Journal of Information Systems and Informatics
Vol. 4, No. 3, September 2022 e-ISSN: 2656-4882 p-ISSN: 2656-5935
http://journal-isi.org/index.php/isi Published By DRPM-UBD

Academic IS Risk Management using OCTAVE Allegro in Educational Institution

Vincentius Gerardo[1], Ahmad Nurul Fajar[2]

[1]Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia
[2]Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia
Email: [1]vincentius.gerardo@binus.ac.id, [2]afajar@binus.edu

Abstract

Today, the use of technology is a common thing that is used to support everyday life. However, this technology also carries risks that can compromise the security of information in organizations. Kalbis Institute is a private campus in the East Jakarta area that has been established since 2012. The academic information system used there includes all actors in the campus environment. This risk analysis is carried out to see and understand what risks exist in the current information system. This risk analysis will assess how likely there are threats and vulnerabilities to information systems. This study uses the OCTAVE Allegro method with the help of the OCTAVE Allegro Worksheet. The purpose of this study is to conduct a risk analysis of the academic information system at Kalbis Institute. The result of this study is to look at risk assessments and recommendations for strategies to protect information systems within organization.

Keywords: Academic IS, IS Risk Management, OCTAVE Allegro, OCTAVE Allegro Worksheets, Risk Management

1. INTRODUCTION

Nowadays, it's common to use technology to help with daily tasks in life. Information technology can be defined as everything computer-based related, tools for providing and supporting information and the requirement for processing information in an organization [1]. Information that is transferred by one division to another can be easily done by using technology. One of the most common usages of information technology is the usage of a web based academic information system inside an educational institution. Web based information systems are very easy to implement inside an organization and is also very easy to access. Inside the information system, there are a few actors namely: students, lecturer, and other employees that are involved in the organization. This academic system is used as a foundation to share information between the students and the lecturers for academic purposes.

However, in daily use, technology can also show risks that can't be avoided. Risk management is one of the most important things in the organization. Risks inside an information system can be categorized into 4 categories, namely: compliance risks, hazard risks, control risks, and opportunity risks [2]. In general, an organization must minimalize the compliance risk, mitigate the hazard risks, manage control risks and embrace opportunity risks [2]. While risk management is a method of determining and implementing actions that will reduce the negative consequences of risk on a business [3]. Risk management can also be defined as a collection of operations carried out inside an organization to provide the most profitable results while minimizing the volatility or fluctuations of those outputs [2].

This research is inducted at Kalbis Institute, a private educational institution that is in East Jakarta and has been around for at least 10 years. The system is used to help support the learning process inside the institution. The system itself was introduced to the institution in 2012, however in recent years the information system has had a few problems. The first one is the availability and the integrity of the information that is shared between the divisions. Another problem is the lack of error handling in the application so the users can see the error from the system. Which can lead to SQL Injection if not treated carefully. There is also the risk of using software that is aging like the usage of Windows 7 for client computers and the usage of Windows Server 2012 for some of the servers and Windows Server 2016 as the main operating system for the production server. These operating systems have been around for a while and for Windows 7 and Windows Server 2012, are near or have already dropped support for security updates. These leave the operating system to have curtain holes inside the security, making it a target for unintended access. Also, there is the lack of awareness for confidentiality of credentials that is given to each user that result in students accessing other student's account to check for the score of a test or to match a schedule when filling the schedule for the semester. There has also been a system change in 2020 that introduces a new system to the institution and there has not been a risk assessment since the system change.

There have been several research that uses OCTAVE Allegro for Educational Institutions. For example, the research from [4] that was conducted in 2018. In this research, the researchers have found that there are 8 critical information assets with 51 areas of concern, where 34 must be migrated, 17 deferred inside MH. Thamrin University to see how big is the risk inside the organization [4]. Another example of Risk Assessment using OCTAVE Allegro inside educational institutions is from [5] that was conducted in 2020. In this research the researchers found that there are a few risks factors inside the educational institution and OCTAVE Allegro can be inducted without direct participation inside the organization. Another research using OCTAVE Allegro in a educational institution is from [6] which was conducted in 2018. In this research, where the

maturity level of the risk management is 89.40% and there is gap between the contingency plan and vulnerability management practices with the score 87.88% and 66.67% respectively [6].

There are 3 main factors that is the main concern in maintaining the security of the information system, specifically: Security of critical data inside the organization, Integrity of the information inside the information system, Availability of information that can be accessed. Each factor is critical to maintain and securing the information inside the institution. The method used inside this research is OCTAVE (Operationally Critical Threats, Assets, and Vulnerability Evaluation) specifically using OCTAVE Allegro. OCTAVE alone is an approach for managing information security risk [7]. There are 3 types of the OCTAVE method, namely: OCTAVE (for large organizations), OCTAVE-S (for small organizations), and OCTAVE Allegro. OCTAVE Allegro focuses primarily on information assets within the context of how the asset is used, where the asset is stored, transported, and processed, and how are the asset are exposed to threats, vulnerability, and disruptions as a result [8].

This research is aimed to list and analyze the risks that may occur inside the academic information system that is used inside Kalbis Institute. In this research, the researcher will conduct the risk listing and analyzing inside the academic information system that is used day-to-day by the institution and will use OCTAVE Allegro The information system has never been taken into risk assessment and there has been a completely new update to the system. Worksheets to help understand and listing the risks that are present. The purpose of this research is to list the risk that can occur inside the academic information system, to perform a risk assessment for the new system and show how much is the impact of a risk, and list which information is critical to the organization, also to create a strategy for reducing the risks to the organization.

2. METHODS

This research is using an exploratory case study for evaluating risk management in Kalbis Institute, a private educational institution located in Jakarta. The methodology that is used in this research is OCTAVE Allegro with the help of OCTAVE Allegro Worksheets to help understand to create risk assessment. Risk assessment itself is an essential part of risk management that is used to identify, analyze and evaluate a curtain risk [9]. In information technology, information security is a new term that is increasing awareness of access, usage, disclosure, disruption, modification, inspection, recording and destruction of data from an organization that can be accessed [10]. Figure 1 below shows the steps that is taken during the research:

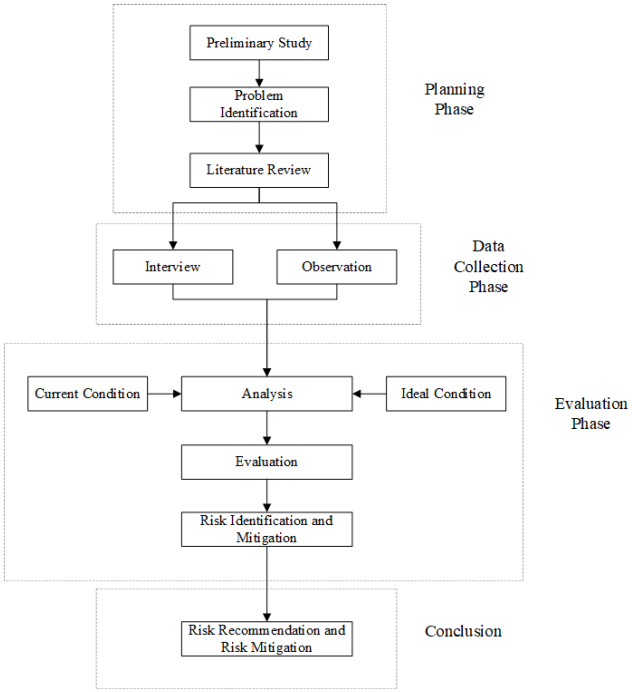

Figure 1. Research Methodology

Based on figure 1 above, the steps that are taken in this research consists of:

1. Planning Phase

   In this phase, the researcher will conduct a preliminary study on the profile of the educational institution and identify the information systems that support the institution's daily activities. After identifying, the researcher will identify the background for the research and will be formulating the problems and do literature studies.

2. Data Collection Phase

   In this phase, the researcher will first interview the head of IT inside the institution, the second will also observe the current information system. Thirdly the researcher will also be looking for spaces inside the policy or procedures that can cause a risk. One of the activities that can be used here is the usage of Gap Assessment. Gap Assessment is the activity of comparing between what exists at the current moment with what is ideal or required by the organization [11].

3. Evaluation Phase

   In this phase, the researcher will conduct an analysis of the current system and the expected ideal system. After analysis, the researcher will conduct the

evaluation using the OCTAVE method and identify the risks and mitigation to prevent future risks.

4. Conclusion

In this stage, the researcher will conduct a report based on the previous step and will also suggest mitigating risk or preventing the risk that can happen to the institution.

There are 10 worksheets that is used in this research and each worksheet has its own role in the process of OCTAVE Allegro. With OCTAVE Allegro, there are 8 steps that the researcher will do inside this research based on the figure 2 below

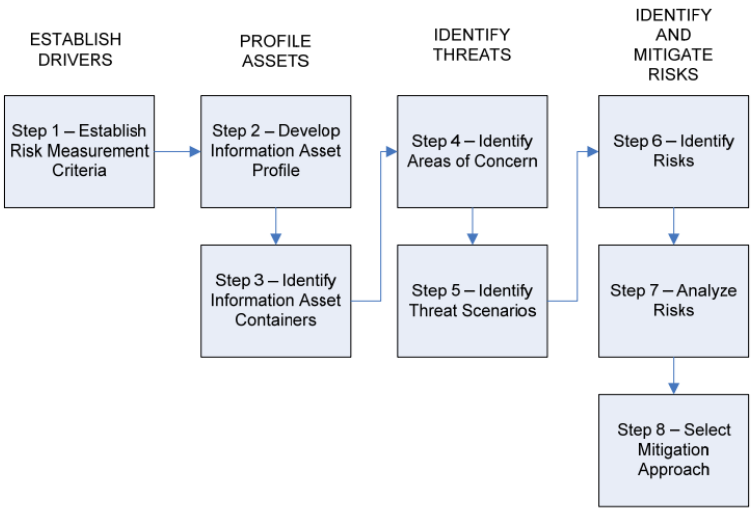

Figure 2. OCTAVE Allegro Workflow [8]

OCTAVE Allegro alone is a phased approach that is an extremely good place to start for those just beginning to implement formal risk assessments within an organization and is an approach that can be implemented by organizations even with a less structure around the application and system deployment life cycle [12].

In this research, the researcher will use the help of OCTAVE Allegro Worksheets to help understand how the process of risk assessment is held. OCTAVE Allegro worksheet is a set of worksheets that is divided into 4 parts, as follows:

1. Risk Assessment Criteria and Impact Area Prioritization Worksheet
2. Information Asset Profile Worksheet
3. Information Asset Risk Environment Worksheet
4. Information Asset Risk Worksheet

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3. RESULTS AND DISCUSSION

Using OCTAVE Allegro as the methodology in this research, there are 8 steps in this part. These 8 steps are specific, and each step is related to each other. The scope of this research is for the IT Department in Kalbis Institute that maintains the system.

In evaluating risk assessment regarding IS in IT Department, the researcher has conducted an interview with the IT Manager and the IT Coordinator. The researcher also did an observation and was given the access to look at the existing information system. OCTAVE Allegro was the first choice of methodology because of its easy to use and the limited involvement of the information system. Below are the 8 steps in OCTAVE that is used in this research:

3.1. Step 1: Establish Risk Measurement Criteria

In this step, there are 2 main activities, namely impact area analysis and impact area prioritization. In this stage, the goal is to find which areas of impact are most affected and what risk assessment is like at Kalbis Institute. Secondly, this measurement can be used as the base to do the calculations on the next step. The purpose of the first step is to identify what is the main criteria for each risk assessment, and to identify which area has the highest impact to the institution. The first step is to find what are the criteria for each impact areas, for each impact area there will be a scale that is set to low, moderate, or high.

There are 5 impact areas in OCTAVE Allegro, namely: reputation and customer confidence, financial, productivity, safety and health, and fines and legal penalties.

The first impact area of the 5 impact areas is for reputation and customer confidence to the organization. In this area, there are 2 main impact areas, which are reputation and customer loss for the organization. For an educational institution, reputation and customer confidence is one of the important areas. Reputation is gained through the results of public trust to an organization. Table 1 below, contains the impact area and the criteria for low, moderate, and high for reputation and customer confidence.

Table 1. Reputation and Customer Confidence

Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected. Little or no effort or expense is required to recover	Reputation is damaged, and some effort and expense are required to recover	Reputation is irrevocably destroyed or damaged

Customer Loss	Less than 5% reduction in customers due to loss of confidence	5% to 10% reduction in customers due to the loss of confidence	More than 10% reduction in customers due to the loss of confidence

The second impact area is for financial costs. In this area, there are 2 impact areas based on the discussion. These 2 areas are operating costs and revenue loss. Operating cost is the amount that is used by the organization run operations, while revenue loss is the amount that the organization loses yearly. Table 2 below contains the impact area and the criteria for low, moderate, and high for financial.

Table 2. Financial

Impact Area	Low	Moderate	High
Operating Costs	Increase of less than 2% in yearly revenue costs	Yearly operating costs increase by 2% to 5%	Yearly operating costs increase by more than 5%
Revenue Loss	Less than 2% yearly revenue loss	2% to 5% yearly revenue loss	Greater than 5% yearly revenue loss

The third impact area is for staff productivity. In this area, the impact area indicator is the increase time of staff hours inside the organization. Staff hours is counted based on the additional time for a staff to complete a task when there is a risk. Table 3 below shows the impact area and the criteria for low, moderate, and high for productivity

Table 3. Productivity

Impact Area	Low	Moderate	High
Staff Hours	Staff work hours are increased by less than 1 week	Staff work hours are increased between 1 to 2 weeks	Staff work hours are greater than 2 weeks

The fourth impact area is safety and health of the staff members. In this impact area, there are 3 indicators for this area which consists of: life, health, and safety of a staff member. Each impact area is for the safety, the health, and the life of the employee. Table 4 below contains the impact area and the criteria for low, moderate, and high for safety and health.

Table 4. Safety and Health

Impact Area	Low	Moderate	High

Life	No loss of significant threat to customers' or staff members' life	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment	Loss of customers' or staff members' lives
Health	Minimal. Immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects or customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated

The fifth impact area is the fines and legal penalties that is faced by the organization when a risk. In this area, there are 2 impact areas that consists of fines and investigations. Fines are the amount of money that is charged to the organization based on the violation that occurs, while investigations are the activity that is used to find the cause of an incident inside the organization. Table 5 below contains the impact area and the criteria for low, moderate, and high for fines and legal penalties.

Table 5. Fines and Legal Penalties

Impact Area	Low	Moderate	High
Fines	Fines less than Rp. 50 million are levied	Fines between Rp. 50 million and Rp. 150 million are levied	Fines greater Rp. 150 million than are levied
Investigations	No quires from government or other investigative organizations	Government or other investigative organizations requests information or records (low profile)	Government or other investigative organization initiates a high-profile. in-depth investigation into organizational practices

Based on the areas of impact mention above, the researcher has concluded that the measurement criteria should be based on the priority of the impact area. The priority is based on discussion and the likelihood of the risk inside the organization. The next step is to list which impact area is prioritized. These areas are the first to mitigate if the risk occurs inside the institution. Table 6 below describes the priority of the impact area.

Table 6. Measurement Criteria

Priority	Criteria
3	Reputation and Customer Confidence
5	Financial
4	Productivity
1	Safety and Health
2	Fines and Legal Penalties

3.2. Step 2: Develop Information Asset Profile

In this step, the researcher will develop the asset profile of the critical information for the institute. The information asset that is mentioned here have a unique feature, characteristic, and value. There are also a few criteria for the critical asset, that is described below:

1. The asset must contain a specific and important information
2. The asset must be used inside the institution and is used to support the information system
3. When there is harm to the asset, there will be a downtime or maintenance to bring back the information asset

Based on the criteria set above, the researcher has described the critical asset profile as follows:

1. Student's Profile
2. Student's absence
3. Student's grades
4. Class schedule
5. Lecturer's Profile
6. Semester Lesson Plans

Based on the six assets that are listed above, the next step is to identify each asset profile and make a list on why the asset above are critical. Each information asset has their own security requirements, description, information owner, and which is the most important security requirements. Each asset here will be identified and will be capture the information on the asset based on the interview. Table 7 to table 12 are the description for each asset.

Table 7. Student's Profile

Critical Asset	Description
Student's Profile	This asset contains the information of the student's background, name, address, gender, phone number, parent's phone number, parent's name
Owner(s)	
Admission, IT	
Security Requirements	

Confidentiality	The data is confidential and can only be accessed by the admission team for student registration, student services, lecturer for student guidance, and the student itself
Integrity	The data can only be edited by the admission team with a replacement application from the student or the student services.
Availability	The data can only be accessed by the student itself
Most Important Security Requirement	Confidentiality

Table 8. Student's Absence

Critical Asset	Description
Student's Profile	This asset contains the list of absence for each student, each subject, and each semester
Owner(s)	
Lecturer Service, IT	
Security Requirements	
Confidentiality	The data isn't confidential but can only be accessed by the student itself and the lecturer for subject, also for the lecturer services for changing the absence
Integrity	The data is inserted by the lecturer of the subject when teaching and is filled by calling out the student's name
Availability	This data can be accessed by the student itself, the lecturer of the subject, IT for changing the absence, lecturer service for reviewing the absence of a student
Most Important Security Requirement	Integrity

Table 9. Student's Grades

Critical Asset	Description
Student's Profile	This asset contains the grade of each student and is inputted by the lecturer for assignments as well as exams for one subject
Owner(s)	
Lecturer service, IT	
Security Requirements	
Confidentiality	This data is confidential and can only be accessed by the student itself and the lecturer that gave the score
Integrity	This data is inputted by the lecturer while doing an assignment as well as exams for the student during the study
Availability	This data can be accessed by the student itself, the lecturer of the subject, lecturer service to file a grade change
Most Important Security Requirement	Integrity

Table 10. Class Schedule

Critical Asset	Description

Student's Profile	This asset contains the schedule for each class inside the institution, including the lecturer's schedule and the student's schedule
Owner(s)	
Lecturer service, IT	
Security Requirements	
Confidentiality	This data is not confidential, but remains a set of important data and can only be arranged by the lecturer service, followed by submitting to IT
Integrity	This data can only be filled by lecturer service and is given to IT for distribution
Availability	This data can be accessed by everyone inside the institution, both lecturers, students, and employees
Most Important Security Requirement	Availability

Table 11. Lecturer's Profile

Critical Asset	Description
Student's Profile	This asset contains the information of a lecturer that consists of lecturer name, lecturer ID, address, gender, income
Owner(s)	
Lecturer service, IT	
Security Requirements	
Confidentiality	The data is confidential and can only be accessed by the lecturer itself and the lecturer service
Integrity	This data can only be filled by the lecturer service and is inputted by the IT
Availability	This data can only be accessed by the lecturer and the lecturer service for data collection
Most Important Security Requirement	Confidentiality

Table 12. Semester Lesson Plans

Critical Asset	Description
Student's Profile	This data contains the plans for the semester for a subject and contains the outline of a lecture as well as the timeline and the lists of assignments and exams for the students for a subject
Owner(s)	
Lecturer, IT	
Security Requirements	
Confidentiality	This data is confidential and can only be filled by the head of department with the help of a lecturer that will be name the lecturer leader
Integrity	This data can only be filled by the lecturer leader and can be distributed by IT

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Availability	This data can be accessed by the teaching team, as well as the students of a certain subject
Most Important Security Requirement	Confidentiality

3.3. Step 3: Identify Information Asset Containers

In this step, the researcher will identify the asset container of the assets mentioned above. Container in this context is considered as a place where the information will be saved, moved, and processed. There are 3 containers here based on OCTAVE Allegro Worksheets, namely technical container, physical container, and people.

Technical containers are usually the hardware, software that is under the control of the organization and beyond the control of the organization. Physical containers are the physical location of the document that is under the organization's control and beyond the organization's control, while people here are the people who know about the information inside and outside of the organization.

Based on the interview, the researcher has listed the technical container to database and web server that is hosted by Kalbis Institute and the system is maintained by the institution. For physical containers, there are a few locations inside the institution that houses the data in their physical form, but there are also data that does not have a physical form, these data are stored digitally and only exists inside the system. These data are student's absence, student's grades, class schedule, and semester lesson plans. Whereas the people container here are the people who know about the information and who has the access to the information.

In this research each information asset gets the same 3 containers for each of them. Each asset has their own internal and external containers and owners. For example, the student profile a database and web server as the internal technical container and both are owned by the IT, while there are no external containers for this. For physical containers, there is the student's form for internal that is owned by the admission and the student services. For people, there are admission staff, IT staff, student services staff, and lecturer for internal people who know the student, while there are a few external personnel such as other students, the student's parents, and the foundation.

For student's absence, the internal technical containers are database and web server which are both owned by the IT and no external technical containers. There are no internal and external physical containers for this because it's done digitally. The people who know this information assets are the IT staff, the lecturer service staff, the student service staff for internal and the foundation for the external personnel.

For student's grades, the internal technical containers are database and the web server that is owned by the IT, with no external technical containers. The internal physical container for student's grades is the student's exam and the student's assignment, while there is no external physical container. The internal personnel for student's grades are student service staff, IT staff, lecturer service staff and for external personnel there is the foundation.

For class schedule, the internal technical containers are database and the web server that is owned by the IT and no external technical containers. The internal physical container for class schedule is the teaching assignment letter and there is no external physical container. The internal personnel for class schedule are lecturer service staff, IT staff, the lecturer for the subject, while the external personnel are the students and the foundation.

For lecturer's profile, the internal technical containers are database and web server which are owned by the IT, with no external technical containers. The internal physical container for lecturer's profile is the lecturer form which is owned by the lecturer service and the employee form that is owned by the human resource division, while the external physical containers are the employment data form which is owned by the minister of labor and teaching form which is owned by the minister of education. For internal personnel, there are lecturer service staff and the human resource staff, while the external personnel for this information are the minister of education staff, the minister of labor staff, students, and the foundation.

For semester lesson plans, the internal technical containers are database and web server that is owned by the IT, with no external technical containers. There is also no internal and external physical container, because of the digitalization of the information. For internal personnel, there are lecturer service staff, IT staff, Head of department, and the lecturer of the subject, with external personnel for this information are the students and the foundation.

3.4. Step 4: Identify Areas of Concern

In this step, the researcher will identify the areas of concern based on the organization. To identify, the researcher must first do a brainstorming session to understand the conditions and the situations that can create a risk to the organization. The steps to identify the areas of concern are described as follows:

1. Review the containers that is described in the step above and find the possibility or chance that the container can cause a risk
2. Risk documentation for risk that can occur in each container
3. Based on the risk that occur, the researcher will explore the risk area

4. After identifying the risk area, the next step is to analyze how the risk can occur and which security requirements is violated
5. Repeat step 1 to 4 for each container and collect the results for each container

Based on the steps above, the researcher will identify what kind of risk that are contained inside each container. Each container will be reviewed and will have at least one risk that can occur, then the risk will be documented, and each risk will be converted into a curtain specific scenario. Therefore, in this step, there will only be the scenario of how the risk can occur and what kind of risk that occurs based on the containers describe before. Table 13 below describes the areas of concern for all the containers above.

Table 13. Area of Concerns

Ref Num	Area of Concern
1	An error occurred when inputting the student's personal data into the system
2	Access for the student differs from other students
3	An error on web server so that it can't be accessed
4	Student form lost when returning the form to the institution
5	An error when giving student account
6	An error on system security which results in the data cannot be taken
7	Cyber-attack on data center
8	Intentional dissemination of data to other parties
9	Users forget to logout after logging in public places
10	An error on the system when system has received an update
11	An error occurred when inputting student's absence into the system
12	Error on system when inserting absence
13	Access error for curtain menu
14	An error occurred when inputting the student's grades
15	An error on the system that results in exchange of grades between students
16	An error occurred when inputting the class schedule
17	An error occurred that results in wrong schedule for lecturer/students
18	An error occurred when inputting lecturer's personal data into the system
19	Employee form lost by the Human Resource department
20	An error when giving access to lecturer
21	Intentional distribution of lecturer data to other parties
22	An error occurred when inputting the semester plan to the system
23	The given course material given to the lecturer is not in accordance with the latest conditions
24	The given material differs the supposed material

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.5. Step 5: Identify Threats Scenarios

In this step, the researcher will identify the threat scenarios that are based on the areas of concern that is listed in the step before. Each scenario in this step will be a simulation that can happen and cause damage to the organization. The purpose of this step is to identify what are the threat and the actor that is involved inside the threat scenario. Each scenario that is listed Table 14 below contains the threat scenario based on the areas of concern above, reach ref number in this table represents the same number for the area of concern.

Table 14. Threat Scenario

Ref Num	Area of Concern
1	The officer accidentally made an error when inputting into the system and the lack of validation or confirmation before submitting
2	The officer accidentally made a mistake when granting access to the student
3	An error inside the system inside the server that is caused by a setting that is misconfigured
4	The officer lost the form when collecting the stack of forms from the admission
5	The officer gave the wrong account to the students
6	Misconfiguration of the firewall inside the system on the server
7	Misconfiguration of the server and the security of the server
8	The officer makes copies of the data of a student and shares with other parties
9	The student didn't logout from the system when accessing the system from public devices
10	An error when there is an update to the existing system
11	The officer accidentally made a mistake when inputting the student's absence
12	A system error when inputting the absent and submitting to the system
13	The officer has accidentally given the wrong access to a curtain user and the lack of confirmation before submitting
14	The officer accidentally made a mistake when inputting the student's grade and the lack of validation or confirmation before submitting
15	A system error when processing the data on submit
16	The officer accidentally made a mistake when inputting the class schedule and the lack of validation or confirmation before submitting
17	A system error when selecting the data for a curtain user
18	The officer accidentally made a mistake when inputting the lecturer's data and the lack of validation or confirmation before submitting
19	The Human Resource officer misplaced the employee form
20	The officer has accidentally given the wrong access to the lecturer

21	The officer created copies of the lecturer's personal data and share to other parties
22	The head lecturer made a mistake when inputting the study plan and the lack of confirmation before submitting
23	The head lecturer uses the same material and there is no review from the head of department
24	The head lecturer made a mistake when inserting material of a subject and there is no review from the head of department

3.6. Step 6: Identify Risks

In this step, the researcher will analyze the threat scenario from the previous step to find the risk that can occur. This step will list the risks and the consequences that can occur.

The risks and consequences will give different impacts and different implementation of mitigation. Each risk has their own consequences for the actor or to the institution. The next step will analyze the risks that is listed in this step and do a calculation for understanding which one should be prioritized and what's the impact to the organization. Table 15 below is the list of consequences for each area of impact.

Table 15. Risk Consequences

Ref Num	Area of Concern
1	The students assume the officer didn't read the form The process of data change will take some time and will be a long process
2	Loss of trust to the IT Department for the mistake Difficulties for students to access the required data
3	Disappointment with IT for access error Difficulties for accessing the required data The system is inaccessible for the time being
4	Loss of trust to the admission staff to fulfill their duty Difficulties to insert the student's personal data to the system A delay in entering students into a batch
5	Difficulties for students entering the system The student cannot see the class schedule for subjects in the semester
6	Loss of trust to the IT Department The possibility of data loss by outside parties The possibility of the data being used for other personal purposes
7	Loss of trust to the IT Department System will be inaccessible The possibility of data loss by outside parties
8	Kalbis Institute's reputation questioned Data leak

	The possibility of paying fines and legal penalties
9	The possibility the system can be used by other people other than the designated student
	The possibility of password change, which results in the student unable to login
10	System inaccessible to the user
	The possibility of features that cannot be accessed
	Changes in the user access
11	The possibility of a student cannot take the exam for a subject if the absence count is more than 3
	The possibility a student must repeat the course
	The process of data change will take some time and will be a long process
12	Loss of trust to the IT Department
	Difficulties to access the required data
	System inaccessible for the time being
13	User cannot access the menu
	User cannot change or do actions for the menu
14	The possibility of a student failing a subject
	The process of data change will take some time and will be a long process
15	The possibility of a student failing a subject
	The possibility of changing the source code to fix the problem
	The process of data change will take some time and will be a long process
16	The possibility of class clashes for lecturer and students
	The class schedules differ between students in the same class
	The process of data change will take some time and will be a long process
17	Lecturers experience teaching schedule clash with other classes caused by schedule changes
	Students experience schedule changes
	The possibility of changing the source code to fix the problem
	The process of data change will take some time and will be a long process
18	Lecturer's data will differ from the one sent to the institution
	The process of data change will take some time and will be a long process
19	The form is lost to the human resource division
	A delay for processing the lecturer's data
	The possibility of the lecturer filling the data again and resubmit to human resource
20	The lecturer cannot access their data
	The possibility of data mismatch between lecturers
	The process of data change will take some time and will be a long process
21	Kalbis Institute's reputation questioned
	Data leak and the possibility of policy review

	The possibility of paying fines and legal penalties
22	The lecturer will teach a topic with the wrong guidance and doesn't align with the subject
	The students will receive a different topic that doesn't align with the subject
	The process of data change will take some time and will be a long process
23	The lecturer will teach a topic that isn't up to date to the students
	Students will learn a topic that isn't up to date
24	The lecturer will teach a topic that doesn't align with the subject
	The students will receive a topic that doesn't align with the subject

3.7. Step 7: Analyze Risks

In this step, the researcher will do a calculation based on the risk and consequences identified in the previous step. The scoring will be a measurement of how big the risk to the organization is.

The score of each impact is calculated based on the impact areas in the first step each impact area will be given a representation of low, moderate, and high, with each representation will be given the value of 1, 2, and 3. The value for each representation will be the value of the priority multiplied by the value of the representation. Table 16 below will determine the score for each impact area.

Table 16. Risk Scoring

Priority	Criteria	Low	Moderate	High
3	Reputation and Customer Confidence	3	6	9
5	Financial	5	10	15
4	Productivity	4	8	12
1	Safety and Health	1	2	3
2	Fines and Legal Penalties	2	4	6

3.8. Step 8: Select Mitigation Approach

In this last step, the researcher will categorize reach risk that is defined in the last step and will decide if the risk should be mitigated, deferred, or accepted by the organization. Table 17 below is a relative risk matrix, a tool to categorize the risks that has been listed above into categories based on their relative scores.

Table 17. Relative Risk Matrix

Risk Score Range		
> 30	**21 – 30**	**0 – 20**
Category 1	Category 2	Category 3

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Based on the categories on table 17 above, there are 3 categories based on their relative score. Category 1 is for risks that must be mitigated and is top priority, while category 2 is for risks that must be discussed with top level management for further actions (deferred) and has a moderate priority, and lastly category 3 is for risks that can be accepted by the organization and has a low priority. Table 18 below, is the approaches are what the researcher recommends.

Table 18. Area of Concerns

Ref Num	Action	Area of Concern
1	Defer	Confirming with top management first, then, if possible, add validation on the form and add confirmation to ensure the officer has inputted and is ready to submit the data
2	Defer	Confirming with top management first, then, if possible, add confirmation to ensure the officer has inputted and is ready to submit the data
3	Defer	Confirming with top management first, then, if possible, set a monitoring system to the server or find another server for the system
4	Defer	Confirming with top management first, then, if possible, add a procedure on how to store the forms and the location of storing and after submitted
5	Defer	Confirming with top management first, then, if possible, add procedure to recheck the student's name on the account and the name of the student receiving it
6	Mitigate	Apply best practice for programmers and have a development standard Perform a penetration test when testing a system before deploying to production Perform a recheck on firewalls and policy on the servers and the network Perform a system security audits on a regular basis
7	Mitigate	Perform a system security audits on a regular basis Perform a recheck to the firewalls on the server Perform a duplication to a server to prepare a backup server
8	Mitigate	Perform a distribution to the student services with and do a recheck there Perform distribution to the students from student services transparently
9	Defer	Confirming with top management first, then, if possible, do a session to help the students understand about the importance of data privacy

10	Defer	Confirming with top management first, then, if possible, do a thorough testing to the implementation and the system flow to ensure the system works perfectly
11	Accept	Consider adding additional validation and confirmation when submitting the student's absence
12	Defer	Confirming with top management first, then, if possible, recheck the system internally and retest to ensure the system is working, if it's not working properly then update and test before deploying to production
13	Accept	Consider adding confirmation to the officer when submitting access to a curtain user
14	Accept	Consider adding validation and confirmation before submitting the form
15	Accept	Consider rechecking the application and retest before deploying to the production server
16	Accept	Consider adding validation and confirmation before submitting the form
17	Accept	Considering adding confirmation as a reminder to recheck the data before submitting
18	Accept	Consider adding validation and confirmation before submitting the form
19	Defer	Confirming with top management first, then, if possible, add a procedure on how to store the forms and the location of storing and after submitted
20	Accept	Consider adding confirmation to the officer when submitting access for a curtain lecturer
21	Mitigate	Perform a distribution to the lecturer services with and do a recheck there
		Perform distribution to the lecturers from lecturer services transparently
22	Accept	Consider adding confirmation to the head of teaching team when submitting semester plans to the system
23	Accept	Consider creating a team to review the material for a subject and see if it aligns with the current condition and is relevant to the subject
24	Accept	Considering the material with a specific topic and have a recheck before submitting to IT

Based on the results above we can conclude that there are 24 risks inside the institution and OCTAVE Allegro has helped the researcher to reveal the risk assessment. Based on the risk assessment, there are 4 risks that must be mitigated, 9 risks that are must be discussed with the top management, and 11 risks that are

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

accepted by the institution. These risks have been identified using the OCTAVE Allegro method that is used in this research. During the research, the researcher has indicated that this study is focused on the academic information system of the institution. This risk assessment has been received from 6 information systems inside the institution, namely: student's profile, student's absence, student's grades, class schedule, lecturer's profile, and semester lesson plans.

Based on the analysis above, the researcher can conclude that there are 2 aspects that are critical to the institution that are people and the system itself. The researcher has also made 4 recommendations to help prevent the possibility of a risk on the system's side, namely:

1. Perform a routine security audit
2. Create a policy for source code standardization
3. Recheck firewall configuration on the network
4. Ensure that every user access to the system is controlled and make sure that each actor inside the system has their own access based on their role

Whereas for the people's side, the researcher has concluded that there are 3 recommendations, namely:

1. Ensure that every person has their training on awareness of account security
2. Ensure that everyone that uses the system understand the procedures tied to the system
3. Use the access given to each user to access the corresponding data based on their roles inside the institution.

The recommendations above are simply to help the institution to understand better about the risks that can happen and the impact that each risk possess. These risks are simply part of the information system, so there are always going to be risks big or small inside the institution.

4. CONCLUSION

Based on the initial aim of this research, there have been a risk assessment towards the information system of Kalbis Institute. The OCTAVE Allegro method used in this research is one of the many ways of defining a risk assessment without direct involvement inside the organization. There are 8 steps inside the OCTAVE Allegro method and each method has helped the researcher to understand the risk assessment. Based on the results, there are 2 main aspects inside this organization that is important which are people and the system itself.

This research has been strictly focused on the academic information system inside Kalbis Institute and to understand the risks that is faced by the institution. The

results state that there are at least 24 risks that have been identified and has also given its mitigation strategies.

There is always room for improvements and based on this research alone there are a few improvements to be made such as performing yearly risk assessments, have a backup plan for the system, make sure that the hardware is well maintained, make sure every actor has their right accesses.

REFERENCES

[1] R. K. R. Jr, B. Prince, and C. Cegielski, *Introduction to Information Systems: Supporting and Transforming Business*. Don Fowley, 2014.
[2] P. Hopkin, *Fundamental of Risk Management, 4th Edition*, no. 1. 2017.
[3] C. Rowe, "What is Risk Management?" https://www.clearrisk.com/what-is-risk-management (accessed Apr. 02, 2021).
[4] 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.
[5] J. Hom, B. Anong, K. B. Rii, L. K. Choi, and K. Zelina, "The Octave Allegro Method in Risk Management Assessment of Educational Institutions," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 167–179, 2020, doi: 10.34306/att.v2i2.103.
[6] 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.
[7] C. Alberts and J. Stevens, "Introduction to the OCTAVE approach," no. August, pp. 121–129, 2010, doi: 10.1016/b978-0-7020-3055-0.00004-2.
[8] R. a R. a. C. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," *Young*, no. May, pp. 1–113, 2007.
[9] S. Amraoui, M. Elmaallam, H. Bensaid, and A. Kriouile, "Information Systems Risk Management: Litterature Review," *Comput. Inf. Sci.*, vol. 12, no. 3, p. 1, 2019, doi: 10.5539/cis.v12n3p1.
[10] D. H. Stamatis, *Introduction to Risk and Failures*. 2014. doi: 10.1201/b16855.
[11] D. Landoll, *The Security Risk Assessment Handbook*. 2016. doi: 10.1201/b10937.
[12] E. Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*, vol. 31, no. 2. 2012. doi: 10.1016/j.cose.2011.12.011.