Analysis of Risk Management on Learning Management System using Octave Allegro Framework

Tristania Setianingrum Dandhung Putri
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
E-Learning or Learning Management System is an electronic-based system that helps facilitate the implementation of learning on educational institutions. The system provides convenience on the teaching and learning process between teachers and students or students and lecturers. This system utilizes technological advances which on its application can pose both negative and positive risks. On this study, the author uses the Octave Allegro framework. This framework aims to analyze the risks that occur to the institution or organization on order to choose actions to prevent these risks. The final result expected from this research is the threat that is the maonpriority and the appropriate mitigation approach to be applied so that the organization or institution can help prevent risks that may arise. The Octave Allegro methodology used on this study can explaonhow to identify the level of risk so that the organization or institution is ready to take action. The risk assessment carried out on this study relates to the risk of mitigation measures to reduce the risk of threats to information assets.

Keywords
Octave Allegro, Risk management, Learning Management System, Risk Analysis

1. INTRODUCTION
Advances on information technology are now widely used by educational institutions. One of the information technologies used is the Learning Management System (LMS) or e-learning to support the further learning process and use it for additional insights.[1] As an academic community, universities also use this information technology. On addition to providing convenience, it also certainly has a negative and positive impact, there are risks faced on its implementation. Seeing the possibility of risks that occur on the Learning Management System (LMS), it is necessary to take regular management and supervision actions and risk management is needed. On this study, the Octave Allegro method was chosen to identify and define risks that may occur on the Learning Management System (LMS) and the handling of these risks.

2. LITERATURE STUDY

2.1 Definition of Information System
The Octave Allegro method can impact the system area with the results of the mitigation approach for lecturer data, student data, assignments are on pool 1 which is mitigated, while quiz activities are on pool 2.[2] On addition, it can also show many weaknesses on terms of good and accurate security of the information system and followed by good habits on using resources at the institution.[3] The risk assessment provides an illustration of the potential threats to critical information assets and allows for appropriate countermeasures to minimize the likelihood of such occurring threats.[4] With the risk assessment, it is hoped that related parties can carry out maintenance to avoid desirable things.[5]From the results of the risk management analysis carried out, it is possible to identify areas of concern regarding changes on e-learning features to access lecture materials, assignments, and quizzes and find out the results of the number of e-learning accesses carried out by students and lecturers.[6]

2.2. Risk Management Concept

2.2.1. Definition of Management
Management is the achievement of organizational goals on an effective and efficient way by planning, organizing, directing, and managing organizational resources.[7] Management can also be interpreted as a science to regulate the process of utilizing human resources and other resources effectively and efficiently to achieve certaongoals.[8] On addition, management is also a process or framework that involves the guidance and direction of a group of people towards the goals.[9]

2.2.2. Definition of Risk
Risk is uncertainty that allows for losses.[10] Risk can also be defined as risk can be defined as Outcame Volatility, generally on the form of asset or debt value.[11] Risk is the possibility of deviations from expectations that can cause losses.[12]

2.2.3. Definition of Risk Management
Risk management is an effort aimed at reducing the possibility of loss from the risks faced. Avoiding risk alone is not enough, it must be managed on a way to minimize the possibility of loss.[13]

2.2.4. Definition of Risk Identification

Risk identification is an activity to collect all information related to business activities.[14] This is done to identify all risks faced by business stakeholders. Business people are faced with many risks, ranging from small risks such as employee negligence to large and widespread risks.[15]

2.2.5. Risk Assessment
Risk assessment is a systematic method of looking at work activities, thinking about what could go wrong, and determining appropriate controls to prevent loss, damage or injury during work. This assessment should also include the controls needed to eliminate, reduce or minimize risks.

2.2.6. Risk Management
There are 11 principles of effective risk management, namely: 1. creating and protecting the values stated on the organization's objectives; 2. an integral part of all processes withonthe organization and is the responsibility of

management; 3. part of decision making; 4. explicitly take into account uncertainty; 5. must be built through a systematic, structured, and timely approach; 6. requires the availability of adequate information; 7. requires customization; 8. must take into account human and cultural factors; 9. must be transparent and comprehensive; 10. must be dynamic, iterative, and responsive to change; 11. Can facilitate sustainable organizational development.[16]

2.2.7.Risk Management Cycle

Figure 1.Risk Management Cycle

The management cycle can visibleon Figure 1. The first step must be to identify risks, then study the characteristics of these risks and conduct evaluations. The next step is to prioritize risk. The next step is to manage risk. And the last step is revisit.[17]

2.3. Information Technology Concept

2.3.1. Definition of Information Technology

Information technology is a science that includes computer systems hardware and software, LAN (local area network), MAN (metropolitan area network), WAN (wide area network), management information systems (SIM), telecommunications systems and others.[18]

2.4. Information System Security

Information system security is an effort to protect information assets from potential threats that may arise. Information security has three aspects, namely Confidentiality (confidentiality), Integrity (integrity), and Availability (availability) commonly abbreviated as CIA Triad based on Figure 2.[19]

Figure 2. Information Security Aspect

2.5. Learning Management System (LMS)

2.5.1.Definition of Learning Management System (LMS)

Learning Management System (LMS) or commonly known as e-learning, E-learning is an educational system that uses electronic applications to support teaching and learning via the internet, computer networks, or standalone computers. The description above can be defined as e-learning as a technology that bridges teaching and learning activities between students and teachers.[20]

2.5.2. E-Learning Characteristics

The characteristics of e-learning include using electronic technology such as computers teaching and learning activities between students and teachers.[20] teaching materials are independent, can be viewed at any time, and are made by a professional team.[21]

2.5.3. E-Learning on Education

Learning technology on this field is called e-learning. With this technology, teachers teach at a computer on one location and students simultaneously follow lessons from a computer on another location. This technology is efficient and supports the teaching and learning process.

2.5.4. Elements of E-Learning

The elements possessed by e-learning are questions, community, multimedia, online teaching, and collaboration opportunities.

2.5.5. Advantages and Disadvantages ofE-Learning

The advantages are personal learning experience and easy access. Weaknesses are the lack of interaction between teachers and students, tend towards training, and not all locations have internet facilities.

2.5.5. Learning Management System (LMS) features

Some of the features it has are learning management, student activity reports and grades, communication media, assignment collection facilities, and material storage.

2.6. Risk Management Method

2.6.1.Octave Allegro Method

Octave Allegro differs slightly from other Octave approaches on that this framework describes how information assets are owned by an organization, agency or company on the context of how they are used, where they are stored, transmitted, and processed, and how the threats, vulnerabilities, and asset disruption occurs.[22] This method consists of 8 steps, namely establishing criteria for measuring risk, creating an information asset profile, identifying information asset containers, identifying problem areas to be considered, identifying threat scenarios, risk identification, risk analysis, and choosing an approach as shown on Figure 3.

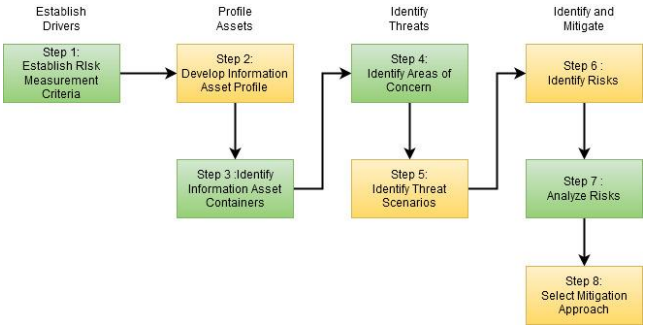

Figure3.Step of Octave Allegro Method

3. METHODOLOGY

This study uses several data collection techniques as follows:

3.1. Observation

The author conducts observations by observing and recording the use of Learning Management System (LMS).

3.2. Study of Literature

This is done by searching, reading, and collecting references that are relevant to the research topic using reference sources from books, articles, journals, and several final assignments.

3.3. Interview

Data collection is done through face-to-face and direct question and answer.

3.4. Questionnaire

Data collection techniques through a list of questions distributed to respondents.

4. RESULT AND CONCLUSION

4.1. Step 1 – Establishing Risk Measurement Criteria

The results on Table 1 show that the impact areas affected are reputation and trust, operational or financial costs, and productivity. Meanwhile, security and health as well as fines and legal sanctions are not affected.

Table 1Impact Area Prioritization

Allegro Worksheet 7	Priority Score Worksheet Impact Area
Priority Score	***Impact Areas***
4	Reputation and Trust
3	Financial
5	Productivity
2	Safety and Health
1	Fines and penalties

4.2. Step 2 – Information Asset Profile Identification

The second step on the Octave Allegro method is to develop an information asset profile. At this stage, the development of information assets is carried out. Information assets contained on the system are identified to identify vulnerabilities that may exist on Learning Management System (LMS) information assets.The results of the identification and profiling process of critical information systems on Table 2 show that the most important security requirement from the Learning Management System (LMS) is integrity.

Table 2.Critical Information Asset Profile

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset What is information asset aset critical?	**(2) Rationale for Selection** Why areassets information important in organizations?	**(3) Description** What is the description of theasset information that?
Learning Management System service information data which includes (lecturer data, student data, learning data, etc.)	Learning Management System information data is important because the data includes lecturer and student data which includes lecturer and student numbers. Therefore, if the data is lost or damaged will interfere with the LMS.	Learning Management System service information data is structured data that covers all activities on the LMS.
(4) Owner (s) Who owns the assets that information?		
Organization		
(5) Security Requirements What are the security requirements for information assets?		
Confidentiality	Maintain the confidentiality of data access rights from unauthorized parties and maintaon the confidentiality of data information. Only registered users can access the entire data.	
Integrity	Maintain data so that it remains integrated so that it does not change or modify data from any parties, except for getting instructions to make changes from the person concerned if there is a problem.	
Availability	Data is always ready to be accessed anytime and anywhere.	
(6) Most Important Security Requirement What are the most important security requirements for the information asset?		
Confidentiality	✓Integrity	Availability

4.3.Step 3 – Containers of Information Assets Identification

The third stage is identifying the containers of information assets. At this stage the information asset containers where the assets are stored, transported, or processed are identified to find out where there are possible risks that can occur. Information asset containers consist of three parts, namely technical containers, physicalcontainers, and people containers, each of which includes external and internal sides. From the results of the interview, it was found that the technical aspect of the container system focuses on the server network managed by organization as an internal party. On the physical container aspect, information assets do not focus on physical assets on the form of stored documents.

4.4.Step 4 – Areas of Concern Identification

On step 4, the identification of areas of concern, namely Technical (TC), Physical (PhC), and People (PC). Table 3 is a table list of identified areas of concern.

Table 3.Area of concern

No	Area of concern	Code	Security Requirments
Technical Container			
1	Learning Management System discontinuation due to Internet connectivity interruption	TC-1	1) Avaibility
2	Learning Management System interruption due to system device being updated/repaired	TC-2	1) Avaibility
3	Learning Management System disruption due to server down	TC-3	1) Avaibility
4	There are loopholes on system security that can be accessed by unauthorized parties	TC-4	1) Confidentiality 2) Integrity
5	Service interruption due to a crash on the service system or operating system.	TC-5	1) Avaibility
Physical Container			
6	The occurrence of natural disasters or environmental threats causes services to stop	PhC-1	1) Avaibility
People Containers			
7	Error inputting data by the employee or administrator	PC-1	1) Confidentiality 2) Integrity 3) Avaibility
8	Distributed access rights (username and password) administrator as a result of the occurrence of social engineering	PC-2	1) Integrity

Based on the results on the table above, there are 6 risks of disruption to the technical containers aspect, 1 risk of disruption to the physical containers aspect, and 4 disruption risks to the people containers aspect.

4.5.Step 5 –Threat Scenarios Identification

On this step, identification of areas of concern is carried out to complete the areas of concern obtained from the previous step by using a questionnaire to determine the effect of risk. The results of the questionnaire on the technical containers section, scenario 1 shows that there is a possible threat from organization. Scenario 2 shows that there is a possibility of threats that are carried out accidentally from outside (external) parties. Scenario 3 shows that there are several situations that allow problems such as damage to the system and hardware, the presence of viruses, disruption of the power supply, network problems, and disasters. On the physical containers section, scenario 1 indicates that there is a possibility of a threat to be revealed and modifications to information assets occur so that it is possible for damage to occur. Scenario 2 shows that a disaster, whether caused by nature or by humans, can cause disturbance or loss. On the people containers scenario 1, it shows that there is a possible threat frominternal organization parties regarding the disclosure of information assets and the possibility of modifications resulting on damage to information assets. While scenario 2 shows that there is a possibility of threats from outside the agency (external) that can modify or disclose information to unauthorized parties causing damage.

4.6. Step 6 – Risk Identification

On this step, it starts by calculating the number of impact area scores by looking back at the risk management criteria that have been obtained on Step 1 as shown on Table 4. The way to calculate the score for each impact area is as follows:

1. If the value or value on the impact area is low, then the value of the value of priority is multiplied by the number 1.
2. If the value or value on the impact area is of medium value, then the value of the value of priority is multiplied by number 2.
3. If the value or value on the impact area is high, then the value of the value of priority is multiplied by the number 3.

Table 4. Score Impact Area

Impact Areas	Value Of Priority	Impact Score		
		Low (1)	Medium (2)	High (3)
Productivity	5	5	10	15
Reputation and Trust	4	4	8	12
Financial	3	3	6	9
Safety and Health	2	2	4	6
Fines and Penalties	1	1	2	3

4.7. Step7 – Risk Analysis

This On this 7th step, a risk analysis will be carried out on all areas of concern, after which it determines all the criteria for low, medium, and high. TC-1 shows that the occurrence of interference with internet connectivity on the LMS (Learning Management System) service is of low value. TC-2 indicates that the LMS (Learning Management System) service is interrupted because the system equipment being updated or repaired is at a low value. TC-3 shows that the LMS (Learning Management System) service is interrupted because the server is down at a medium value. TC-4 indicates that there is a gap on system security that can be accessed by unauthorized parties at medium value. TC-5 indicates that the LMS (Learning Management System) service has stopped due to a crash on the service or the operating system is at medium value. PhC-1 shows that the cessation of LMS (Learning

Management System) services due to a disaster is at a high value. PC-1 shows that the occurrence of data input errors by the employee or administrator is at a medium value. PC-2 shows that the distribution of access rights (username and password) of administrators as aresult of the occurrence of social engineering is of medium value.

4.8. Step 8 – Choosing Mitigation Approach

On the 8th step, a mitigation selection will be carried out, carrying out an elaboration of the risk profile described on the 7th Step. TC-1 shows that the occurrence of interference with internet connectivity on the LMS (Learning Management System) service is of low value and the action that needs to be taken is accept. TC-2 shows that the LMS (Learning Management System) service is interrupted because the system device is being updated or updated is at a low value and the action that needs to be taken is accept. TC-3 shows that the LMS (Learning Management System) service is interrupted because the server is down at a medium value and the action that needs to be taken is defer (delay) for some time and will perform the scheduled system when the server is down.TC-4 shows that there is a gap on system security that can be accessed by unauthorized parties at a medium value and theaction that needs to be taken is mitigate or defercan be done with the need for education and socialization regarding the importanceof maintaining confidentiality, maintaining data.confidentiality of access rights and maintaining integrity personal data and system .TC-5 shows that the cessation of the LMS (Learning Management System) service due to a crash on the service system or operating system is at a medium value and the approach that needs to be taken is mitigate or defer. PhC-1 shows that the cessation of LMS (Learning Management System) services due to a disaster is at a high value and the approach that needs to be taken is to mitigate or defer. The suggested approach of the actions that need to be taken is mitigate to take a decision on this mitigation approach depending on the condition of the problem that occurs and review the impact of the risk by maintaining a backup of system service data. PC-1 shows that the occurrence of data input errors by the employee or administrator is at a medium value and the approach that needs to be taken is mitigate or defer. The recommended approach for the actions that need to be taken is to mitigate, namely by re-checking the population data before submitting it to the system. PC-2 shows that the distribution of administrator access rights (username and password) as a result of social engineering is of medium value and the approach that needs to be taken is to mitigate or defer. The suggested approach of the action that needs to be taken is to mitigate, namely by providing regular briefing and socialization related to the importance of maintaining the confidentiality of access rights and integrity of system services. Then after compiling the risk based on the total risk score, the next step is to group the number of threats on Table 5.

Table 5. Grouping Number of Threats

Mitigation Approach	Technical Container (TC)	Physical Container (PhC)	People Container (PC)
Mitigate	1	1	2
Defer	2	0	0
Accept	2	0	0
Total	**5**	**1**	**2**

5. CONCLUSION

The results of the tests carried out on the LMS (Learning Management System) service at organization, obtained the mitigated approach amounted to 4, defer amounted to 2, and accept amounted to 2. The relatively high risk value is on Physical Container (PhC) with a total risk value of 29, namely due to a natural disaster that caused the LMS (Learning Management System) service to stop. A relatively low risk value is found on Technical Container (TC) with a total risk value of 15, namely due to internet connectivity disruptions so that the Learning Management System service is interrupted or temporarily stopped.Further research is suggested to be able to carry out risk management analysis by referring to this research data using other methods or frameworks that have the same function and purpose so that risk management in the Learning Management System (LMS) service system is more accurate.

6. REFERENCES

[1] Virtanen, M. A. (2018).The development of ubiquitous 360 learning environment and its effects on students' satisfaction and histotechnological knowledge. Graduate School University of Oulu

[2] Dewi, N. A. N., &Yudana, I. G. P. H. 2016. Analysis of Risk Management on Academic Systems at STMIK STIKOM Bali. National Seminar on Information Technology and Multimedia, (pp. 7–12). Yogyakarta: STMIK AMIKOM.

[3] Saragih, S.P. 2018. Implementation of Octave-S on Evaluation of Information System Risk Management at Batam Health Training Center. Scientific Journal of Informatics (JIF), (pp. 18-19).

[4] Ikhsan, H., &Jarti, N. 2018. Analysis of Information Technology Security Risks Using Octave Allegro. Responsive Journal, (pp. 32-33). Batam: STT IbnSina.

[5] Setyawan, A.A., &Wijaya, A.F. 2018. Analysis of Technology Risk Management at DISKOMINFO Salatiga City Using the Octave-S Method.National Seminar on Indonesian Information Systems.

[6] Catherine, Angela, Sylvia, C. 2019. Analysis of Electronic-Based Learning System Risk Management at XYZ College. National Seminar on Information and Communication Technology 2019 (SENTIKA 2019) ISSN: 2089-9815.

[7] Taufiq, R. 2013. Management Information Systems Basic Concepts, Analysis and Development Methods. Yogyakarta: Graha Ilmu.

[8] Taufiq, R. 2013. Management Information Systems Basic Concepts, Analysis and Development Methods. Yogyakarta: Graha Ilmu.

[9] Taufiq, R. 2013. Management Information Systems Basic Concepts, Analysis and Development Methods. Yogyakarta: Graha Ilmu.

[10] M. Hanafi 2012. Risk Management. UPP STIM YKPN, Yogyakarta. Book

[11] MamduhM.Hanafi (2012) Risk Management (second edition). Yogyakarta: UPP STIM YKPN

[12] M. Hanafi 2012. Risk Management. UPP STIM YKPN, Yogyakarta. Book

[13] MamduhM.Hanafi (2012) Risk Management (second edition). Yogyakarta: UPP STIM YKPN

[14] Kasidi 2010, title of risk management book. Bogor : Ghalia Indonesia

[15] Kasidi 2010, title of risk management book. Bogor : Ghalia Indonesia

[16] ISO 31000. (2009). ISO 3100 Risk Management. Australia: International Organization for Standardization.

[17] MamduhM.Hanafi (2012) Risk Management (second edition). Yogyakarta: UPP STIM YKPN

[18] Prasojo, L.D. and Riyanto. 2011. Educational Information Technology. Yogyakarta :Gava Media.

[19] Sarno, R and Iffano. I. 2009. Information Security Management System. Surabaya: Itspress.

[20] Sarno, R and Iffano. I. 2009. Information Security Management System. Surabaya: Itspress.

[21] Prasojo, L.D. and Riyanto. 2011. Educational Information Technology. Yogyakarta :Gava Media.

[22] Mulyawan, S. 2015. Risk Management. Bandung: Faithful Library.

[23] Saragih, S.P. 2018. Implementation of Octave-S on Evaluation of Information System Risk Management at Batam Health Training Center. Scientific Journal of Informatics (JIF), (pp. 18-19).

[24] Arum, Kalkim. 2018. Analysis of Risk Assessment Using Octave Allegro Framework Case Study of Library Management Information System of SMA Muhammadiyah 1 Yogyakarta. Thesis, Information Systems, Ahmad Dahlan University Yogyakarta.

[25] Mackay, M., &Tymon, A. 2014. Taking a risk to develop reflective skills on business practitioners. Journal of Education and Work, (pp. 1–20).