carnegie Mellon University, 1999 allows organizations to do the above.

OCTAVE is an approach to comprehensive, systematic, self-directed and self-directed evaluation of information security risk. The approach is structured around a set of criteria that define the essential elements of an information security risk evaluation. The OCTAVE criteria require evaluation to be carried out by an interdisciplinary team consisting of the organization's information technology and business personnel. Team members work together to make risk-based decisions on the organization's critical information assets.

Ultimately, the OCTAVE criteria require a of information to measure organizational practices, analyze threats, and develop protection strategies and these catalogs become a source of knowledge databases. This catalog includes:

- *catalog of practices* – a collection of information security strategies and practices
- *generic threat profile* – a collection of common threat sources
- *catalog of vulnerabilities* – a collection of vulnerabilities by platform and application

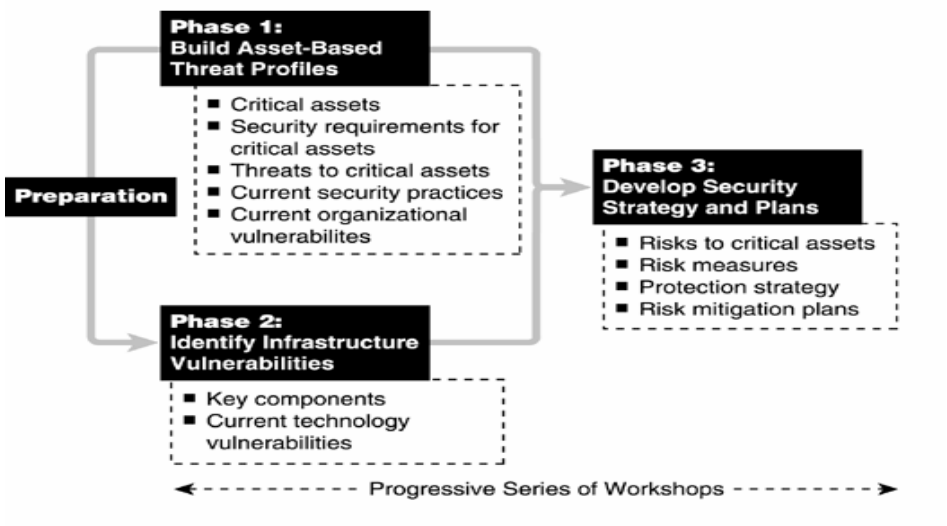


Figure 3 OCTAVE method

Using a three-step approach, the OCTAVE method examines organizational and technology issues against the formulation of comprehensive problems based on an organization's information security needs. The OCTAVE stages are:

a) Preparation phase :

At this stage are preparatory activities that must be carried out before implementing the OCTAVE method, namely:
schedule, form an analysis team, request support and prepare logistics.

b) Stage 1: Building Threat-Based Assets Profile

The outputs in this stage 1 include

i. Assets that are important to the organization
ii. The need for security of important assets is inseparable from 3 aspects of security, namely confidentiality, integrity and availability.
iii. The organization's current security practices or the organization's efforts to protect information assets
iv. Weaknesses of current organizational policies

c) Stage 2: Identify Infrastructure Vulnerabilities

This is the evaluation of computer network infrastructure information. Key operational components of information technology infrastructure (servers, PCs, laptops and network devices) identified weaknesses in terms of technology and configuration, which can make access to security by unauthorized persons easier

d) Stage 3: Develop Security Strategy and Planning

The output of this stage is:

i. Risks to critical assets
ii. Measuring the level of risk
iii. Protection strategy
iv. Risk reduction/mitigation plans

1.1 Analysis and Discussion

1.1.2. Phase I Building Threat-Based Assets Profile

In the OCTAVE method, the sources of threats to information assets are in 4 sources, namely:

i. Deliberate action by people, both from inside (inside) and from outside (outside).

ii. Unintentional actions by humans (Accidental Action by people) both from inside (inside) and from outside (outside).

iii. Problematic systems (systems problems) include defective hardware and software, malicious code (virus worms, trojans, back doors).

iv. Other problems (other problems) such as power outages, threats of natural disasters, environmental threats, telecommunications disturbances.

From the threat of giving the result of influence *(outcomes)* attacks on assets, namely:

- *Disclosure* : can reveal sensitive information informasi
- *Modification* : change of information by unauthorized persons.
- *Destructive and lost* : damage and loss of sensitive information.
- *Interruption* : distraction access to the required information

This can be seen in the image below:

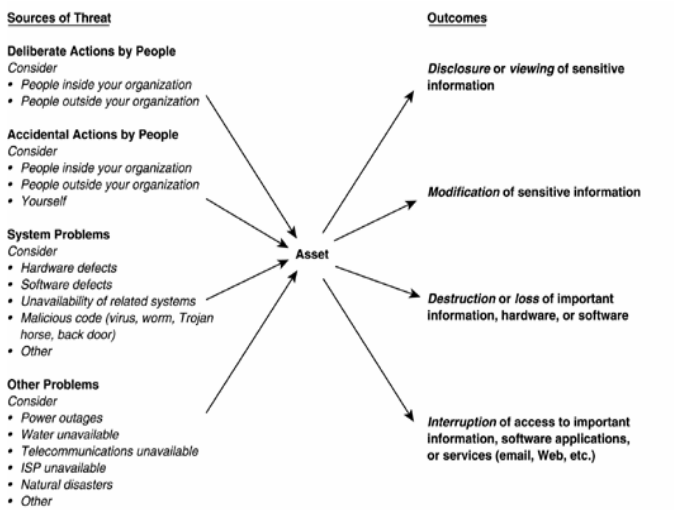


Figure 4 The relationship of threat sources and their effect on assets.

From the above conditions, the OCTAVE method is described in the form of a tree diagram as below to facilitate the mapping of threat sources and their effects.

Where the property of the threat consists of assets, access (how to obtain information), Actor (actor that comes from inside and outside), motive (reason for accessing information intentionally or unintentionally) and outcome (disclosure of information, changes, destruction and disappearance and disruption of access to information.).

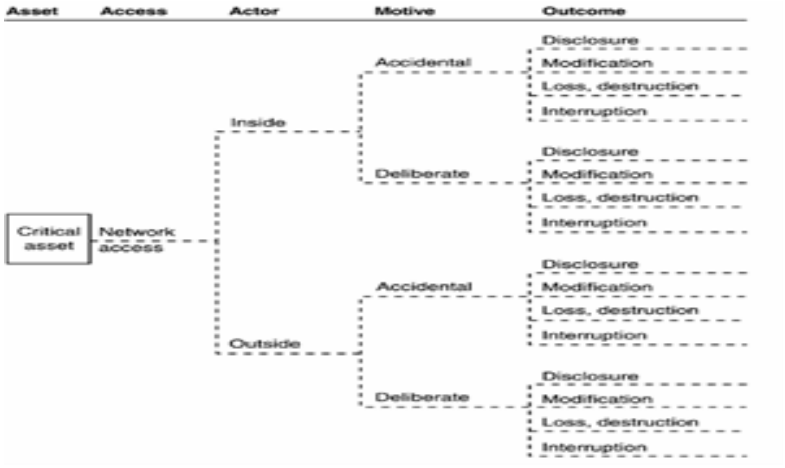


Figure 5 Threat profile tree diagram.

Then next by evaluating catalogs of security practices.

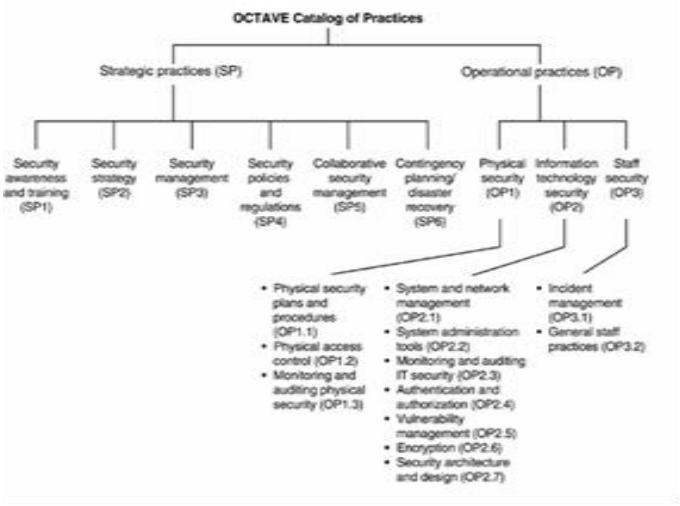


Figure 6 Diagram of the catalog documentation and practices of the OCTAVE method. If there are documents mentioned in the picture above, a compliance test can be carried out. If there is no document, then an effort is made to make a document to facilitate evaluation.

2. RESULTS AND DISCUSSION

The first stage of implementing the risk assessment begins with contacting the management in the IT division, including division heads, systems analysts and programmers to obtain the necessary data. The next stage is to conduct interviews to obtain information about critical operational assets for the organization.

Step 1 - After developing organizational drivers, the most important impact areas are determined and the priority scale values are assigned to the impact areas that have been determined. As a consideration for determining the impact area is the mission and business goals of the organization. The priority impact areas selected first are reputation and customer trust, finance, productivity, safety and health as well as fines and penalties. Table 1 contains the

results of determining the impact area – reputation and customer trust and table 2 is the priority scale of the impact area.

TABLE I. IMPACT AREA REPUTATION AND KTRUSTPCUSTOMER

Impact Area	Low	Medium	High
Reputation	Reputation was slightly affected; no effort or small business needed for repair	Reputation is badly affected, and it takes effort and money to repair	Reputation was affected so badly that it was almost impossible repaired
Customer Loss	Less than 2% customer loss due to loss trust	2% to 10% reduction in lost customers trust	More than 10% customer reduction due to loss trust

TABLE II. SKALA PRIORITY IMPACTAREA

Priority	Impact Areas
5	Customer reputation and trust
4	Financial
3	Productivity
1	Safety and Health
2	Fines and Penalties

Step 2 - In developing the information asset profile, critical information assets must be determined based on the core process of the organization, starting from student data to the final grade report in the form of a transcript. The next activity is to determine the critical information assets that are recorded on the critical asset information worksheet. The selected information asset should consider the following:

-Information assets that are important and used in daily activities.

-Information assets that if lost could interfere with the organization's goals and mission.

From the results of the above considerations, the information categorized as important information assets include student profiles, lecturer profiles, course profiles and student value transactions. Table 3 contains examples of information asset profiling for student value transactions.

TABLE III. IINFORMATION ASSET PROFILLING – TTRANSACTIONNILA MSTUDENT.

Critical Asset	Student value transactions
Rationale for Selection	Used to determine the GPA and determine the quality of students
Description	Consists of student final grades
Owner	Manager

Security Requirements	Confidentiality	Value information is very important fo students, lecturers & majors. Student administration uses the information to print grade transcripts
	Integrity	Information must be true and accurate can be changed and replaced by lecturers, only operators in the student administration section can enter or modify student scores
	Availability	Information must always be available to students, lecturers and the student administration department
Most Important Security Requirements		Integrity Reason: Values are important information for students, if there are errors it will harm students

Step 3 - Identify the information asset container which is divided into three, namely technical, physical and people, each of which has an external and internal side assisted by using the Information Asset Risk Environment Map worksheet. Table 4 contains an example of an Information Asset Risk Environment Map (Technical) – Student Value Transactions.

TABLE IV. IINFORMATION ASSET RUTI ENVIRONMENT (TECHNICAL) – TTRANSACTION NILAMSTUDENT

Student Value Transaction Data	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	Owner(s)
Module: Value Input TransactionInput student value transactions for processing student grades	Student Administration, Department Staff
External	Owner(s)
Container Description	College student
Application: Value Web	
Students can view grades	

Step 4 – Identify areas of concern by reviewing each container to see and determine potential areas of concern followed by documentation of each area of concern that has been identified. Areas of concern are expanded to obtain threat scenarios and then documented to see if they affect security requirements. Table 5 contains examples of areas of concern for student value transactions

TABLE V. AREA OF CONCERN – STUDENT VALUE TRANSACTIONS

No	Area of Concern
1.	A large amount of value data can cause data input errors by student administration staff
2.	Distribution of value transaction password access by section staff administration with access
3.	A security vulnerability in the student grades web application that can exploited by internal /external parties
4.	*Error* what happens during the insert/update /delete transaction module process value done together

Step 5 – Identify threat scenarios that provide a detailed description of the properties of the threat, including actors, means, motives, outcomes and security requirements. Complete Information Asset Risk Worksheets for each common threat scenario. Table 6 is an example of the properties of threat resulting from the expansion of areas of concern for student value transactions.

TABLE VI. PROPERTIES OF THREAT – STUDENT VALUE TRANSACTION

1.	Area of Concern	Threat of Properties	
	The large amount of value data causes an error in inputting value data by the student administration staff	1. Actors	Administrative staff student
		2. Means	Staff use student grade application mo
		3. Motives	*human error (accidental)*
		4.Outcome	*Modification, interruption*
		5. Securiy Requiremen	-alidate the value data input i the field. -ecturer or Departmentverify the value that has been inputted by the staff Student administ ation.
2.	Area of Concern	Threat of Properties	
	Distribution of value transaction password access by student administration staff who have access	1. Actors	Administrative staff
		2. Means	Value app module college student
		3. Motives	Intentionally /unintentionall revealing passwords (deliberate,*accidental*)
		4.Outcome	*Disclosure, Modification, Interruption*
		5. Security Requirements	Provide an understanding to maintain the confidentiality of passwords and penalties.

Step 6 – identification risk aim for determine how the threat scenario has an impact on the organization and determine whether the level is high, medium or low. Followed by calculating the relative score to assist the organization in analyzing risk and determining the right strategy to deal with risk. Table 7 shows how to calculate the relative score.

TABLE VII. CALCULATE THE SCORE IMPACT AREA

Impact areas	Priority	Low (1)	Medium (2)	High (3)
Reputation and trust customer	5	5	10	15
Financial	4	4	8	12

Step 7 - Risk analysis is carried out on each area of concern of the information asset and the consequences that occur based on the relative risk score. Below is an example table of risk analysis - student value transactions.

TABLE VIII. ANALISIS RESICO – TTRANSACTION NILAM STUDENT

Areas of concern	*risk*			
The large amount of value data causes an error in inputtin value data by the student administration st	Conse-quences	Additional time is needed to correct data input errors score		
	Severity	Impact Area	Value	Score
		Reputation an trust customer	Med	10
		Financial	Low	4
		Productivity	High	9
		Security and Health	Low	1
		Fines and Penalties	Low	2
		Relative Risk Score		26

Step 8 – The selection of the mitigation approach is carried out based on the risk grouping. Table 9 shows an example of grouping mitigation measures based on the Relative Risk Matrix, in table 10 is a grouping of mitigation measures, table 11 is an example of risk mitigation based on areas of concern

TABLE IX. RELATIVE RUTIMATRIX

RISK SCORE		
30 TO 45	16 TO 29	0 TO 15
POOL 1	POOL 2	POOL 3

TABLE X. TABLE VIII. MITIGATIONAPPROACH

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABLE XI. TABLE IX. CEXAMPLE MITIGATION RRISK BASED ON AREA OF CONCERN

Risk mitingation	
Area of Concern	The large amount of value data causes value data input error by student administration staff
Action	Mitigate
Container	Control
Value data module college student	Created input validation on certain fiel
Department Staff / Lecturer	Lecturers or department staff can verif the value that has been inputted by the staff student administration

3. CONCLUSION

OCTAVE Allegro is one of the information system risk management methods that can be applied to universities without requiring extensive involvement within the organization and focused on information assets that are critical to the organization's sustainability in achieving its mission and objectives.

Risk assessment can provide an overview of possible threats to critical assets and take appropriate preventive steps to minimize the possibility of these threats occurring. From the results of the risk assessment, policy makers can make strategic plans to properly safeguard critical information assets as well as recovery steps if a threat scenario does occur.

REFERENCE

1. Alberts, Christopher and Dorofee, Audrey, Managing Information Security Risks: The OCTAVESM Approach, 2017.

2. Hughes, G. 2016. Five Steps to IT Risk Management Best Practices. Risk Management, Vol 53, Issue 7. 34

3. G. Blokdijk, C. Engle, J. Brewster. (2008).
IT Risk Management Guide: Management Implementation Guide, Presentations, Blueprints, Templates. AU: Emereo Pty Limited.

4. Prabawati, VA., Rachmadi, A., & Perdanakusuma, A. R. (2018). Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S pada Unit Pengelola Sistem Informasi dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya. Jurnal Pengembangan.

5. Pande Putu Gede Putra Pertama, W. A. (2019). Audit Keamanan Sistem Informasi Perpustakaan STMIK. *Jurnal Sistem Dan Informatika, Vol. 13, No. 2*, 77-86.