International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 2
ISSN: 2088-5334

An Information System Risk Management of a Higher Education Computing Environment

Artika Arista [a,*], Khairun Nisa Meiah Ngafidin [b]

[a] *Department of Information Systems, Universitas Pembangunan Nasional Veteran Jakarta, Pondok Labu, South Jakarta, Indonesia*
[b] *Department of Information Systems, Institut Teknologi Telkom Purwokerto, Banyumas, Jawa Tengah, Indonesia*
*Corresponding author: *artika.arista@upnvj.ac.id*

***Abstract*— Cyber risks, data loss or data leakage, loss exposure are one of the most customer and business significant threats. Those data contained information and were stored in electronic form that made them vulnerable to be hacked. The major target of hackers intruding is the higher education institutions. Therefore, many organizations perform information system risk management to identify their weaknesses and enforce the security of their system. The study aims to identify, analyze, and measure the risks associated with information systems specifically evolve in the higher education sector environment. Then it provides solutions and recommendations for the higher education sector to improve the quality of their information systems. Information system risk management was performed in the computing environment of the Faculty of Medicine, X University. It was conducted using the OCTAVE Allegro framework. The framework can streamline and optimize the information system risk management process through eight steps and various worksheets and questionnaire sheets for guidelines. After completing all the required data, the analysis was conducted to determine the critical information assets for the organization. The results showed that there were 8 (eight) critical information assets. One of them is the Student Profile. It was continued to be assessed using a chronological approach of information system risk management for improving security awareness and formulating mitigation strategies as the control actions. This paper's analysis and results are expected to contribute to the implementation of information system risk management for real case applications in different sectors.**

***Keywords*—Information system risk management; OCTAVE Allegro; higher education sector.**

Manuscript received 10 Dec. 2020; revised 28 Apr. 2021; accepted 24 Jun. 2021. Date of publication 30 Apr. 2022.

I. INTRODUCTION

Nowadays, business movement is inseparable from the role of technology, especially the information system (IS) and information technology (IT). IT and IS plays an important role in supporting every transaction, decision-making, reporting, analysis, controlling, security, business strategy, service quality, and business processes [1]. Cyber risks, data loss or data leakage, loss exposure related to electronic data on computers, virtual reality, and information technology are one of the most customer and business significant threats. As a result of cyber risks, digital data and information can be exposed to confidentiality and integrity loss either deliberately or incidentally [2]. Those data contain financial, customer or health information are stored in electronic form that made them vulnerable to be infected by viruses, malware, tracking software, or hacked [3].

In 2019, 39% of EU people who accessed the Internet had security concerns in cyberspace. This indicator has a wide range of values in different member states, ranging from more than 50% in the United Kingdom to 10% in Lithuania. Confidential data may be utilized for unlawful activities or sold on dark websites in the event of an information security breach, resulting in a loss of business reputation for both financial institutions and their clients [4]. The risks of the data leakage or data breaches are also related to potential financial loss and create a future injury risk such as fraud, identity thief, blackmail, intellectual property thefts, or damaged reputations) [5], [6]. Due to an increase in the frequency of losses among private institutions, there is a need for systematic management so that risk can be adequately managed. Risk management is something that the Board of Directors (BODs) and its members should be aware of. The justification for having this kind of knowledge is that it may help institutions reduce uncertainty [7].

Today's universities are inseparable from the development of computing and network applications. Universities are now equipped with high-end technological infrastructures. These advancements result in more valuable support for the learning environment. Every advancement is also having potential risks, such as security threats and a vulnerable computing environment. The technological advancement provides university campuses with the most technologically advanced facilities such as a digital library, web conferencing, extensive Wi-Fi support, classroom virtualization, online learning, etc. Besides the high technological advancement that creates university faculty's computing environment, there is also a highly vulnerable environment. As we can see recently, the hacking targets are organizations such as banks and large open networks such as university and college computing environments.

It is a huge challenge for protecting and managing a large open network such as university faculty's computing environment against evolving threats and vulnerabilities. The open computing university network environment supports different users such as students, administration, and faculty. These types of users have access to university resources at varying levels. Therefore, university faculty's campus network environment must be protected from vulnerabilities and security breaches to ensure only secure access is provided to users [8].

Despite the growing fears of cyber risks, only a few studies have been published on determining and assessing the harm and impact of the cyber risks [9]. Therefore, there is a need for identifying risk-related information systems to improve security effectiveness in the Faculty of Medicine campus network. This paper proposes OCTAVE Allegro's information system risk management framework to identify, analyze, and measure the risks and security dangers associated with information systems present in the computing environment of the faculty of Medicine, X University. First of all, it requires operational critical threat identification. The proposed model assesses the security risks qualitatively by identifying potential threats and information processes inside the university faculty's computing environment. Then, it continues with a vulnerabilities assessment to measure the risk level. The last one is offering mitigation solutions and recommendations. For better results, it is also supposed to be followed by continuous monitoring of the computing environment of the Faculty of Medicine, X University. These studies are expected to contribute to risk analysts and security managers of different institutions to carry out a realistic and affordable information system risk management for different sectors.

II. Materials and Method

A. Information System (IS)

An information system is a collection of people, hardware, software, network communications, and data resources that work together to collect, process, and disseminate information inside an organization for specified goals [10]. The information systems can be characterized as a collection of interconnected pieces that flow information in a systematic and consistent manner to and from the company's activities, as well as assisting managers and employees in problem-solving, visualizing a complex issue, and developing new products [11]. The information systems are the foundation utilized as support for the company's business strategy in order to improve the quality of services and business operations, in order to meet the company's business goals [12].

B. Risk

A risk is a potential of an unfavorable event occurring or the absence of the desired event [13]. Risk is defined as the influence of uncertainty on desired objectives, expressed as a positive or negative divergence from the expected outcome[14]. Once risks have been identified, they must be evaluated for their possible degree of impact (i.e., damage or loss) as well as their likelihood of occurrence [15]. Risks can have an impact on an organization's financial performance, business continuity, reputation, environmental, and social outcomes; as a result, risk management assists organizations in achieving their goals, reducing potential losses, and exploring new opportunities in an uncertain environment. As a result, many types of businesses are becoming more interested in risk management [14].

C. Risk Management

Risk management is a continuous process that involves setting goals, recognizing sources of uncertainty, calculating the likelihood and severity of alternative outcomes, and creating managerial responses to risks and opportunities. The goal of risk management is to lower the likelihood of risks and to lessen the effect of potential losses [14]. To do so, you'll need to create and maintain an organizational structure, processes, and resources that are focused on detecting, assessing, managing, and monitoring risks [16].

A risk management strategy based on a process approach that identifies probable causes and consequences in a systematic manner. To model uncertainty bounds for risk assessment and specific risk of activities in the contextual setting, key parts of standards and risk management are used [17]. Effective risk management should be a holistic, systemic, and scientifically based process that builds on formal risk assessment and management [18]. Risk identification, risk analysis, risk prioritizing, risk resolution, and risk monitoring are the five steps of a commonly acknowledged risk management approach [13].

D. Information System Risk Management

A continuous cycle of risk detection, evaluation, and prioritizing characterizes an information system risk management process. Information system risk management is a procedure that guarantees that employees in charge of information systems have a high level of awareness. Information system risk management not only develops employee awareness, but also provides an atmosphere where problems linked with weaknesses and dangers are routinely solved. The reduction of risks to a level of acceptability is one of the specific priorities for certain dangers. The other options are risk mitigation, risk transfer to a third party, risk avoidance, and risk acceptance. It is feasible to limit the frequency and severity of risk-related incidents in the system with adequate information system risk management [15]. It can be seen that the four primary functions of information

system risk management are consistent across sectors, with risk identification, risk analysis, risk assessment, and risk management being the four key functions [19].

E. Octave Allegro

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a collection of techniques, methods, and tools for assessing information security risk assessment. OCTAVE is a security framework for assessing risk and preparing defenses against cyber-attacks, with a primary focus on: a) assisting organizations in minimizing their exposure to likely threats, determining the likely consequences of an attack, and dealing with successful attacks; and b) leveraging the experience and expertise of people within the organization [20]. This framework was developed through a CERT program developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. The key benefit of OCTAVE is that it connects organizational goals to risk assessment and vulnerability management. OCTAVE is designed to be a flexible strategy that can be tailored to the needs of any institution's IT and business departments [21]. The latest version of the OCTAVE framework is the OCTAVE-Allegro. The OCTAVE-Allegro is specifically used to conduct information security risk assessments. Without extensive risk assessment knowledge, an organization can carry out a broad operational risk assessment using the OCTAVE-Allegro. This OCTAVE-Allegro framework is using a different approach from the prior OCTAVE.

The OCTAVE-Allegro focuses more on information assets, especially where the data are stored, transported, and processed, how the data are used, and how the data are exposed to threats, potential vulnerabilities, and disruptions. There are several options to perform the OCTAVE-Allegro framework such as a collaborative setting with guidance, worksheets, as well as a questionnaire or workshop style. However, the OCTAVE-Allegro is also suitable for individual use without extensive organizational involvement, expertise, or input to perform the risk assessment process [1].

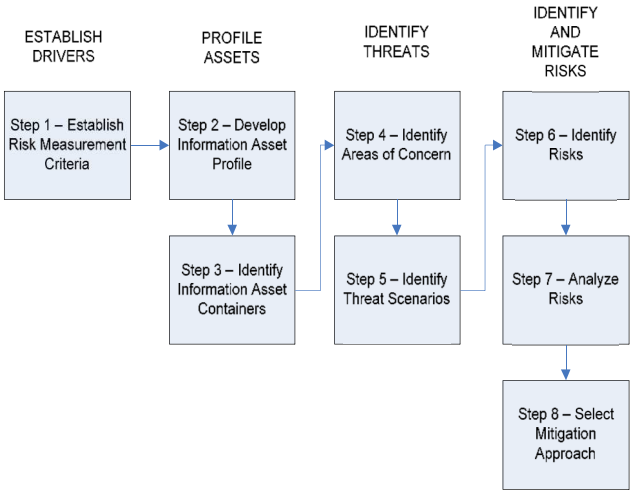

Fig. 1 OCTAVE Allegro Roadmap [1]

OCTAVE-Allegro describes how to assess risks in an organization or, more specifically, an asset in an organization using eight steps and various worksheets and questionnaire sheets for guidelines. OCTAVE Allegro contains eight steps consisting of four phases, as illustrated in Figure 1. Starting from the first phase, the organization builds up risk measurement criteria under the organizational drivers. In the second phase, create an asset profile for critical information. The profiling process identifies security requirements and determines the asset locations (where they are stored, transported, and processed). In the third phase, information assets are identified in asset locations (where they are stored, transported, and processed). In the final phase, identifying and analyzing the risk of information assets and the formulation of mitigation strategies.

The main goal of designing a security risk assessment framework is "security controls should be selected based on real risks to an organization's assets and operations". The proposed model is based on OCTAVE Allegro, the most popular risk management framework currently in use. The framework aims to measure and assess risk levels quantitatively. Thus, it can help the institution to understand security risks.

In the OCTAVE Allegro framework, there are four different activities carried out through eight steps. Here are the activities:

- The organization develops risk measurement criteria under organizational drivers.
- The organization establishes a critical information assets profile and identifies the assets' containers.
- The organization identifies threats and records them in a structured process.
- Organizations identify and analyze the risks based on threat information and formulate mitigation strategies to control and minimize the risks.

This research performs a practical approach in a real organization environment using eight steps activities from the OCTAVE Allegro framework. The research aims to identify and analyze the possibility of security violations, realize the causes that make the system vulnerable, and formulate mitigation strategies to control and minimize the risks. The primary focus of the conducted risk management is understanding the security weakness of university faculty's computing environment, Faculty of Medicine and then focusing on which areas with the highest risks from risk scoring results. The last step is creating a remediation plan for the faculty of Medicine environment. The aim of assessing the faculty of Medicine computing environment is to collect input regarding vulnerabilities and threats and result in quantitative risk level measurement and remediation.

III. Result and Discussion

Assessing information system risk at the Faculty of Medicine, X University, started by explaining the aim of the assessment with the IT Officer. Then, it continued by obtaining the required data. The interview process is carried out to find out the important information assets of the academic operation. The OCTAVE Allegro method, which consists of eight steps, performs the information system risk management process. The activity for conducting the assessment processes follows the OCTAVE Allegro road map illustrated in Figure 1. Every output from each step was documented on a series of worksheets. Then it was used as

input to the next step. The series of assessment processes are explained in more detail below.

A. Step 1: Establish Risk Measurement Criteria

This step was begun by interviewing the IT Officer Faculty of Medicine, X University. Then, it continued by determining risk measurement criteria from the results of the interview. This step consists of two activities, (1) determining the impact area, and (2) setting the impact area priorities. The faculty of Medicine, X University's business objectives and mission are considered in determining the impact area. The determined impact area is safety and health, fines and penalties, productivity, financial reputation, and customer confidence.

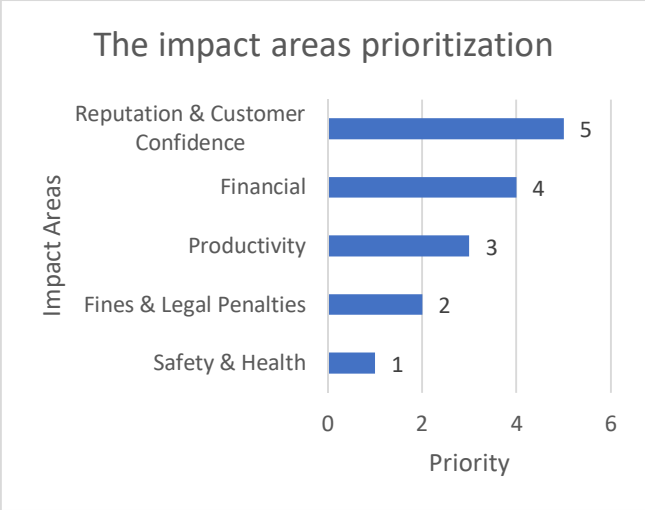

Fig. 2 The impact areas prioritization

Based on all aspects determined, the highest priority of the Faculty of Medicine, X University is reputation and customer confidence. These aspects are the most important factor influencing prospective decisions when shortlisting universities was a good academic reputation. The prestige or reputation for an institution quality is often more important than its actual quality because it represents the perceived excellence of the institution. It guides prospective students' decisions to enroll in the institution. Universities have been attempting to stimulate customer/student participation in building and delivering their university experiences by providing a wonderful university computing environment in order to provide a unique and memorable student experience [22]. Therefore, the more the admission number of the Faculty of Medicine, X University increases, the more likely they are to increase financial income. If a significant issue caused a fine and legal penalty for the faculty, reputation, customer confidence, financial areas, and faculty productivity are affected. The faculty cannot operate well. This condition impact safety and health because the faculty was unable to serve a safe learning environment.

B. Step 2: Develop an Information Asset Profile

It is necessary to relate with the Faculty of Medicine, X University core processes when selecting critical information assets. The core process of the Faculty of Medicine, X University are as follows:

- Education
- Admission
- Regulation and scheduling
- Teaching and learning
- Examination evaluation, thesis, and graduation
- Alumni, career development, and entrepreneurship program.

All critical information assets obtained were documented on the OCTAVE Allegro critical information asset worksheet. The important consideration for selecting critical information assets are:

- The Faculty of Medicine, X University is the most valuable asset.
- The information assets for daily operations and processes.
- If the information asset is lost, it significantly disturbs its ability to fulfill its business objectives and mission.

The classified critical assets from the above considerations are:

- Student Profile
- Lecturer Profile
- Course
- Student Score
- Class Schedule
- Lecturer Attendance
- Payment of Tuition
- Curriculum

TABLE I
INFORMATION ASSET PROFILE OF STUDENT PROFILE

Critical Asset		Student Profile
Rationale for Selection		Students have an important role in the business processes in the Faculty of Medicine, X University core process. The student profile itself is used almost in every process in Faculty of Medicine itself. Student profiles that are recorded and used are the data obtained from the process of new students' admission until student's graduation.
Description		This asset consists of students' personal data, such as registration number, student number, name, address, religion, study program, semester, class, cellphone number, email etc.
Owner		IT Division
Security Requirement	**Confidentiality**	Information about student profiles is privacy for students. This information is only given access to certain parties to help students and prevent misused by irresponsible parties, such as student affairs, admissions, and the academic department.
	Integrity	Information about student profiles must be relevant to the real conditions, and the student courses are taken status. The admission fills in the information, and if there is a modification, and revisions can be made by contacting the academic department.
	Availability	Information should be available to students, student services, and academic departments.

Critical Asset	Student Profile
Most Important Security Requirement	**Integrity** Information about student attendance must be under the real conditions because this student profile is widely used during studies for various purposes. If it provided false information, students would not be able to take the exam, affecting the completion of their studies.

C. Step 3: Identify Information Asset Containers

A container for storing, transmitting, or processing information assets is called Information Asset Containers. On the worksheet for the asset information risk environment map, the container can be classified based on 3 (three) categories:

- Technical. Technical assets include hardware (CPU, data storage, and RAM), software (application systems, DBMS, cloud storage), servers, and networks (technology assets), which the organization controls (internal) or outside the control of organizations (external).
- Physical. The physical object includes file folders (where written form information is stored) or documents or the physical location of information assets both inside and outside the organization.
- People. People include internal or external (who carry important information such as intellectual property) from organizations with detailed information assets.

TABLE II
INFORMATION ASSET CONTAINERS (TECHNICAL) – STUDENT PROFILE

Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Palawa: A student's academic information system for storing student academic data.	Academic department
Gamel: An academic information system for Faculty of Medicine students only that used for academic learning.	IT department Faculty of Medicine
Elisa: An e-leaning system for students.	Academic department
External	
Container Description	**Owner(s)**
Internet. Student profile data was accessed using internet electronically.	unknown

TABLE III
INFORMATION ASSET CONTAINERS (PHYSICAL) – STUDENT PROFILE

Information Asset Risk Environment Map (Physical)	
Internal	
Container Description	**Owner(s)**
The student profile printed version that kept for academic department documentation.	Academic department
External	
Container Description	**Owner(s)**
The student profile printed version that kept by student.	Academic department

TABLE IV
INFORMATION ASSET CONTAINERS (PEOPLE) – STUDENT PROFILE

Information Asset Risk Environment Map (People)	
Internal Personnel	
Name or Role / Responsibility	**Department / Unit**
IT unit Staff Faculty of Medicine	IT department Faculty of Medicine
Academic Staff	Academic department
IT Staff	IT department university
External Personnel	
Name or Role / Responsibility	**Department / Unit**
Student	Student

D. Step 4: Identify Areas of Concern

The following activities that need to be carried out for identifying the areas of concern including:

- To see the area of concern potential, it is necessary to review each container.
- Using Information Asset Risk Worksheet to document each areas of concern.
- Establish threat to scenarios using the area of concern extension.
- Document each threat and how it affects the information asset security requirements.
- Run on each container on Information Asset Risk Environment Maps and archive areas of concern as much as possible.

TABLE V
AREA OF CONCERN - STUDENT PROFILE

No	Area of Concern
1	Due to a large number of student profiles, there were errors in data input by Academic staff.
2	Bug/error found in Palapa, Gamel & Elisa that arises when IT staff performs maintenance.
3	A possibility of vulnerability attack by internal/external parties in Palapa, Gamel & Elisa application.

E. Step 5: Identify Threat Scenarios

According to the Information Asset Risk Worksheet, it is necessary to develop threat scenarios in each area of concern to specify the nature of the threat.

TABLE VI
THREAT SCENARIOS – STUDENT PROFILE

Area of Concern	Threat Scenario	
Due to a large number of student profiles, there were errors in data input by Academic staff.	**Actor**	Academic staff
	Means	Staff using Palapa
	Motives	Accidentally occurs (human error possibility)
	Outcome	Modification, Interruption
	Security Requirements	Add a validation function to the fields entered by the staff. If necessary, do training to reduce errors.

Area of Concern	Threat Scenario	
Bug/error found in Palapa, Gamel & Elisa that arises when IT staff performs maintenance.	**Actor**	IT staff
	Means	Access in modifying Palapa, Gamel & Elisa application
	Motives	Accidentally occurs (human error possibility)
	Outcome	Modification, Interruption
	Security Requirements	Strengthen the control of testing and QA before deployment.
Area of Concern	**Threat Scenario**	
A possibility of vulnerability attack by internal/external parties in Palapa, Gamel & Elisa application.	**Actor**	Unknown
	Means	Vulnerabilities on databases, servers, and application modules are identified and exploited by inside or outside parties.
	Motives	Third parties either inside or outside want to change or harm the database, application modules, and server.
	Outcome	Destruction, Interruption, Disclosure, Modification
	Security Requirements	To avoid any kind of system infiltration and damage, it is necessary to enhance the software, hardware, and networks security and continuously monitor system security loopholes.

F. Step 6: Identify Risks

Determine how the recorded threat scenarios can have impacts on the organization by conducting the following activities:

- Determine how Faculty of Medicine, X University would be impacted if the threat scenarios were realized.
- Record the consequences specifically, for example, by considering the evaluated impact areas.

G. Step 7: Analyze Risks

Step 6 and step 7 are closely related steps in which each area of concern for any given asset information is considered as a possible consequence.mIn this step, the consequences are determined. Then, each impact area is assessed by completing the impact value, whether high, medium, and low for the organization. After that, multiply the impact area rank by the impact value to calculate the impact area score. It helped the Faculty of Medicine, X University, to formulate mitigation strategies to control and minimize the risks. The score calculation is illustrated in Table 8.

TABLE VII
THE SCORE CALCULATION FOR THE IMPACT VALUES OF EACH IMPACT AREAS

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

Due to a large number of student profiles, there were errors in data input by Academic staff. Consequences are (1) the Academic department staff or IT staff have to re-input the data & it was wasted time; (2) the students would not be able to take the exam and it would affect the completion of their study. The total relative Risk Score is 41, as shown in Fig. 3.

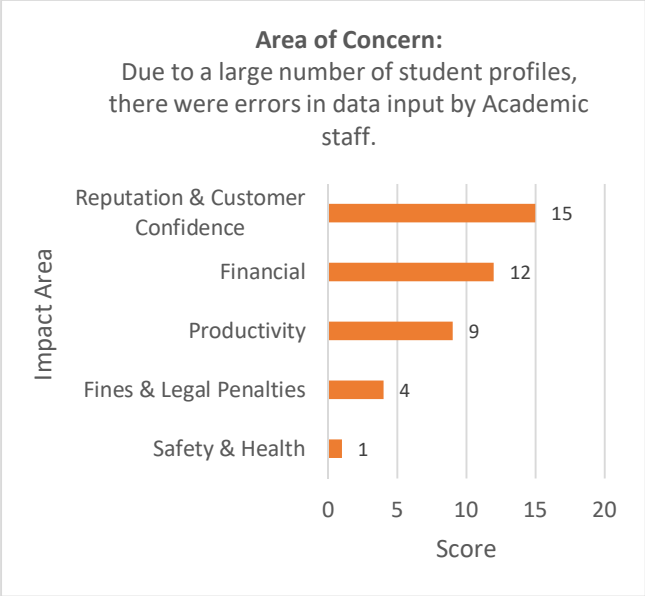

Fig. 3 Risk Analysis Area of Concern 1

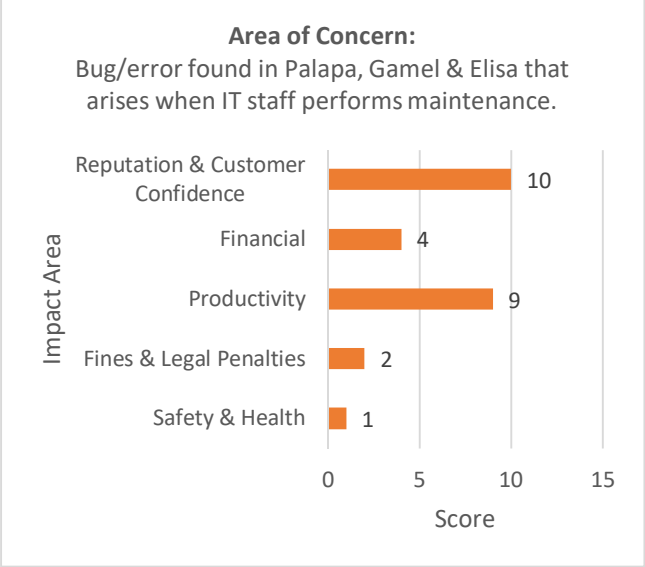

Fig. 4 Risk Analysis Area of Concern 2

Bug/error found in Palapa, Gamel & Elisa that arises when IT staff performs maintenance. Consequences are Bugs/errors made by IT staff during maintenance greatly reduced the productivity of IT and greatly reduced the productivity of IT and users who use related applications. It developed distrust to the application being used. The total relative Risk Score is 26, as shown in Fig. 4.

A possibility of vulnerability attack by internal/external parties in Palapa, Gamel & Elisa application. Consequences are the public's overall opinion of the institution could be affected adversely. The institution's productivity would be also impacted. The total relative Risk Score is 31, as shown in Fig. 5.

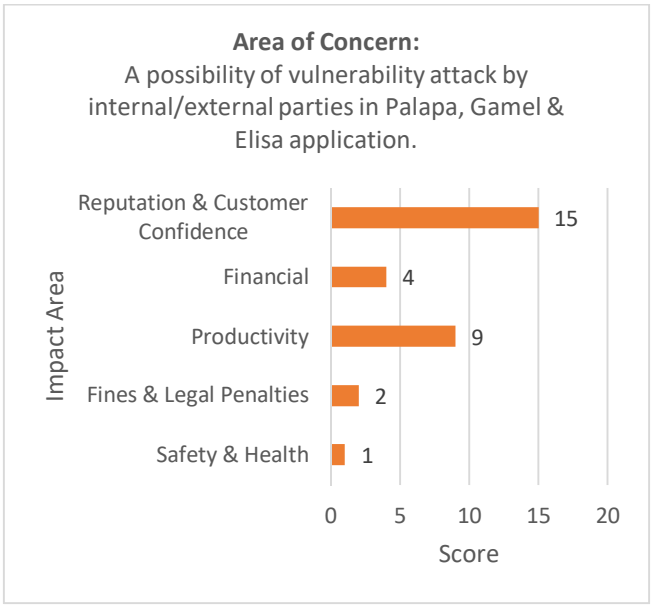

Fig. 5 Risk Analysis Area of Concern 3

H. Step 8: Select Mitigation Approach

The identified risks are sorted by risk score. Then, categorize the risks by sorting them from highest to lowest to help to formulate better mitigation strategies. After that, creating Relative Risk Matrix by separating the risks into three groups with the same number of risks.

TABLE VIII
RELATIVE RISK MATRIX

Risk Score		
35 TO 45	**25 TO 34**	**15 TO 24**
Pool 1	Pool 2	Pool 3

The next activity is deciding the mitigation approach based on pool from the Relative Risk Matrix. If the risk score is high, then it was placed in pool 1. The mitigation approach for pool 1 is mitigated. It explains the need for direct action to try to lessen the seriousness of the risks. If the risk score is medium, then it was placed in pool 2. The mitigation approach for pool 2 is mitigated or defer. It explains the need for direct action or later time action. The final one, If the risk score is low, then it was placed in pool 3. The mitigation approach for pool 3 is accepted. It explains the willingness to accept conditions.

TABLE IX
MITIGATION APPROACH

POOL	Mitigation Approach
1	Mitigate
2	Mitigate or Defer
3	Accept

TABLE X
RISK MITIGATION – STUDENT PROFILE

Area of Concern	Due to the large number of student profiles, there were errors in data input by Academic staff.
Relative Risk Score	41
Pool	Pool 1
Action	Mitigate
Container	**Control**
Palapa, Gamel & Elisa ▪ IT unit Staff Faculty of Medicine ▪ Academic Staff ▪ IT Staff	Add notification for validation entries in the input fields. Each field must be validated before execution to the next process / page. Immediately modify the invalid data if it is known that an error has occurred.
Area of Concern	Bug/error found in Palapa, Gamel & Elisa that arises when IT staff performs maintenance.
Relative Risk Score	26
Pool	Pool 2
Action	Mitigate or Defer
Container	**Control**
▪ IT unit Staff Faculty of Medicine ▪ IT Staff	If it's an important issue, then immediately resolve application bugs/errors or crashes. However, if it's not crucial, then it can be deferred. Ensure the application passes testing and QA before deployment. Control and maintain periodically to ensure the application are free of bug/error and does not crash.
Area of Concern	A possibility of vulnerability attack by internal/external parties in Palapa, Gamel & Elisa application.
Relative Risk Score	31
Pool	Pool 2
Action	Defer
Container	**Control**
Database server and Palapa, Gamel & Elisa	Use/activate the transaction log on network equipment and enforce policies to review the log periodically. Adding features in the application. For example, if the application is idle for more than five minutes, it automatically logs out from the application.

Information system risk management was performed in the computing environment of Faculty of Medicine, X University. It was conducted using OCTAVE Allegro framework. The framework provides the capability to streamline and optimize information system risk management process through eight

steps and various worksheets and questionnaire sheets for guidelines. After completing all the required data, the analysis was conducted to determine the critical information assets for the organization. The results showed that there were 8 (eight) critical information assets, including Student Profile, Lecturer Profile, Course, Student Score, Class Schedule, Lecturer Attendance, Payment of Tuition, and Curriculum.

Student Profile is one of the critical information assets. It was continued to be assessed using a chronological approach of information system risk management for improving security awareness and formulating mitigation strategies as the control actions. Based on the results of the assessment: (1) errors in data input are getting the highest score and need mitigation; (2) while for the bug/error and a possibility of vulnerability attack are in pool 2 (mitigate or defer), where the institution can choose either to mitigate with the mitigation strategies offered or to delay the control actions (but if it disrupts the operation, it should be hastened).

IV. Conclusion

Information system risk management was conducted using OCTAVE Allegro framework. The results showed that there were 8 (eight) critical information assets. Student Profile is one of the critical information assets. It continued to be assessed. Based on the assessment results, there is a need for mitigation strategies offered or the control actions. The analysis and results of this study are expected to contribute to implementing information system risk management for real case applications in different sectors.

Acknowledgment

This work is supported by the Institute for Research and Community Service (LPPM) Universitas Pembangunan Nasional "Veteran" Jakarta (UPNVJ), Faculty of Computer Science UPNVJ, Information Systems Study Program UPNVJ for providing funding support and assisting the implementation of this research.

References

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

[2] G. Strupczewski, "Defining cyber risk," Safety Science, vol. 135, no. December 2020, 2021, doi: 10.1016/j.ssci.2020.105143.

[3] S. A. Talesh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," Law & Social Inquiry, vol. 43, no. 2, pp. 417–440, 2018.

[4] P. J. O. Management Studies Kuzmenko, O. v Kubálek, J. Bozhenko, V. v Kushneryov, and I. Vida, "An Approach to Managing Innovation to Protect Financial Sector Against Cybercrime," vol. 24, no. 2, 2021, doi: 10.17512/pjms.2021.24.2.17.

[5] H. Tao et al., "Economic perspective analysis of protecting big data security and privacy," Future Generation Computer Systems, vol. 98, pp. 660–671, 2019, doi: 10.1016/j.future.2019.03.042.

[6] D. K. Citron and D. Solove, "Risk and Anxiety : A Theory of Data Breach Harms," Texas Law Review, vol. 96:737, 2018.

[7] M. Setapa, M. Mamat, H. A. Bakar, S. N. S. Yusuf, and S. Kazemian, "Enterprise Risk Management: Impact on Performance of Private Higher Educational Institutions In Malaysia," Polish Journal of Management Studies, vol. 22, no. 1, pp. 485–501, 2020, doi: 10.17512/pjms.2020.22.1.31.

[8] C. Joshi and U. Kumar, "Information security risks management framework – A step towards mitigating security risks in university network," Journal of Information Security and Applications, vol. 35, pp. 128–137, 2017, doi: 10.1016/j.jisa.2017.06.006.

[9] L. Paoli, J. Visschers, and C. Verstraete, "The impact of cybercrime on businesses : A novel conceptual framework and its application to Belgium," Crime, Law and Social Change, 2018.

[10] W. Sardjono, E. Selviyanti, W. G. Perdana, and Maryani, "Modeling of development of performance evaluation on health information systems implementation," in Journal of Physics: Conference Series, Mar. 2020, vol. 1465, no. 1. doi: 10.1088/1742-6596/1465/1/012025.

[11] T. Hidayat, O. Rukmana, and A. A. Nurrahman, "Design information system of registration and scheduling information laboratory of information systems and the decision of Bandung Islamic University," in Journal of Physics: Conference Series, Feb. 2020, vol. 1469, no. 1. doi: 10.1088/1742-6596/1469/1/012134.

[12] E. Selviyanti and W. Sardjono, "Risk management information systems assessment at the television broadcasting company," in Journal of Physics: Conference Series, Mar. 2020, vol. 1465, no. 1. doi: 10.1088/1742-6596/1465/1/012016.

[13] T. Žužek, L. Rihar, T. Berlec, and J. Kušar, "Standard project risk analysis approach," Business Systems Research, vol. 11, no. 2, pp. 149–158, Oct. 2020, doi: 10.2478/bsrj-2020-0021.

[14] P. F. de A. Lima and C. Verbano, "Project Risk Management Implementation in SMEs: A Case Study from Italy," Journal of Technology Management & Innovation, vol. 14, no. 1, 2019, [Online]. Available: http://jotmi.org

[15] H. Očevčić, K. Nenadić, K. Šolić, and T. Keser, "The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents," 2017.

[16] O. v. Kondratyeva, O. A. Kondratyeva, and I. A. Kondratev, "The Risk Management Methodology of the Quality Reducing Process of Enterprise Management Information Systems Service Support," in IOP Conference Series: Earth and Environmental Science, Mar. 2021, vol. 666, no. 6. doi: 10.1088/1755-1315/666/6/062128.

[17] N. M. S. Algheriani, V. D. Majstorovic, S. Kirin, and V. Spasojevic Brkic, "Risk model for integrated management system," Tehnicki Vjesnik, vol. 26, no. 6, pp. 1833–1840, Nov. 2019, doi: 10.17559/TV-20190123142317.

[18] T. Karkoszka, "Risk Management System in Metallurgical Production," Metalurgija, vol. 60, no. 1–2, pp. 133–136, 2021.

[19] W. Zhu and Y. Jia, "The Research on Safety Management Information System of Railway Passenger Based on Risk Management Theory," in IOP Conference Series: Earth and Environmental Science, Jan. 2018, vol. 108, no. 4. doi: 10.1088/1755-1315/108/4/042067.

[20] B. Irvin Lamarca, "Cybersecurity Risk Assessment of the University of Northern Philippines using PRISM Approach," in IOP Conference Series: Materials Science and Engineering, Jun. 2020, vol. 769, no. 1. doi: 10.1088/1757-899X/769/1/012066.

[21] A. Amini and N. Jamil, "A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing," in Journal of Physics: Conference Series, Jun. 2018, vol. 1018, no. 1. doi: 10.1088/1742-6596/1018/1/012004.

[22] P. Foroudi, Q. Yu, S. Gupta, and M. M. Foroudi, "Enhancing university brand image and reputation through customer value co-creation behaviour," Technological Forecasting and Social Change, vol. 138, pp. 218–227, Jan. 2019, doi: 10.1016/j.techfore.2018.09.006.