Identification of Information Asset in Academic Information System

Risnal Diansyah, Ikko Claudya Armae, Melly Novalia, Nesdi E. Rozanda

Universitas Muhammadiya Riau

Correspondence e-mail: risnal@umri.ac.id

Abstract. The application of Information Technology (IT) in the form of Academic Information Systems at the University of Muhammadiyah Riau (UMRI) has been carried out since 2010. Currently, academic activities at UMRI are very dependent on the existence of the information system. Activities carried out through academic information systems include student lecture registration, student study results, lecturer and student master data, scheduling lectures, lecture absences, and others. The application of this academic information system can pose a risk if the UMRI fails to assess the source of risk threats. This can result in the impact of information services being disrupted and the cessation of the decision making process. Risk is an uncertainty that can have a negative impact on an organization. Since its implementation to date, UMRI has never carried out systematic risk management. Even though the use of academic information systems at UMRI is currently crucial. Risk management is an effort from planning, organizing, leadership, controlling resources and activities to minimize the impact of losses and uncertainty on costs and consequences. Thus, risk management of information systems should be carried out by organizations that utilize Information Technology to support their activities. One method that can be used to build risk management of information systems is the Octave Allegro method. This method is a methodology for identifying risks to information systems related to information system security. Octave defines important components in a comprehensive, systematic, context-based information system security risk evaluation. The Octave Allegro method consists of 8 (eight) stages. The final result of this study is in the form of a risk assessment table and mitigation of risks to information assets. There are 8 (eight) crucial assets with a level of risk assessment of as low as 1 (one), moderate as much as 5 (five) and high as much as 2 (two).

Keywords : Academic Information Systems, Risks, Management Risk, Octave Allegro, Low, Moderate, High.

1. Introduction

The following are the things that underlie the research related to asset identification at Universitas Muhammadiyah Riau.

1.1 Background

Information technology is one of the supporting factors in increasing the productivity of business processes of an organization in the era of globalization that is growing rapidly. The application of information technology must be balanced with adequate management. The same is true with education service providers that need information as a foundation for successful performance. One application of information technology in the academic field is an academic information system. According to Rilyani (2015), the academic information system is one of the integrated systems that become a media link

between academic communities. Thus, the information system can simplify the work and accelerate the work process related to academic activities in educational institutions.

Universitas Muhammadiyah Riau (UMRI) is one of the private educational institutions in Riau Province. Academic activities at UMRI have been supported by information technology in the form of Academic Information System of Universitas Muhammadiyah Riau. Academic Information System at UMRI has been used since 2010. It is supported by various features that enable Academics in UMRI to interact through an integrated system. Activities that are usually carried out through an Academic Information System include academic registration, scheduling of lectures, academic results, master data of lecturers and students, and others. The increasing use of Information Technology in the academic field, especially the use of information systems at UMRI, is also in line with the increasing risk of Information Technology that must be faced by UMRI. This happens because in addition to the positive effects that arise due to the development of information systems, security problems and management of IT resources also occur. The security problem referred to in this statement relates to the risk of Information Technology.

In this study, the risk identification stage is carried out. At the initial stage, identification of information assets is carried out in the implementation of academic information systems at Universitas Muhammadiyah Riau.

2. Method

In identifying information assets, it is carried out in three stages using a worksheet developed by octave allegro. The following are the stages of asset identification.

2.1 Developing an Information Asset Profile

The risk assessment conducted focuses on assessing the information assets of the Academic Information System. This step begins by defining the information assets of the Academic Information System, in the form of names, user descriptions, and core processes in carrying out these assets. This helps the Information Technology and Database Unit of UMRI (TIPD) to identify all information assets vulnerable to disclosure, modification, loss/damage, and interruption. Profiles are created for each information asset.

2.2 Identifying crucial asset

To determine critical information assets in the Academic Information System, it can be seen from the system process, what activities are related to the system. Academic Information System is used by UMRI for data processing activities of students and employees/lecturers, namely processing the complete profile of students and lecturers, and student financial data. The Information System has several uses by dividing into several modules, namely employee modules, lecturers and student modules. The form of a table is to determine the critical information assets that contain modules, users and core processes. The module means the system information section used and in the module there are menus for system activity. The intended user is the owner or the party operating the module. The core process is the activity carried out on the information system used. Before determining the most critical information assets, the worksheet critical asset is used as follows:

Table 1 *Critical asset (Menu name)*

Critical Asset	(Menu name)		
Rational for Selection			
Description			
Owner			
Security Requirements	*Confidentiality*	*Integrity*	*Availability*
Important Security Requirement			

In table 1, critical asset is to determine the menu to be documented in column (1). The next step is to use Rationale for selection to document the reasons for selecting critical information assets in column (2) in the Critical Information Asset Profile. Then fill in a description of the critical information assets in column (3) of the Critical Information Asset Profile. Define the scope of Information Asset and that agreed and general definitions will be used. Then identify and document the owner of critical information assets (referring to the definition provided to determine which one is the owner). This information is filled in column (4) Critical Information Asset Profile. Furthermore, filling security needs for Confidentiality means that the confidentiality of information from these assets, Integrity means the truth and accuracy of the information on the related assets and Availability means the availability of information on the asset related information in column (5) on the Critical Information Asset Worksheet. It starts by marking needs that can be applied to information assets and forwarded by filling out information that complements the statement of security needs. On the right of this statement, it can be added with needs or more specific needs. Then the next step is to identify the most important security needs for information assets by selecting one of the security needs in column (6) of the Critical Information Asset Worksheet. This information is used when determining the potential impact of risk.

2.3 Identifying the Information Asset Container

There are 3 very important points about security and the concept of information asset containers, namely technical, people and physical. Container is a place where information assets are stored, sent, or processed so that they can be points of vulnerability and threats that position information assets at risk, and conversely containers, can be places where control can be implemented.

The container is specifically identified from several types of information technology assets such as hardware, software or systems. The first is done by determining information assets in a technical asset container that includes technological assets (software, application systems, servers, networks or hardware), physical containers can also be physical objects such as paper and container people in the form of ownership such as who is the user of the information assets. The following are forms of technical, people and physical container asset tables. To identify container assets, the following sheet is used:

Table 2 Container asset menu of employee data

Menu of Employee and Lecturer Data		
Information Asset Risk Environment Map (Technical)		
Internal		
Container Description		Owner(s)
External Container Description	-	Owner(s)

In table 2, the asset technical container in column (1) is used to fill in the menu name, information asset risk environment map (technical) in column (2) is to state the mapping of information asset risk environment including software, hardware, server, application system, internal in column (3) is to state the organization that uses it. Container description for descriptions of asset information stored, sent and processed are in column (4). Owners to state the system owner or user are in column (5). And column (6) is to state that there is no outside party involved in the activity on the related information system.

Container asset people are to state the owner or user of the information system, and who carry and store the information assets. The container description contains the user related to the information system used, while the owners are the names of the information assets used.

Physical asset containers are used to declare file folders where they are stored in physical form, for example paper. As in the table 1.4, container physical assets the employee data menu is for the container description containing a paycheck/slip, while the ownesr is the employee and lecturer concerned.

2.4 Data Collection Stages

Data collection methods are carried out to obtain information, main data and other supporting data needed in order to achieve the research objectives. Data collection is obtained from research objects in the following ways:

1. Literature Study

   Literature study activities are carried out by studying and researching various literature. The literature is obtained from libraries such as from books, scientific journals, internet sites, and other literature related to this research.

2. Field Study

   Field study activities are carried out by conducting a direct or indirect review study. The review was conducted at the Head of the UPT Information Technology and Database of UMRI, lecturers, students and employees as well as document review.

3. Results and Discussion

The following are the results of asset identification carried out.

3.1 Developing Information Assest Profile

The risk assessment conducted focuses on assessing the information assets of the Academic Information System. This step begins by defining the information assets of the Academic Information System, then identifying the container assets, where the assets are stored and who owns the assets. This helps the TIPD UMRI to identify all information assets vulnerable to disclosure, modification, loss/damage, and

interruption. Profiles are created for each information asset. At this stage, 11 assets are produced from the academic information system.

3.2 Identifying crucial asset

Determination of critical information assets refers to the process of Academic Information Systems. Critical information assets are information assets used in the processing of Academic Information Systems. The information assets that have been determined as critical information assets are recorded in the critical asset information worksheet. The information assets selected after considering several questions are:

1. An important information asset for UMRI
2. Asset information used in daily operational activities
3. Information assets which, if lost, can interfere with the ability of UMRI in achieving UMRI's goals and mission.

From the results of the above considerations, there are several information assets categorized as important information assets: Employee and lecturer modules consisting of employee data menu, attendance menu, attendance correction menu, academic menu, and research and publication menu. Student modules consist of academic record transcripts, study plan, study results, exam card, schedule, and payment data menu.

From the information assets that have been determined, the most critical information assets for UMRI are deterimined. A bad impact will be faced by UMRI if the following things happen regarding the critical information asset:

1. The information assets are modified without authorization
2. The information assets are lost or damaged
3. The information assets are accessed by people who do not have permission
4. The information assets are critical for academic information systems and UMRI

From the above questions and the considerations of the TIPD UMRI, the critical assets are the information assets contained in student modules and employee & lecturer modules, because this is where the core process is carried out. The critical information assets are: The employee and lecturer modules consisting of employee data menu, attendance menu, research and publication menu and academic menu. Student modules have a menu of academic record transcripts, study plan menu, study results menu and payment data menu. Then the critical assets above are documented on the critical asset worksheet. After filling in the critical asset worksheet, 8 critical information asset tables are obtained, namely employee data menu, attendance menu, research and publication menu, academic menu, academic transcript menu, study plan menu, study result menu and payment data menu.

3.3 Identifying Container from Information Asset

There are 3 very important points about security and the concept of information asset containers, namely technical, people and physical. Container is a place where information assets are stored, sent, or processed so that they can be points of vulnerability and threats that position information assets at risk, and conversely containers, can be places where control can be implemented.

Specifically it is identified from several types of information technology assets such as hardware, software or systems. The first is done by determining information assets in a technical asset container that includes technological assets (software, application systems, servers, networks or hardware), physical containers can also be physical objects such as paper and container people are in the form of ownership such as who the user of the information assets is.

Based on the results obtained after carrying out container assets in 3 aspects, namely technical, people and physical, technical containers are employee data menu, attendance menu, research and publication menu, academic menu, academic transcript menu, study plan menu, study results menu , and payment data menu. People container includes employee data menu, attendance menu, research and publication menu, academic menu, academic transcript menu, study plan menu, study result menu and payment data menu. While physical containers include employee data menu, research and publication menu, academic menu, academic transcripts menu, study results menu and payment data menu.

References

[1] Abbass, W., Baina, A., & Bellafkih, M. (2016). Improvement of information system security risk management. 4*th* IEEE *International Colloquium on Information Science and Technology (CiSt)* (pp. 182-187). Tangier-Assilah, Marocco: IEEE.

[2] Al-Ahmad, W., & Mohammed, B. (2015). A code of practice for effective information security risk management using COBIT 5. 2015 *Second International Conference on Informastion Security and Cyber Forensics (InfoSec)* (pp.145-151). Cape Town, South Africa: IEEE.

[3] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W.R. (2007*). Introduction OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* United State: Carnegie Mellon University.

[4] C. Alberts, A. Dorofee, J. Stevens, and C. Woody. (2005). *Introduction to the OCTAVE Approach*. PA 15213-3890. Versi 1, Carnegie Mellon Institute.

[5] Damayanti, Vani. (2015). Manajemen Risiko Aset Informasi Sistem Langgeng Pada Bank BPR Taeh Baruh Kec Payakumbuh Dengan Menggunakan Metode Octave Allegro. *Ancaman Sistem Informasi*. Pekanbaru: Uin Suska Riau.

[6] Damayanti, Vani. (2015). Manajemen Risiko Aset Informasi Sistem Langgeng PAda Bank BPR Taeh Baruh Kec Payakumbuh Dengan Menggunakan Metode Octave Allegro. *Manajemen Risiko Aset Informasi Berdasarkan Octave Allegro*. Pekanbaru: Uin Suska Riau.

[7] Ermatita. (2016). Sistem Informasi. *Jurnal Sistem Informasi (JSI)*- Volume 8 Nomor 1, 1-12

[8] Gibson, D. (2011). *Managing Risk In Information System*. Jones & Bartlett Learning.

[9] Harris, I., Tarigan, M. L., & Mawlan, S. (2013). *Analisis Manajemen Risiko pada Implementasi Sistem Informasi Keamanan di PT. Pupuk Sriwidjaja dengan framework COBIT 4.1*. Palembang: STIMIK MDP.

[10] Jakaria, D. A., Dirgahayu, R. T., & Hendrik. (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi menggunakan Metode Octave Allegro. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 37-42.

[11] Kang, Y., & Liu, R. (2016). Development of a rail breaking risk management information system. 3rd *International Conference on Systems and Informatics (ICSAI)* (pp.492-496). Shanghai China:IEEE.

[12] Lokobal, A, Sumajouw, M.D. & F. Sompie, B., 2014. *Manajemen Risiko Pada Perusahaan Jasa Pelaksanaan Konstruksi Di Provinsi Papua (Study Kasus di Kabupaten Sarmi),* Volume 4, pp. 109-118.

[13] Masky, M., Young, S. S., & Shoe, T. Y. (2015). A Novel Risk Identification Framework for Cloud Computing Security. *2nd International Conference in Information Science and Security (ICISS)* (pp. 61-64). USA: IEEE.

[14] Nurochman, A. (2014). Manajemen Risiko Sistem Informasi perpustakaan (Studi Kasus di Perpustakaan Universitas Gadja Mada Yogyakarta). *Berkala Ilmu Perpustakaan dan Informasi – Volume X Nomor 2*, 1-13.

[15] Pradana, Y. A & Rikumahu, B., 2014. *Penerapan Manajemen Risiko terhadap Perwujudan Good Corporate Governance pada Perusahaan Asuransi,* Desember, Volume 13, pp. 195-204.

[16] Rilyani, A. N., Firdaus, Y., & Jatmiko, D. D. (2015). *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus :i-Gracias Telkom University).* Bandung: Universitas Telkom.

[17] Rosini, R, Meutia., M, Badollahi. (2016). *Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro*. Jurnal Pustakawan Indonesia - Volume 14 Nomor 1, 1-9.

Vol 3-Sep2018
ISSN: 2541-3023

[18] Wijanarka, H. (2014). IT risk management to Support the realization of IT value in public organization. 2014 *International Conference on ICT For Smart Society (ICISS)* (pp. 113-117). Bandung: IEEE.