Available online at https://journal.rescollacomm.com/index.php/ijeer/index

International Journal of Ethno-Sciences and Education Research

Vol. 3, No. 4, pp. 137-145, 2023

Information Security Risk Management Using OCTAVE Allegro Method at University

Utami Aryanti[1*], Moch. Taufan Anwar[2], Tina Rahmawati[3]

[1,2,3]*Information Systems, Computer Faculty, Masoem University, Bandung, Indonesia*

**Corresponding author email: utamiaryanti@gmail.com*

Abstract

Information is one of the important and valuable assets for the life of an organization's business. Information management is needed to maintain the confidentiality, integrity, and availability of the information from cyber attacks. These cyber attacks can be in the form of viruses, malware, phishing, Distributed Denial-of-service (DoS), fraud, and Ransomware. The education sector is a significant contributor to the increase in cyber attacks during the COVID-19 pandemic. The use of ICT in higher education must have proper information security. This study aims to analyze the risks of information security in higher education. Identification of information security risks necessary for the organization to take appropriate preventive and mitigating actions. OCTAVE Allegro is the framework used to perform risk management in this research. This framework focuses on the information assets owned by the organization. How the asset is used, stored, transferred, occurs and how threats (threats), vulnerabilities (vulnerabilities) and disturbances can be on the asset. The results of this study are recommendations for mitigating approaches for identified risks.

Keywords: Higher Education, Information Security, Information Security Management System (SMPI), Information Security Risk Management (MRKI), OCTAVE Allegro.

1. Introduction

The Government of the Republic of Indonesia is trying to tackle the COVID-19 pandemic by issuing regulations related to the implementation of the PSBB through the Regulation of the Minister of Health of the Republic of Indonesia Number 9 of 2020 concerning Guidelines for Large-Scale Social Restrictions (PSBB) to expedite the handling of the COVID-19 outbreak, several regulations related to the implementation of the PSBB are explained, including regarding the holiday of school activities, namely the teaching and learning process at school is stopped and replaced with a teaching and learning process from home through the most effective media (Rahmatullah & Ghufron, 2021). This pandemic is a challenge for every individual and educational institution to increase creativity in the use of information technology (IT) so that teaching and learning activities can be implemented and continued.

In its implementation, the use of IT increases vulnerability to cyber attacks such as viruses, malware, Phishing, Distributed Denial-of-service (DDoS), Ransomware, and data breaches that can cause losses. According to cybersecurity company Kaspersky in its security report “DDoS during the COVID-19 pandemic: attacks on educational and municipal websites tripled in Q1 2020”, the total number of DDoS attacks increased generally by 80% for Q1 2020 when compared to Q1 2019. Notable growth was seen in attacks on the educational resources and official municipal websites. increased tripled compared to the same period in 2019. The proportion of such attacks reached 19% of the total number of incidents in Q1 2020 (Saleous et al., 2023).

The use of IT in educational institutions must be balanced with the use of appropriate information security. Universities as providers of higher education need to carry out information security risk management to identify important information resources that need to be protected by determining threats and vulnerabilities to assess risks.

A systematic framework is needed as a reference in implementing information security risk management. OCTAVE Allegro is a risk assessment method that focuses on information assets based on three basic principles of security administration, namely: confidentiality, integrity, availability. OCTAVE Allegro has the ability to deliver strong risk assessment results, with a relatively small investment in time and resources, even for organizations that do not have extensive risk management expertise (Gerardo & Fajar, 2022).

Based on the previous explanation, this study will implement the OCTAVE Allegro method to identify and evaluate risks to the confidentiality, integrity, and availability of information assets owned by universities in the use of information technology. The results of this study are recommendations for mitigating approaches to identified risks.

2. Literature Review

An information system can be defined technically as a set of interrelated components who collects (or extracts), processes, stores, and distributes information for facilitating decision-making and control in an organization. With information, data is formed into factors that are meaningful and useful to the organization.

Information security refers to the processes and methodologies designed and implemented to protect electronic information or other forms of confidential personal information and sensitive data from unauthorized access, misuse, disclosure, destruction and modification and disturbances. The main principle of information system security consists of confidentiality, integrity and availability or often abbreviated CIA (Chapple et al., 2018).

Risk is a critical vulnerability that causes differences in the application of information technology. Non-conformity refers to positive or negative events that can affect system performance information and information technology (Standing et al., 2009).

Risk management is a process that enables IT managers to balance operational costs and economic costs for security measures in an effort to protect IT systems and data that supports the mission of the organization (Stoneburner et al., 2002; Peltier, 2005).

3. Materials and Methods

3.1. Materials

3.1.1. Object of Research

Higher education institutions have an obligation known as the Tridharma Higher Education, namely the obligation of higher education institutions to organize education and teaching, research and development, and community service as stated in RI Law Number 12 of 2012 concerning higher education.

To be able to fulfill the Tridharma obligations of higher education during the pandemic, MA'SOEM university carries out teaching and learning activities boldly using electronic learning systems, as well as the use of information systems and information technology to support academic operations and administrative activities related to education and teaching, research and development and service to Public.

At the end of 2020 MA'SOEM College received cyber attacks in the form of DDoS attacks on electronic learning systems, online document storage systems, and malware attacks on several study program websites. The impact of the attack caused learning services to be disrupted, the availability of learning resources and information became inaccessible to lecturers and students.

3.1.2. Data Collection

The data used in this research was obtained based on a case study conducted at Ma'soem university in Bandung, Indonesia. Data collection methods in this study are observation, interviews with all related stack holders, namely Academic Administration Bureau, Finance Bureau, staff in Information Technology Center (ITC), Lecturers, Students, and questionnaires.

3.2. Methods

The method used to assess information security risks in this study is the OCTAVE Allegro method. OCTAVE is a set of tools, techniques and methods for risk-based information system security assessment and planning. The OCTAVE method stands for the Operationally Critical Threat, Asset, and Vulnerability Evaluation which is used to identify and evaluate information system security risks. The OCTAVE method conducts risk assessments based on three basic principles, namely:

a. Confidentiality is the process of securing and ensuring that information can only be accessed by authorized persons. This information is usually related to personal data and is confidential.
b. Integrity, is ensuring that all data is available in one piece and complete.
c. Availability, is trying to make data accessible at any time, without delay, and available intact without defects.

OCTAVE has three variants namely OCTAVE, OCTAVE-S and OCTAVE Allegro. OCTAVE Allegro is a risk assessment method that focuses on information assets. OCTAVE Allegro consists of eight steps that divided into four phases as follows.

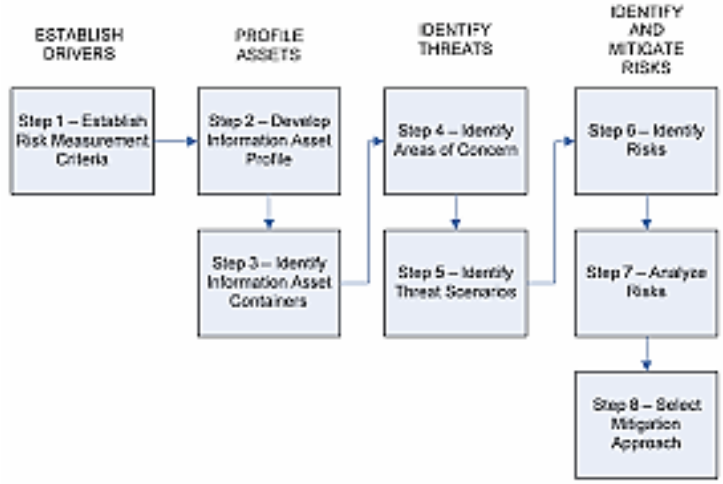

Figure 1: The Steps of Octave Allegro (Caralli et al., 2007:4).

3.2.1. Establish Drivers

The first phase in OCTAVE Allegro is to establish a benchmark that will be used by universities to assess the impact of risks on mission and business goals. This phase consists of one step, namely determining the risk measurement criteria which is a collection of qualitative measures to evaluate the impact of risk and form the basis for assessing information assets. The use of information measurement criteria is used to ensure the way measurement is consistent across various information assets and operating units or departments.

3.2.2. Profile Assets

The second phase is to determine the information asset profile, in which the assets that are the focus of the risk assessment are identified and profiled. In order to develop a profile of information assets, it is necessary to first identify the main set of assets and supporting assets in the tertiary institution. This phase consists of 2 steps, namely:

a. Develop an Information Asset Profile. The risk assessment carried out focuses on the information assets of higher education institutions. In this step, begins with the process of determining information assets. Further identification is carried out regarding the container in which the information asset "lives" and the security of the container to identify all points where the information asset may be vulnerable to disclosure, modification, loss/destruction, or tampering.
b. Identify Information Asset Containers. Places where information assets are stored, transported, or processed can be points of vulnerability and threats that place information assets at risk. Conversely, they can also be places where controls can be put in place to ensure that information assets are protected from damage so that they can be used as intended.

3.2.3. Identify Threats

In this phase threats to information assets are identified and collected through a structured process. This phase consists of 2 steps, namely:

a. Identify Areas of Concern. In Step 4 the process of developing an information asset risk profile begins. Identify possible conditions or situations that could threaten information assets. Based on the critical information asset pool identified previously, areas of concern were captured and used for risk profile development in Step 5.
b. Identify Threat Scenarios. The areas of concern that may affect the information assets identified in Step 4 are expanded into threat scenarios that further detail the nature of the threat. An understanding of the basic components of a threat is needed to expand the area of concern into threat scenarios.

3.2.4. Identify and Mitigate Risk

Risks are identified and analyzed based on threat information, and mitigation strategies are developed to address these risks. This phase consists of 3 steps, namely:

a. Identify Risks. Implement by identifying the threats and impacts received by tertiary institutions as a result of these threats. The risk equation can be illustrated as follows:

Threat (condition) + Impact (consequence) = Risk

[Steps 4 and 5] + [Step 6] = Risk

b. Analyze Risk. In this step, the calculation of the risk score for each information asset is carried out to measure the extent of the threat to tertiary institutions. This assessment is used to determine which risks need immediate mitigation and prioritize preventive actions in the next step.
c. Select Mitigation Approach. To reduce risk, this can be done by prioritizing risks, and determining approaches to mitigate important risks based on a number of factors in tertiary institutions, and developing mitigation strategies taking into account the value of assets and places to live.

4. Results and Discussion

Step 1. Establish Risk Measurement Criteria

In the first step of OCTAVE Allegro interviews were conducted with the Head of ITC, Head of the Academic Bureau, Head of the Finance Bureau, and staff at MA'SOEM University to establish a benchmark that will be used by universities to assess the impact of risks based on mission and business goals of the university. From the results of these interviews, criteria for risk measurement are determined. The criteria for measuring risk at MA'SOEM university can be seen in the following Table 1:

Table 1: Example of Risk Measurement Criteria

Allegro Worksheet 1	**RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE**		
Impact Area	**Low**	**Moderate**	**High**
Staff Reputation	Reputation is minimally distracted, and no charge or effort is required to recover reputation	Reputation is damaged, and charge or effort is required to recover reputation	Reputations are permanently or irreparably damaged
Customer Loss	Reduction in new student admissions less than 1%	reduction in new student admissions between 5% to 10%	reduction in new student admissions more than 50%

Then prioritize the impact areas from the risk measurement criteria table from the most important to the least important, namely sorted by the most significant impact area on the University, the priority impact areas can be seen in the following Table 2:

Table 2: Impact Area Prioritization

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

Step 2. Develop an Information Asset Profile

In order to develop a profile of information assets, it is necessary to first identify the main set of assets and supporting assets in the university. Academic information is the most valuable information asset for universities, where this information asset is most often used in daily work processes and operations. If these information assets are lost, it will significantly impair the university's ability to achieve its goals and contribute to achieving the university's mission. The selected critical information assets will be profiled using Worksheet 8 Octave Allegro as Table 3:

Table 3: Example of Information Asset Profile – Academic Information

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset	**(2) Rationale for Selection**	**(3) Description**
Academic Information	As a guide in managing academic business processes starting from the financial registration of new students to students graduating from college which is the core business of the university	It is a computer-based system connected to the internet that can receive, send, store, process and present data and information related to academic business processes. Academic data/information assets consist of financial data which includes tuition billing data and payment history data, student data which includes personal data, study plans, study results, attendance, transcripts, lecture schedule data including lecture schedules and curriculum
(4) Owner(s)		
Academic Administration Bureau, Bureau of Finance, Information Technology Center (ITC), Lecturers, Students		
(5) Security Requirements		
Confidentiality	Only authorized personnel can view this information asset, as follows:	Access to academic information is restricted based on certain users from the Academic Bureau, Finance Bureau, ITC and the system has been determined
Integrity	Only authorized personnel can modify this information asset, as follows	Only authorized personnel or systems can create new data and or make changes to data, so that the process of collecting, processing and presenting, and using data / information for decision making can be accounted for.
Availability	This asset must be available for these personnel to do their jobs, as follows:	Information must be available according to their respective roles in the Bureau of Academic, Finance, PTI and other users who need information according to their authority.
	This asset must be available for 24 hours, 7 days/week, 52 weeks/year.	Must be available whenever needed, especially during working hours when business processes take place.
(6) Most Important Security Requirement		
Confidentiality	Integrity **Availability**	Other

Step 3. Identify Information Asset Containers

An information asset container is a place where information assets are stored, transported, processed, or where information assets "live". Containers generally include hardware, software, application systems, servers, and networks (technology assets), but can also include items such as file folders (where information is stored). Critical information asset containers are divided into three categories, namely:

a. Technical includes hardware, software or system under the control of the company (internal), and outside the control of the company (external).
b. Physical is the physical location or document that is under the control of the company (internal), and outside the control of the company (external).
c. People are anyone who knows the information under the control of the company (internal), and outside the control of the company (external).

In this study, 20 information asset containers were identified, one of them is in the Table 4:

Table 4: Example of Information Asset Risk Environment Map (Technical)

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**	
	INTERNAL	
	CONTAINER DESCRIPTION	**OWNER(S)**
1.	The academic information system web application is a place for billing data, tuition payments and academic data consisting of database servers and application/web servers.	Academic Bureau, Finance Bureau, ITC
2.	Web-based software for teaching and learning activities with the concept of electronic learning or e-learning, has features for presenting courses.	Academic Bureau, ITC
3.	Server devices where all transactions are processed and stored. College internal network (Cable and Wireless). All system transactions run on this network.	ITC

Step 4. Identify Areas of Concern

Identify Areas of Concern explain detailed descriptions of real-world conditions or situations that may affect information assets in higher education. Based on previously identified critical information asset containers, in this study 23 areas of concern were identified, Table 5 is some of the areas of concern identified.

Table 5: Area of Concern

No. Area of Concern (AC)	**Area of Concern**
1	There is a bug in the academic information system web application so that data can be accessed and or changed by unauthorized parties. Besides that, bugs can also cause disruption of academic services or business processes.
2	The academic information system web application server and e-learning software are down so that services cannot be accessed or disrupted.
3	Denial-of-service (DoS) attacks against elearning software by hackers that can render elearning services unusable

Step 5. Identify Threat Scenarios

To complete this step, use the Information Asset Environment Map created in Step 3 (Worksheet 9a) as a guide. Continue by completing the Threat Scenario Questionnaire 1 – Technical Container based on the technical container that has been included in Worksheet 9a, Answer the questions. Circle the appropriate answer as the Table 6.

Table 6: Example of Threat Scenarios Questionnaire 1

Threat Scenario Questionnaire 1	**Technical Containers**		
Scenario: There is a bug in the academic information system web application so that data can be accessed and or changed by unauthorized parties. Besides that, bugs can also cause disruption of academic services or business processes, which cause assets to:			
Disclosed to unauthorized individuals?	No	Yes (accidentally)	Yes (intentionally)
Modified so that it is not usable for intended purposes?	No	Yes (accidentally)	Yes (intentionally)
Interrupted so that it cannot be accessed for intended purposes?	No	Yes (accidentally)	Yes (intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	Yes (accidentally)	Yes (intentionally)

Furthermore, an Information Asset Risk Worksheet is created for each identified common threat scenario to consider each threat scenario created.

Table 7: Information Asset Risk Worksheet

	Allegro Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**
	Information Asset	Academic Information
	Area of Concern	There is a bug in the academic information system web application so that data can be accessed and or changed by unauthorized parties. Besides that, bugs can also cause disruption of academic services or business processes.
Threat	Actor	Hacker
	Means	Using the Scanning toolkit, then perform an injection attack
	Motive	Economy, Entertainment
	Outcome	Disclosure Modification Destruction Interruption
	Security Requirements	Applications are supposed to be protected from injection .

Step 6. Identify Risk

In this step, identification of the impact received by the university is based on the threat scenario that was created in the previous step. Determine the impact and consequences received by university for each threat scenario that has been documented on the information asset risk worksheet. The following are some of the consequences that can occur as Table 8:

Table 8: Identify Risk

No	**Threat Scenario**	**Consequence**
1.	There is a bug in the academic information system web application so that data can be accessed and or changed by unauthorized parties. Besides that, bugs can also cause disruption of academic services or business processes.	Operations of academic and/or e-learning services are disrupted or even stopped. Bugs in a website application can be a door for hacking other systems which can cause financial losses and a decline in the university's reputation.
2.	The academic information system web application server and e-learning software are down so that services cannot be accessed or disrupted.	The teaching and learning process will be disrupted. The addition of working hours for ICT employees can increase depending on the damage experienced by the server.
3.	Denial-of-service (DoS) attacks against elearning software by hackers that can render elearning services unusable	E-learning services are paralyzed which causes a decrease in productivity and a decline in the reputation of universities.

Step 7. Analyze Risk

Referring to the risk measurement criteria created in Step 1, classify the consequences of each threat on universities according to the criteria of low, moderate, and high.

Next, a relative risk score will be calculated which can be used to analyze risk and help universities determine the right risk strategy. The relative risk score calculation refers to the Impact value. The impact value is derived from the risk measurement criteria. Impact Area Value Low = 1, moderate = 2, High = 3. Relative risk scores will be calculated and used to analyze risk and help organizations to determine the right risk strategy, here are some of the results of risk analysis in this study as Table 9:

Table 9: Analyze Risk

Area of Concern	Consequence	Impact Area	Ranking	Impact Value	Score
AC.1	1	Reputation	4	Moderate (2)	8
		Financial	3	Low (1)	3
		Productivity	5	Moderate (2)	10
		Legal Penalties	1	Low (1)	1
		User Defined	2	Low (1)	2
				Total Score	24
Area of Concern	**Consequence**	**Impact Area**	**Ranking**	**Impact Value**	**Score**
AC.2	2	Reputation	4	High (3)	12
		Financial	3	Low (1)	3
		Productivity	5	High (3)	15
		Legal Penalties	1	Low (1)	1
		User Defined	2	Moderat (2)	4
				Total Score	35
Area of Concern	**Consequence**	**Impact Area**	**Ranking**	**Impact Value**	**Score**
AC.3	3	Reputation	4	Moderat (2)	8
		Financial	3	Low (1)	3
		Productivity	5	High (3)	15
		Legal Penalties	1	Low (1)	1
		User Defined	2	Moderat (2)	4
				Total Score	31

Step 8. Select Mitigation Approch

In this step considerations are made to accept risks, reduce them, or postpone them based on a number of important factors related to conditions at the university. The first activity is sorting each identified risk based on its risk score. Categorizing risks based on relative risk score can assist in making decisions about their mitigation status. Categorizing relative risk score divided into as Table 10:

Table 10: Relative Risk Matrix

RELATIVE RISK MATRIX			
	RISK SCORE		
RELATIVE SCORE	30 to 45	16 to 39	0 to 15
POOL	POOL 1	POOL 2	POOL 3
MITIGATION APPROACH	Mitigation	Mitigation or Deffer	Accept

As the final result of calculating the risk assessment, the results of determining mitigation can be seen in the following Table 11:

Table 11: Mitigation Approach

Area of Concern	Relative Risk Score	Pool	Mittigation Approach
AC.1	24	POOL 2	Mitigation or Deffer
AC.2	35	POOL 1	Mitigation
AC.3	31	POOL 1	Mitigation

Mitigation measures on asset containers with certain controls as a solution to risk. Risk mitigation carried out can consist of administrative, technical and physical controls.

5. Conclussion

Based on the research that has been implemented by conducting a risk assessment analysis in accordance with the steps in OCTAVE Allegro, 23 risk scenarios (areas of concern) are produced from 1 critical asset, namely academic data/information managed by ITC. The results of the risk analysis are in the form of a risk score relative to the impact area and the impact value. The results of the risk assessment of academic data/information management at ITC were the highest risk in the data updating process, with four high risk categories (relative risk score: 41, 34.39, 41) and five medium risk categories (relative risk score: 36, 30, 35, 32, 30).

References

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.

Gerardo, V., & Fajar, A. N. (2022). Academic IS Risk Management using OCTAVE Allegro in Educational Institution. *Journal of Information Systems and Informatics*, *4*(3), 687-708.

Peltier, T. R. (2005). *Information security risk analysis*. CRC press.

Rahmatullah, A. S., & Ghufron, S. (2021). The Effectiveness Of'facebook'as Indonesian Language Learning Media For Elementary School Student: Distance Learning Solutions In The Era Of The Covid-19 Pandemic. *Multicultural education*, *7*(04), 27-37.

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, *9*(1), 211-222.

Standing, C., Sims, I., & Love, P. (2009). IT non-conformity in institutional environments: E-marketplace adoption in the government sector. *Information & Management*, *46*(2), 138-149.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30.