Journal of Theoretical and Applied Information Technology
31st October 2022. Vol.100. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INFORMATION SYSTEM RISK MANAGAMENT WITH OCTAVE ALEGRO AT ED-TECH COMPANY (PT RAKAMIN KOLEKTIF MADANI CASE STUDY)

[1] INTAN BEREANI WIGUNA, [2]JAROT S. SUROSO, [3]SANDY ANUGERAH
Information Systems Mangament Department
BINUS Graduate Program Master of Information Systems Management
Bina Nusantara University, Jakarta, Indonesia.
[1]intan.wiguna@binus.ac.id, [2]jsembodo@binus.edu, [3]sandy.anugerah@binus.ac.id

ABSTRACT

Today, various areas of business depend on information systems. The more sophisticated the technology, the more diverse the data collected to help business processes. However, as technology develops, there are also information system security risks that must be a concern. Therefore, various areas of the company need to mitigate to overcome possible security problems that arise. One of the fields of business that currently uses information systems to assist its business processes is education. Many education technology companies create educational platforms in their business processes. As the number of students increases, there needs to be a qualified risk assessment. One of the common methods is using OCTAVE Allegro is a method that helps organizations to detect risks and make decisions.

Keywords: *OCTAVE Allegro, Risk Assessment, Information Security, Risk*

1. INTRODUCTION

As technology develops, the types of jobs available will be more complex and competitive, especially in the digital and technology fields. For enterprises, it is critical to master digital transformation to drive innovation. Robotic technology, artificial intelligence, Big Data, infrastructure, and security are the key technologies for digital transformation. Companies must have the ability to carry out this digital and technological transformation in order to survive in the future [1]. Recognizing this, it is important for companies to have the best resources who understand digital and technology. The need for experts in this field is also increasing. Many fresh graduates or experienced workers want to increase their skills in technology and digital through free or paid courses.

Rakamin academy, is a company in Indonesia that provides courses in technology and digital. This company offers in-depth training on digital marketing techniques, data science, and UI/UX design by bringing in tutors who are proven in this field. The training was carried out for 3 months with the number of students in each batch ranging from 30-50 people. Currently, teaching and learning activities at Rakamin Academy have reached the 15th batch with more than 1,000 students. This number will continue to grow every month in accordance with the target of Rakamin Academy which wants to become the leading Ed-tech in Indonesia.

Applications of technology for the educational process (Ed-Tech) are technological devices used in the education sector to assist the educational process [2]. Towards an ed-tech based company, Rakamin Academy tries to innovate by creating an education platform for students. Education platforms can help ed-tech companies to develop businesses and summarize user data to become a valuable commodity [3]. The education platform created by Rakamin Academy is in the form of software used by teachers and students to connect with each other and carry out the teaching and learning process. The use of this platform is not only for managing online learning, but students can continue to use this platform to consult careers or get the latest job information throughout their careers.

Table 1 Information system development History

Date	Information System Development
April 2020	Using 3rd party for the learning system. Namely Google Classroom
April 2021	Started to use independent learning management system for learning process
July 2021	Matured learning management system which have after sales purpose to track student careers and solved their problem to have new job.

The table above showed the system development history of this company. With the new system, the companies started to collect students' data to maximize their information system usability.

However, in data collection it is necessary to have a great responsibility to protect the data, include customer or companies' data. Mayer stated that in this network world, every organization required to implement information security and risk management if they want to survive [4].

Not many online learning companies have carried out risk assessments on the information systems they use, whereas on the other hand, information systems have become an inseparable part of almost every business process in an academic institution. If there is a disturbance in the information system, it can disrupt the continuity of the business process of the academic institution concerned if it has not carried out a risk assessment. Several studies have shown that internal data corruption can be caused by several things, such as accidentally spilling data, loss of transmission, or even an attack on the data [5]. Based on the results of an interview with the Learning Manager of Rakamin Academy, this company has never conducted a risk assessment and does not yet have formal/written rules/policies regarding risk mitigation so that this company does not yet know what appropriate action to take to reduce the risks that occur.

Table 2 Risks that occur at Rakamin Academy in 2021

Event	Impact
Network Problem	User can't access the internet and ac can't access education platform. If the education platform can't access, user won't be able to upload the assignment in time, so they'll get low score because this issue. This issue can potentially damage companies' reputation.
Software bugs	Some of software bugs occurred. For example, when student can't upload their assignment, or the assignment uploaded more than 1 time. It causes wrong scoring process and increase the number of user complaints
Server Problem	Damage to server that make user can't access the education platform. It can cause the user can't upload their assignment in time and potentially damage companies' reputation.

Information assets can be in the form of hardware, software, systems, information, and people, this is an important asset for an organization that needs to be protected from security risks from both external and internal parties of the organization. Information security does not only depend on information security tools or technology but requires an understanding on the part of the organization to prioritize what must be protected and determine exactly what solutions can be used to address the problems of information security needs.

Figure 1 Three Aspects of Information Security

The picture above represents three important elements of information security and should serve as the basis for guidelines in risk management, namely [12]:

1. Confidentiality

   Confidentiality is an aspect that ensures the confidentiality of data or information, ensures that information can only be accessed by authorized persons and ensures the confidentiality of data sent, received and stored.

2. Integrity

   Integrity is an aspect that ensures that data is not changed without the permission of the authorized party, the accuracy and integrity of the information must be maintained.

3. Availability

   Availability is an aspect that ensures that data will be available when needed, ensuring that authorized users can use the information and related tools when needed.

For this reason, it is necessary to identify threats and analyze risks to improve security and reduce the risk of damage to information systems. With information technology risk management, it is expected to reduce the impact of damage in the form of: financial impact, declining reputation caused by unsafe systems, cessation of business operations, failure of assessable assets (systems and data) and delays in the decision-making process [6]. One method that can be used for information technology risk management and analysis is to use the OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation) method. OCTAVE was developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. OCTAVE known as a suite methods, tools and techniques for the assessment and planning of risk-based information system [7]. There are three different types of OCTAVE, namely: OCTAVE, OCTAVE-S and OCTAVE Allegro. For this research, we use OCTAVE Allegro which known to focus on the information and data assets that support the information and is considered suitable for use in conducting comprehensive risk assessments without extensive involvement of the organization.

In this study, an observation of website-based academic services will be carried out that focuses on the identification, analysis and risk assessment of website-based academic information systems at universities using the OCTAVE Allegro method. Based on the study described above, the formulation of the problem that will be raised in this research is determined, namely the occurrence of difficulties experienced by the management regarding the delivery of the importance of risk management in maintaining the information system and its assets for the sustainability of business processes. This is related to the absence of policies and risk assessments related to the management of information systems at Rakamin Academy.

In addition to the formulation of the problem that has been determined, the objectives and benefits of this research are also determined. The purpose of this research is to facilitate the process of identifying, analyzing, and managing information system risks at Rakamin Academy, to make risk management policies to support academic goals in reducing the impact of losses due to damage to information systems at Rakamin Academy, as well as to develop security strategies to improve security for information system at Rakamin Academy.

And finally, the results of this research are expected to provide benefits for reducing risks and losses when damage occurs to the information system and its assets at Rakamin Academy, increasing the security of information systems at Rakamin Academy, and so that the management has a firm grip on the policies that have been made regarding maintain the security of information systems that can cause disruption of business processes in Rakamin Academy. The scope of this research is to carry out a risk assessment that will focus on information systems only to protect important assets. The risk assessment carried out only relates to the IT Division which is responsible for managing the academic information system at Rakamin Academy, and the method used in risk assessment is the OCTAVE Allegro method.

2. LITERATURE REVIEW

2.1 Information System

Nowadays, many companies using information system as the foundation of their business model. According to Berdik, Information system already became a fundamental role in this era [8]. This statement matched with Gordon & Otoum statement that Information system refer to hardware, storage, internet utilities, digital application and any other aspect of technological infrastructure of business, government, schools, organizations, or other firm which using the notion of big data structure and management [9][10].

2.2 Information System Security

Companies commonly using Information System security as a way to maintain the privacy and protect companies important information [11]. As the objective of information security, there are 3 main pillars in information security. The three main pillars are confidentiality, availability, and integrity [12].

Based on industry survey, Humans are the highest factor causing data breaches compared to technical issues [13]. When building information system, we need to take care with information system security. It is because someone can potentially enter the organization's account and take the data. So the information system security created to prevent outsider who doesn't have access to get into the system [14].

2.3 Risk

Risk can be defined as the possibility of loss, injury and damage if something occurs [15]. This situation is such as uncertainty situation. So, the companies or organizations should be understood and effectively managed by the organization itself. When the risk managed effectively, this can be a good value and help the companies to achieve their objectives or goals [16].

Identifying risk must be followed by risk analysis. As part of information system security, risk analysis used to examine the current system and find the likelihood of exposure and the impact of the risk when it happens [17].

2.4 Risk Management

Risk management is a process that allows IT managers to balance operational costs and economic costs for security measures in an effort to protect IT systems and data that support the organization's mission [14].

Information system and risk management are required for every organization [18]. To meet the specific needs of the organization, successful risk management must balance risk control and risk financing techniques by considering the vision, mission, values, and goals of the organization.

Risk management in general is a process with the aim of striking a balance between efficiency and realizing opportunities to gain profits and minimize vulnerabilities and losses. Risk management should be created by organizations which have the objective to assess the level of risk associated with Information system assets. With risk management, the organizations or companies can reduce the risk to an acceptable level [19].

2.5 Risk Assessment

Risk assessment is part of risk management, risk assessment is a process to assess how often the risk occurs or how big the impact of the risk. Risk assessment is a continuous work and must be followed by accumulating, evaluating, and processing information about factors that affect the risks[20].

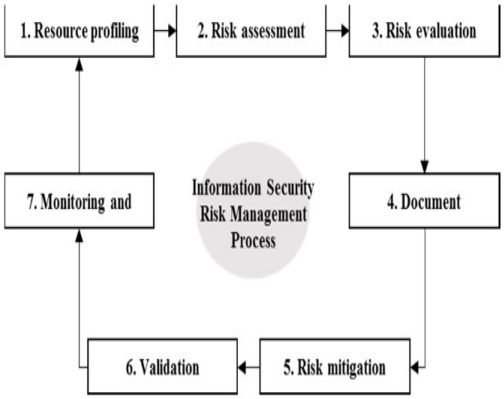

Figure 2 Information System Security Risk Management Workflow [12]

Commonly, risk assessment is carried out using qualitative techniques. The qualitative techniques mention three categories of risk assessment, namely : low, medium, and high [21]. These scales captured by interviewing the expert and other intelligent method and represent the importance of the risk.

The benefits of conducting a risk analysis include creating a clear cost-to-value ratio for security protection. It also affects the decision-making process related to hardware configuration and system software design.

The purpose of the risk assessment is to identify: (i) threats to the organization (e.g., operations, assets, or individuals) or threats addressed through the organization to other organizations or countries; (ii) Possible harm to the organization resulting from exploitation of vulnerabilities; (iii) the identification and analysis of security controls for the information system [20].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.6 OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) known as a methodology or technique to identify and evaluate information security risks in organizations or companies [6]. The use of OCTAVE itself are consists of 3 phases.

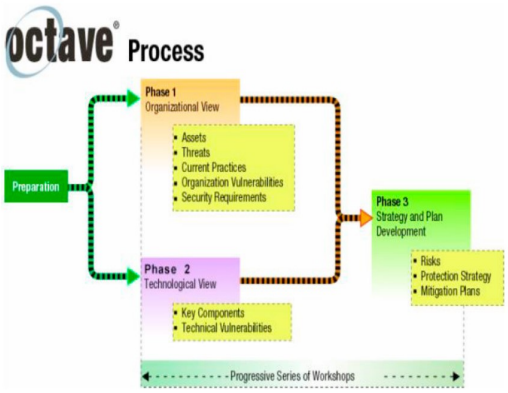

Figure 3 OCTAVE Steps [6]

The processes involved in each phase are [22]:

A. Process in phase 1:

- Process 1: Identifying Senior Management Knowledge. The participants in this process are senior managers of the organization.
- Process 2: Identify Operational Area Management Knowledge. The participants in this process are the organization's operational area (middle) managers.
- Process 3: Identify Staff Knowledge. The participants in this process are members of the organization's staff. Information technology staff members who typically participate in a workshop separate from those attended by general staff members.
- Process 4: Create a Threat Profile, The participants in this process are team member analysis. During process 4, the team identified the assets that were most important to the organization and explained how those assets were threatened

B. Process in phase 2:

- Process 5: Identification of key components the participants in this process are the analysis team and selected members of the information technology (IT) staff. The main objective of process 5 is to select infrastructure components to be examined for technological weaknesses during process 6.
- Process 6: Evaluating Selected Components The participants in this process are the analysis team and selected members of the IT staff. The objective of process 6 is to identify technology weaknesses in the infrastructure components identified during process 5.

C. Process in phase 3:

- Process 7: Conducting Risk Analysis The participants in the analysis process 7 are team members, and the purpose of this process is to identify and analyze risks to the organization's critical assets.
- Process 8 : Develop a Safeguard Strategy The objective of process 8 is to develop a safeguard strategy for the organization, a mitigation plan for risks to critical assets, and a list of short-term actions.

Nowadays, there are three different types of OCTAVES, namely: OCTAVE, OCTAVE-S and OCTAVE Allegro. Different with other OCTAVE methods, OCTAVE Allegro focused on getting information of 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 [6].

3. RESEARCH METHODOLOGY

Many risk assessment methods which we can implement to assess information system security. One of the popular methods is OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). OCTAVE is a method that can evaluate the information security risks and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

defines its critical components of a comprehensive, systematic, and context-driven evaluation [23]. With OCTAVE method, organizations can take a decision based on CIA (Confidentiality, Integrity, Authentication). This decision can be implemented for critical information technology assets and protect the organizations information [24].

To evaluate and identify the information security risks, OCTAVE intended to help the company in terms of: (a) Develop a qualitative risk evaluation criteria that describe the company's operational risk tolerance; (b) Identify assets that are important for achieve the company's mission; (c) Identify vulnerabilities and threats to those assets; (d) Determine and evaluate to deal with the consequences that occur to the company if the threat occurs.

Nowadays, there are three known variants of OCTAVE. The variants are OCTAVE, OCTAVE-S and OCTAVE Allegro. OCTAVE is a set of techniques, methods and tools which can be used for risk-based information system security assessment and planning. Basically, OCTAVE Allegro created with more simple method with a focus on information assets. We can use OCTAVE Allegro using a collaborative method and workshop-style. There are eight steps of OCTAVE Allegro to evaluate and identify the information security risks in the company.

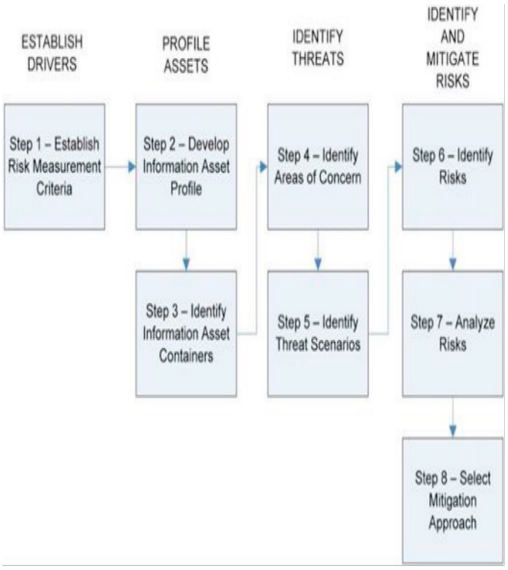

Figure 4 OCTAVE Allegro

OCTAVE Allegro consist of 4 main activity area that mentioned 8 activities. Here are the activity area of OCTAVE Allegro [19]:

A. Establishing drivers: in this area, the companies will develop criteria of risk measurement that are consistent with companies' drivers. In this area, there is one step to do, namely Establish Risk Measurement Criteria.

B. Profile Assets: this area consists of Develop Information Asset Profile and Identify Information Asset Containers. These activities' purpose is to identify the critical assets, so the critical assets will be focused on risk assessment. To do that, companies should understand each of assets so they can identify the potential thread and vulnerabilities.

C. Identify threats: this area's purpose is to make documentation of vulnerabilities based on their containers. These vulnerabilities documented through identifying areas of concern and threat scenarios.

D. Identify and mitigate risks: after risks already analyzed and identified based on thread information, the next step is to create mitigation strategies to overcome the risks. In this area, there are several activities to do, namely: identify risks, analyze risks, and select mitigation approach.

4. RESULT AND DISSCUSSION

From the methods that have been selected and explained from the previous methodology chapter, the following is a description of the results of the methods that have been chosen:

4.1 Establishing Risk Measurement Criteria

In the first step, the organizational drivers that have been built will be used to evaluate the impact of a risk on the company's mission and business objectives which will be identified as the basis for determining the impact area. Then the determination of the impact area that is considered to be the most important will be carried out along with the value of the priority scale in the predetermined impact area. Risk measurement criteria are used to evaluate the impact in each

area. It includes qualitative measures whose risk can be evaluated and forms the basis of an information system risk assessment. The following is a priority impact area and the determination of the impact area of reputation and trust:

Table 3 Impact Area Priority Scale and Values

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

Table 4 Impact Area – Customer Reputation and Trust

Impact Area	Low	Medium	High
Reputation	Reputation was slightly affected; it only takes a small effort to repair	Reputation is being affected; reputation has been badly affected and it takes effort and money to repair	High reputation affected; the reputation has been so badly affected that it can barely be repaired
Customer Trust	Customer Trust was slightly affected; customer reduction < 2%	Customer Trust is being affected; customer reduction < 2% - 10%	High Customer Trust is affected; customer reduction > 10%
Financial	Financial are slightly affected; financial reduction < 2% of income	Financial are being affected; financial reduction < 2% - 10% of income	High financial affected; financial reduction > 10% of income
Productivity	Productivity is slightly affected; productivity down < 2% from many activities that existed before	Productivity is being affected; productivity down < 2% - 10% from many activities that existed before	High productivity affected; productivity fell >10% from many previous activities
Fines and Penalties	Fines and Penalties are slightly affected; fines and penalties are subject to <2% of income	Fines and Penalties are being affected; fines and penalties are subject to < 2% - 10% of income	High Fines and Penalties affected; fines and penalties are subject to > 10% of income
Safety and Health	Safety and Health are slightly affected; it only takes a small effort to repair	Safety and Health; health and safety has been badly affected and efforts and costs are required for repairs	High Safety and Health affected; safety and health have been impacted so badly that they can hardly be repaired

4.2 Building an Information Asset Profile

The second step is to build an information asset profile on critical information assets based on the company's core processes. A profile is a representation of an information asset that describes its unique features, qualities, characteristics, and values. This method is very useful for ensuring that the assets are clearly and consistently described so as to avoid ambiguous definitions of asset boundaries and make it easier to formulate information security requirements. In this case study, it will start from student data to the final grade report in the form of a grade transcript. Then the next activity is to determine the critical information assets that will be recorded on the critical asset information worksheet. The selected information assets must be considered based on their importance in daily activities and which if lost could interfere with the mission and objectives of the company. Based on the above considerations, the distribution of important information assets is divided into three categories, namely: subject profiles, student profiles, lecturer profiles, and student value transaction profiles. The following is an information asset profiling of value transactions from students:

Table 5 Information Asset Profiling: Student Data

Critical Asset	Rational Selection
Student Data	The role of students is very important in every company's business processes so that if student data is damaged/lost it will have an impact on the continuity of company activities.
Owner	
Learning Manager	
Security Requirement	
Confidentiality	Only certain parties can access this

	asset. This information is very important for students, lecturers, and departments, so only certain administrative divisions can use this information to print student transcripts.
Integrity	Only certain parties can modify this asset. This information must be true and accurate, subject to change and modification by the lecturer, and only certain operators in the administration section can enter or modify student scores. Values are important information for students, if there are errors it will harm students, therefore the value of integrity is very important.
Availability	These assets must be available to all parties, safe 24 hours, 7 days/week, 52 weeks/year. This information should always be available to students, faculty, and student administration.

Table 6 Information Asset Profiling: Student Value Transactions

Critical Asset	Rational Selection
Transcripts	Used to determine the GPA and determine the quality of students consisting of the final grades of students.
Owner	
Learning Manager	
Security Requirement	
Confidentiality	Only certain parties can access this asset. This information is very important for students, lecturers, and departments, so only certain administrative divisions can use this information to print student transcripts.
Integrity	Only certain parties can modify this asset. This information must be true and accurate, subject to change and modification by the lecturer, and only certain operators in the administration section can enter or modify student scores. Values are important information for students, if there are errors it will harm students, therefore the value of integrity is very important.
Availability	These assets must be available to all parties, safe 24 hours, 7 days/week, 52 weeks/year. This information should always be available to students, faculty, and student administration.

Table 7 Information Asset Profiling: Application

Critical Asset	Rational Selection
Application	Used to input, store, and process transaction data to simplify the company's business processes.
Owner	
IT Unit	
Security Requirement	
Confidentiality	Only certain parties can access this asset. This information is very important for students, lecturers, and departments, so only certain administrative divisions can use this information to print student transcripts.
Integrity	Only certain parties can modify this asset. This information must be true and accurate, subject to change and modification by the lecturer, and only certain operators in the administration section can enter or modify student scores. Values are important information for students, if there are errors it will harm students, therefore the value of integrity is very important.
Availability	These assets must be available to all parties, safe 24 hours, 7 days/week, 52 weeks/year. This information should always be available to students, faculty, and student administration.

Table 8 Information Asset Profiling: Application

Critical Asset	Rational Selection
Server	Used for the center of all data generated by the company, including storing applications and databases on client or connected computers, providing security features, protecting all connected computers and providing IP addresses on connected computer machines.

Owner	
IT Unit	
Security Requirement	
Confidentiality	Only certain parties can access this asset. This information is very important for students, lecturers, and departments, so only certain administrative divisions can use this information to print student transcripts.
Integrity	Only certain parties can modify this asset. This information must be true and accurate, subject to change and modification by the lecturer, and only certain operators in the administration section can enter or modify student scores. Values are important information for students, if there are errors it will harm students, therefore the value of integrity is very important.
Availability	These assets must be available to all parties, safe 24 hours, 7 days/week, 52 weeks/year. This information should always be available to students, faculty, and student administration.

Table 9 Information Asset Profiling: Switch

Critical Asset	Rational Selection
Switch	Used to connect all existing computer networks.
Owner	
IT Unit	
Security Requirement	
Confidentiality	Only certain parties can access this asset. This information is very important for students, lecturers, and departments, so only certain administrative divisions can use this information to print student transcripts.
Integrity	Only certain parties can modify this asset. This information must be true and accurate, subject to change and modification by the lecturer, and only certain operators in the administration section can enter or modify student scores. Values are important information for students, if there are errors it will harm students, therefore the value of integrity is very important.
Availability	These assets must be available to all parties, safe 24 hours, 7 days/week, 52 weeks/year. This information should always be available to students, faculty, and student administration.

Table 10 Information Asset Profiling: Access Point/ Lightweight Access Point Protocol (LWAPP)

Critical Asset	Rational Selection
Access Point/ Lightweight Access Point Protocol (LWAPP)	Used to manage a large number of light-weight access points by network admin staff.
Owner	
IT Unit	
Security Requirement	
Confidentiality	Only certain parties can access this asset. This information is very important for students, lecturers, and departments, so only certain administrative divisions can use this information to print student transcripts.
Integrity	Only certain parties can modify this asset. This information must be true and accurate, subject to change and modification by the lecturer, and only certain operators in the administration section can enter or modify student scores. Values are important information for students, if there are errors it will harm students, therefore the value of integrity is very important.
Availability	These assets must be available to all parties, safe 24 hours, 7 days/week, 52 weeks/year. This information should always be available to students, faculty, and student administration.

4.3 Information Asset Profiling: Student Value Transactions

In the third step, identification of the information asset container will be carried out. Containers are places where information assets are stored, shipped, and processed. In the third step, all

containers that store, ship and process, both internal and external will be identified. The following is an example of an Information Asset Risk Environment Map (Techniqal) from Student Value Transactions:

Table 11 Information Asset Container

Container	Description	Internal/ External	Owner(s)
Technical	Module: Data input transactions can be processed	Internal	IT Unit
	Database: Data is stored in enterprise database for web applications.	Internal	IT Unit
	Internal network: All transactions run in the network.	Internal	IT Unit
	Academic Information System: Data is accessed and processed in a web application for changes to student data information.	External	Student
Physical	Request data: Student Administration Staff requests student data using a data request letter to the IT unit	Internal	Department Staff Student Administration IT Unit
	Student files at admission	External	Department Staff Student Administration Student
Human	Department Staff Student Administration	Internal	Department Staff Student Administration
	Student	External	Student

4.4 Identifying Areas of Concern

In the fourth step, identification of areas of concern is carried out by reviewing each container to see and determine potential areas of concern, then proceed with documenting each identified area of concern. The area of concern will be expanded to obtain threat scenarios and then documented to see if these threats affect security requirements. The following is a table of areas of concentration from the case studies in this study:

Table 12 Area of Concern

No	Area of Concern	Related Asset
1	Network failure	Infrastucture
2	Hacker Attack	
3	Fire	
4	Change of master data and transaction data	Application
5	Theft or dissemination of important information	
6	Abuse of access rights	
7	Human or technician error	People

4.5 Identifying Threat Scenarios

In this fifth step, the areas identified in the previous step will be expanded into a more detailed threat scenario and detail the properties of a threat, including using actors, means, motives, outcomes, and security requirements. This step is useful for giving consideration to the possibilities in the threat scenario. The following is a table of properties of threat from student value transactions:

Table 13 Threat Scenarios

Area of Concern	Threat of Properties	
Network failure	Actors	IT Unit
	Means	Error in network configuration
	Motives	Accidental
	Outcome	Interruption
	Security Requirements	Carry out network control by always monitoring and maintaining system security which is reviewed regularly
Hacker Attack	Actors	IT Unit
	Means	Lack of security guard
	Motives	Human error (Accidental)
	Outcome	Destruction Modification Interruption
	Security Requirements	Protect against all possible hacker attacks

Fire	Actors	Department staff Student Administration IT Unit
	Means	Mistakes in guarding against disaster
	Motives	Accidental
	Outcome	Destruction
	Security Requirements	Providing a safe space for disaster protection
Change of master data and transaction data	Actors	Department staff Student Administration IT Unit
	Means	Loss or overwriting of data in backing up data that is done routinely (transaction data) or occasionally (master data) is enforced
	Motives	Human error (Accidental)
	Outcome	Destruction Modification Interruption
	Security Requirements	Planning a periodic data back-up schedule
Theft or dissemination of important information	Actors	Department staff Student Administration IT Unit
	Means	Data loss or leakage occurs
	Requirements	data access rights and log every activity carried out on the application
Abuse of access rights	Actors	Department staff Student Administration IT Unit
	Means	The occurrence of abuse of access rights owned
	Motives	Human error (Accidental)
	Outcome	Destruction Modification Interruption
	Security Requirements	Doing logging of every activity carried out on the application
Human or technician error	Actors	Department staff Student Administration IT Unit Student
	Means	An error occurred due to an action taken by the user
	Motives	Human error (Accidental)
	Outcome	Destruction Modification Interruption
	Security Requirements	Guidance and socialization are provided for using the application

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

Theft or dissemination of important information	Motives	Human error (Accidental)
	Outcome	Destruction Modification Interruption
	Security	Manage limited

4.6 Identifying Risk

In the sixth step, risk identification will be carried out which aims to determine how the threat scenario will have an impact on the company and determine grouping based on high, medium, or low levels. Identification of this risk is important to see the consequences for the organization if a threat occurs and needs to be recorded, in order to get a complete risk picture because a threat can have potential consequences for the company.

Table 14 Impact Area Value

4.7 Analyzing Risk

In the seventh step, the relative score will be calculated to assist the company in analyzing risks in determining the right strategy to deal with these risks. A quantitative measurement of the extent to which the company is affected by the threat is calculated. The relative risk value is obtained by considering the extent of the consequences of the risk impact on various impact areas and estimating the likelihood.

Table 15 Relative Risk Value

Area of Concern	Risk			
Network failure	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	Med	10
		Financial	Med	8
		Productivity	High	9
		Safety and Health	Low	1
		Fines and Penalties	Low	2
	Relative Risk Score			30
Hacker Attack	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	High	15
		Financial	High	12
		Productivity	High	9
		Safety and Health	Low	1
		Fines and Penalties	Med	4
	Relative Risk Score			41
Fire	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	Low	5
		Financial	High	12
		Productivity	High	9
		Safety and Health	High	3
		Fines and Penalties	Med	4
	Relative Risk Score			33
Change of master data and transaction data	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	High	15
		Financial	High	12
		Productivity	High	9
		Safety and Health	Low	1
		Fines and Penalties	Med	4
	Relative Risk Score			41
Theft or dissemination of important information	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	High	15
		Financial	High	12
		Productivity	High	9
		Safety and Health	Low	1
		Fines and Penalties	High	5
	Relative Risk Score			42
Abuse of access rights	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	High	15
		Financial	High	12
		Productivity	Low	3
		Safety and Health	Low	1
		Fines and Penalties	High	5
	Relative Risk Score			35
Human or technician error	Severity	Impact Area	Value	Score
		Customer Reputation and Trust	High	15
		Financial	High	12
		Productivity	High	9
		Safety and Health	Low	1
		Fines and Penalties	Med	4
	Relative Risk Score			35

4.8 Choosing a Risk Reduction Approach

In the last step of the OCTAVE process Allegro will determine the risks that require mitigation and develop strategies to reduce those risks. This is done by prioritizing risks based on relative risk values, then developing a mitigation strategy by considering the value of assets and security needs, containers of assets, and the company's unique operational environment.

Table 16 Relative Risk Matrix

Relative Risk Range Score	Pool
30 - 45	Pool 1
16 - 29	Pool 2
0 - 15	Pool 3

Table 17 Mitigation Approach

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

Table 18 Risk Mitigation by Area of Concern

Risk Mitigation	
Area of Concern: Network Failure	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Carry out network control by always monitoring and maintaining system security which is reviewed regularly
Area of Concern: Hacker Attack	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Protect against all possible hacker attacks
Area of Concern: Fire	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Providing a safe space for disaster protection
Area of Concern: Change of master data and transaction data	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Planning a periodic data back-up schedule
Area of Concern: Theft or dissemination of important information	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Manage limited data access rights and log every activity carried out on the application
Area of Concern: Abuse of access rights	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Doing logging of every activity carried out on the application
Area of Concern: Human or technician error	
Pool	Pool 1
Action	Mitigate
Container	Control
Security Requirement	Guidance and socialization are provided for using the application

5. CONCLUSION

Based on our research, the Octave Allegro method is one of the methods in information system risk management that can be applied to course student without requiring extensive involvement in the company and is focused on critical information assets for the sustainability of the company's business processes in achieving its mission and goals.

This risk assessment can provide an overview related to the possibility of threats to the company's critical assets as well as how to take steps for appropriate prevention in minimizing the possibility that these threats will occur.

As a result of the risk assessment, policy makers can make and decide on a strategic plan to properly safeguard critical information assets with recovery measures if a threat scenario does occur.

REFERENCES

[1] V. Ignat, "Digitalization and the global technology trends," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 227, no. 1, 2017, doi: 10.1088/1757-899X/227/1/012062.

[2] A. Baldominos and D. Quintana, "Data-driven interaction review of an ed-tech application," *Sensors (Switzerland)*, vol. 19, no. 8, pp. 1–14, 2019, doi: 10.3390/s19081910.

[3] N. Selwyn *et al.*, "What's next for Ed-Tech? Critical hopes and concerns for the 2020s," *Learn. Media Technol.*, vol. 45, no. 1, pp. 1–6, 2020, doi: 10.1080/17439884.2020.1694945.

[4] N. Mayer and C. Feltus, "Evaluation of the risk and security overlay of archimate to model information system security risks," *Proc. - IEEE Int. Enterp. Distrib. Object Comput. Work. EDOCW*, vol. 2017-October, pp. 106–116, 2017, doi: 10.1109/EDOCW.2017.30.

[5] X. Zhang, L. Zhao, A. P. Boedihardjo, and C. T. Lu, "Online and distributed robust regressions under adversarial data corruption," *Proc. - IEEE Int. Conf. Data Mining, ICDM*, vol. 2017-Novem, pp. 625–634, 2017, doi: 10.1109/ICDM.2017.72.

[6] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," *Procedia Comput. Sci.*, vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.

[7] W. Sardjono and M. I. Cholik, "Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank," *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 38–42, 2018, doi: 10.1109/ICIMTech.2018.8528108.

[8] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102397, 2021, doi: 10.1016/j.ipm.2020.102397.

[9] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, 2018, doi: 10.1016/j.csbj.2018.06.003.

[10] S. Otoum, I. Al Ridhawi, and H. T. Mouftah, "Blockchain-Supported Federated Learning for Trustworthy Vehicular Networks," *2020 IEEE Glob. Commun. Conf. GLOBECOM 2020 - Proc.*, 2020, doi: 10.1109/GLOBECOM42002.2020.9322159.

[11] J. S. Suroso, A. R. Putra, J. Gunawan, and D. W. Danuanindito, "Smartphone user awareness of personal information security and privacy," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 8, pp. 2416–2428, 2018.

[12] E. Wheeler, *Security Risk Management: Building An Important Security Risk Management Program From The Ground Up*. 2011.

[13] Y. Gangire, A. Da Veiga, and M. Herselman, "A conceptual model of information security compliant behaviour based on the self-determination theory," *2019 Conf. Inf. Commun. Technol. Soc. ICTAS 2019*, 2019, doi: 10.1109/ICTAS.2019.8703629.

[14] M. T. Jufri, M. Hendayun, and T. Suharto, "Risk-assessment based academic information System security policy using octave Allegro and ISO 27002," *Proc. 2nd Int. Conf. Informatics Comput. ICIC 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/IAC.2017.8280541.

[15] S. H. Sung, "Quantitative and Qualitative Approach for IT Risk Assessment," *Asia-pacific J. Converg. Res. Interchang.*, vol. 1, no. 1, pp. 29–35, 2015, doi: 10.21742/apjcri.2015.03.04.

[16] A. Leonard, N. Anggito, F. Sialagan, and J. S. Suroso, "Information system security risk management e-learning using fmea in university," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 7565–7568, 2020, doi: 10.30534/ijatcse/2020/93952020.

[17] M. A. Rivai, J. S. Suroso, and F. Pangemanan, "Review of the risk analysis using MEHARI model: The guideline to analyze risk for startup educational platform," *Proc. 2020 Int. Conf. Inf. Manag. Technol. ICIMTech 2020*, no. August, pp. 577–582, 2020, doi: 10.1109/ICIMTech50083.2020.9211204.

[18] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management," *Softw. Syst. Model.*, vol. 18, no. 3, pp. 2285–2312, 2019, doi: 10.1007/s10270-018-0661-x.

[19] J. S. Suroso, S. M. N. Rahaju, and Kusnadi, "Evaluation of IS Risk Management Using Octave Allegro in Education Division," *2018 Int. Conf. Orange Technol. ICOT 2018*, pp. 1–8, 2018, doi: 10.1109/ICOT.2018.8705866.

[20] V. Nitsenko *et al.*, "Automatic information system of risk assessment for agricultural enterprises of ukraine," *Montenegrin J. Econ.*, vol. 15, no. 2, pp. 139–152, 2019, doi: 10.14254/1800-5845/2019.15-2.11.

[21] S. T. Cruz, "Information security risk assessment," *Inf. Secur. Manag. Handbook, Sixth Ed.*, pp. 243–250, 2007, doi: 10.3390/encyclopedia1030050.

[22] C. Woody, "OCTAVE: Applying OCTAVE: Practitioners Report," *Young*, no. May, 2006.

[23] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," *Pittsburgh, PA, Carnegie Mellon Univ.*, no. August, 2003.

[24] S. K. PANDEY, "A Comparative Study of Risk Assessment Methodologies for Information Systems," *Bull. Electr. Eng. Informatics*, vol. 1, no. 2, pp. 111–122, 2012, doi: 10.12928/eei.v1i2.231.