International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

University Information System Security Risk Assessment using NIST 800-30

Monika Evelin Johan, Moh Fahrur Rizqon, Ir. Jarot S. Suroso M. Eng

Abstract*: *A good and fast information system is supported by good information technology. To achieve its business goals, optimal and integrated information technology will support good quality services. The XYZ University Information System (UIS) provides a variety of information needed by students, lecturers, and all staff. But the system that is running is still experiencing problems in its use that can pose various risks. To prevent that, a risk assessment is carried out on the UIS to identify various possible risks and prevent them by forming a risk management. This research will be conducted using NIST 800-30. This standard is used with the aim of anticipating risks so that the organization does not experience losses. The preparation of UIS information security risk management carried out in this study has succeeded in identifying 32 risk scenarios, prioritizing risks, providing direction in managing risks and accepting processes whether risks are acceptable or should be mitigated.

Keywords* : *information system risk assessment, NIST 800-30, risk management, university information system.

I. INTRODUCTION

Activities in an institution are the main business processes that play an important role which generates a lot of data such as research, service, teaching, finance and student affairs. To achieve its business goals, optimal and integrated information technology will support good quality services. The increasing needs of the information system used; the risk also increases. One risk that arises is the risk of information security, this becomes important because information must always be available and kept confidential from unauthorized parties.

The XYZ University Information System (UIS) provides a variety of information needed by students, lecturers, and all staff. But the system that is running is still experiencing problems in its use, including:

1. Inputting data is done by the admin, so that there is still often error input data by the admin.
2. The system runs semi-manually, so the information generated is very slow.
3. The absence of an appropriate repository or is still simple so that the data stored is not complete. This is an obstacle because it is difficult to find information if an error occurs and data loss.
4. The constraint of using hosting is if the server traffic is congested, access to information is slow and configuration problems are crashing or inappropriate.
5. Scheduling student that still manual causes difficulty in determining the appropriate time between lecturer and student. Because scheduling does not use an automated system, it is often the case of lecturers who ask for a schedule as they wish which causes clashes.
6. There is no repository for the lecturer research journal data collection.
7. Calculation and inputting student grades that are manual causes the information obtained to be slow and an error in data input occurs.
8. Lack of proper supervision and planning in managing data and information security often results in errors and damage to data.

With the things that happened above can disrupt business processes, it is necessary to handle and assess risk in order to provide solutions to the information security needs. Education information system services that are efficient, effective, accurate data, fast data processing, and guaranteed security can improve the quality of higher education.

Information security risk management is a method of assessing and mitigating risks to information security that contains elements of confidentiality, integrity, and availability. These three aspects are vulnerable to the threat of information both physically and through the network [1].

Existing data in the University Information System (UIS) is one of the assets that must be protected in processing data for operational purposes, data security, and data distribution. In dealing with the risks that arise, it needs to be regulated so as to minimize the impact of losses if those risks occur.

A similar study of an academic information system at MH Thamrin University showed how information security risk management was strongly supported, of the 286 responses obtained, there was no disagreement with the proposed mitigation [2].

Manuscript published on 30 September 2019
* Correspondence Author
Monika Evelin Johan*, Information System Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480. Email: monika.johan@binus.ac.id
Moh Fahrur Rizqon, Information System Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480. Email: Moh.Rizqon@binus.ac.id
Dr. Ir. Jarot S.Suroso, M.Eng., Information System Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480. Email: jarot_suroso@binus.ac.id

Risk management that will be used in this research is to use the NIST (National Institute of Technology Standard) framework developed by the US Department of Commerce. This standard is used with the aim of anticipating risks so that the organization does not experience losses.

By identifying the risks that will occur, it can protect important business processes from security threats and minimize the risks of information systems and technology in tertiary institutions.

II. LITERATURE REVIEW

A. Risk Management

The risk management that will be used in this research is to use the NIST (National Institute of Technology Standard) framework developed by the US Department of Commerce. This standard is used with the aim of anticipating risks, so that the organization does not experience losses. By identifying the risks that will occur, it can protect important business processes from security threats and minimize the risks of information systems and technology in tertiary institutions [3].

A book written by Fahmi stated that risk management is

Using various management approaches to measures existing problems [4].

Another statement said that risk management is approach to manage uncertainty, using resource management in risk assessment and developing strategies to manage and mitigate risks [5].

The IT risk management is expected to reduce the damage of financial, reputation decrease, business operations cessation, assets (system and data) failure and a delay in the decision-making process [6].

B. Information Security

In Evan Wheeler's book entitled Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, there are 4 factors that must be taken into account [7]:

1. Confidentiality: information must not accessible to unauthorized individuals, processes, or devices.
2. Integrity: information protection against unauthorized permission to create, modify, or delete.
3. Availability: reliable access to data and information services for authorized users anytime.
4. Accountability: the ability to trace activities to a responsible source.

According to ISO 27002 (2005), information security is protecting information from various threats by minimizing business risks and maximizing investment returns in order to ensure the continuity of business processes

According DJ White, United Stated National Information System Security state that information system security is protecting information systems against unauthorized access and modification of information including detect and fight the threat [8].

C. Information Security Risk

Information security risk is the loss probability of confidentiality, integrity, availability or accountability in the future [9].

D. *NIST SP 800-30*

NIST SP 800-30 is a standard that contains guidelines for conducting risk assessments in an organization. This standard is developed by the National Institute of Standards and Technology. These are stages of risk assessment based on NIST 800-30 [6]:

1. System Characterization
   At this stage, IT systems boundaries including resources and information must be identified.
2. Threat Identification
   The possibility of threats and information of threats such as sources, potential vulnerabilities and existing controls is reviewed.
3. Vulnerability Identification
   Create list of systems vulnerabilities by vulnerability identification
4. Control Analysis
   Minimize or eliminate the possibility of developing threats by analyzing controls that have been implemented or planned by organization.
5. Likelihood Determination
   The ranking process of potential vulnerability can be carried out in the system. The considered factors are the threat (source and capability), the nature of the vulnerability, the existence and effectiveness of the control.
6. Impact Analysis
   This stage is used to determine the negative impacts from measurement.
7. Risk Determination
   The level of risk assessment in an IT system is carried out at this step.
8. Control Recommendations
   This stage assesses which controls can reduce or eliminate the identified risk. The recommended control should be able to reduce the level of risk in IT systems to acceptable level.
9. Results Documentation
   At this stage the report of risk assessment will be developed (source of threats, vulnerabilities, risks assessed and recommended controls).

III. RESEARCH METHODOLOGY

A. Research Flow

The flow of research in this study is in accordance with Figure 1 in the operational and IT departments of XYZ tertiary institutions in relation to the presence or absence of information security risk management in UIS, and how important information security risk management in UIS needs to be made if there are no guidelines in this UIS.

Information obtained from interviews with the IT and Operational Section related to the application of information security risk management and data processing / input procedures. Information obtained from interviews conducted is certainty that the UIS does not yet have information security risk management.

After collecting data from the results of the interview, the first step is the preparation of information security risk management with the output of basic criteria, the scope and limits of implementation, and the organization of information security risk management.

Based on the basic criteria that have been prepared, what is next done is to carry out a risk assessment. Risk assessment starts from identifying assets, identifying vulnerabilities, and identifying threats, determining the impact value, determining the likelihood value, and determining the value of risk. The output of this step is a list of risks.

From the list of available risks, an evaluation of those risks is then carried out. to then determine risk priorities based on predetermined values.

For risks that have been identified and prioritized, the next step is to implement controls that are risk management and lead to risk acceptance where the output of this process is a list of mitigated and accepted risks. The risk received has been approved by the risk owner unit which is a tolerance limit for acceptance of risk.

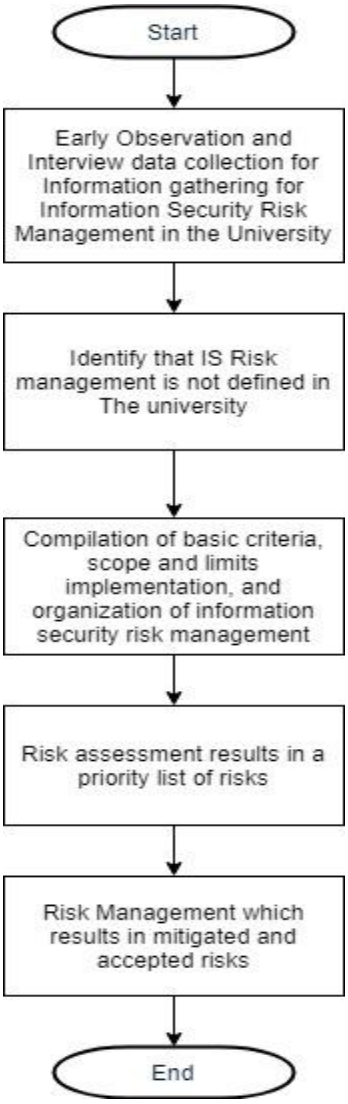

Fig. 1 Research Flowchart

B. List of Questions

The questions raised in this study aim to explore information about vulnerabilities / weaknesses related to information security related to UIS.

The list of questions was prepared using the NIST SP 800-26 standard guide. NIST SP 800-26 is a standard that contains information security self-assessment guidelines on information technology.

In total, the number of questions contained in NIST SP 800-26 is + 219 questions, and all of these questions are used to assess vulnerabilities / weaknesses of information security in UIS.

There are three main parts to the distribution of the questionnaire contained in NIST SP 800-26:

1. Management Control

Management control focuses on the management of information technology security systems and risk management of the system. There are 5 sub-sections to this process:

- Risk Management
- Review of Security Control
- Life Cycle
- Authorize Processing
- System Security Plan

2. Operational Control

Operational control focuses on applied and implemented mechanism by staffs. On operational control, there are nine subsections of questions, namely:

- Personnel Security
- Physical Security
- Production, Input/output Controls
- Contingency Planning
- Hardware and Systems Software
- Documentation
- Data Integrity
- Security Awareness, Training, and Education
- Incident Response Capability

3. Technical Control

Technical control focuses on the computer systems used by staff. In technical control, there are three sub-sections, Identification and Authentication

- Logical Access Control
- Audit Trails

IV. RESULT AND DISCUSSION

The results of the preparation of information security risk management in the University Information System (UIS) are as follows:

A. Setting the Context

The initial process undertaken to determine the basis of the entire process of developing UIS information security risk management is to apply context. The following are the results of the context applied to UIS:

1. Basic Criteria

According to ISO 27005, the basic criteria in developing information security risk management are impact criteria, likelihood criteria, risk rating criteria, and risk acceptance criteria. Then this study presents the risks identified, the impact of those risks, the likelihood of those risks arising, and the value of the risks and how they were received.

2.Scope and Limitation of Implementation

Information security risk management in this study is limited to the University Information System (UIS).

3.Information Security Risk Management Organization

Information security risk management in this UIS is carried out by the unit responsible for the development and implementation of the UIS, chaired by the UIS development and implementation coordinator.

B. Risk Assessment

1.Identification of assets

Assets according to ISO 27005 are divided into two namely primary and secondary assets. Primary assets are the main processes or business or activities or information of an organization while secondary assets are hardware, networks, software, locations, data centers, personnel who work on and the structure of the organization. In this study identified 6 primary assets and 12 secondary assets that are directly related to the scope.

2.List of vulnerabilities

This study identifies vulnerabilities in UIS using the list of questions contained in NIST SP 800-26. The number of questions asked to the UIS development and implementation coordinator was 219 questions.

3.List of threats

This study also uses a list of threats in NIST SP 800-30 and ISO 27005 confirmed by the UIS development and implementation coordinator.

4.Impact Value

This research compiled the impact criteria and the impact value which was consulted to the UIS development and implementation coordinator, as outlined in the table shown below.

Table- I: Impact Table

Impact	Impact Value
Not Significant - does not interfere with the UIS system process	1
Minor - a little disruptive to the UIS system process but still running	2
Moderate - interferes with the UIS system process, causes faltering, Internal impact	3
Major - Stop the UIS system process, Public Impact	4

5. Probability Value

In this study a risk likelihood table is arranged, in Table 2 the likelihood and probability values are displayed.

Table- II: Possibility Table

Possibility	Value Possible
Can Happen	1
Might Happen	2
Often Happen	3

6. Risk Value

Risk can be assessed on the level of risk to be mitigated or not based on the risk value in table 3 compiled from this study.

Table- III: Risk Value

Risk Level	Risk Value
Low – risk is acceptable, can be ignored	1 - 2
Medium – risk can be mitigated	3 – 7
High – risk is not acceptable, must be mitigated	8 - 12

7.List of Risks

From the identification of existing vulnerabilities and threats, the risk identified were 32 risks.

C. Risk Evaluation

Risk evaluation is the process of assessing that have been successfully identified, assessed their impact if they occur and the likelihood of them occurring so that the risk is known to have a risk value. One form of risk evaluation is also to prioritize risks. Prioritizing risks is done by sorting the largest to smallest risk values.

In Table 4, there are 32 risks identified, identified the value of risks and arranged according to risk priorities.

Table- IV: Risk Evaluation and Priority

No	Impact	Likelihood	Risk Value
R1	4	2	8
R2	4	2	8
R3	4	2	8
R5	4	2	8
R6	4	2	8
R7	4	2	8
R15	4	2	8
R17	4	2	8
R20	4	2	8
R29	4	2	8
R30	4	2	8
R4	3	2	6
R8	3	2	6
R10	3	2	6
R12	3	2	6
R14	3	2	6
R18	3	2	6
R19	3	2	6
R22	3	2	6
R24	3	2	6
R9	2	2	4
R11	2	2	4
R13	2	2	4
R16	2	2	4
R21	2	2	4
R23	2	2	4
R25	2	2	4
R27	2	2	4
R28	4	1	4

R31	2	1	2
R26	1	1	1
R32	1	1	1

The explanation of the risk code in Table 4 is as follows:

Table- V: Risk Code

No	Risk
R1	UIS doesn't operate.
R2	UIS cannot be operated.
R3	Computers that operate UIS cannot be used.
R5	Documents are lost, damaged, or distributed by irresponsible people.
R6	UIS Operations Team does not operate.
R7	All data theft.
R15	The building has a fire.
R17	All data was accidentally exposed.
R20	All Student Data exposed accidentally.
R29	Social Engineering targeted to the UIS Operations Team.
R30	Unauthorized access to UIS.
R4	The impact arises from the exploitation of threats to vulnerability.
R8	Partial data theft.
R10	All University Financial Management Activities cannot be carried out.
R12	All university student management activities cannot be carried out.
R14	Total Student Data Theft.
R18	Data partially exposed accidentally.
R19	Student data some have been accidentally exposed.
R22	All data is corrupted.
R24	All student data is corrupted.
R9	Some College Financial Management Activities cannot be carried out.
R11	Some college student management activities cannot be carried out.
R13	Student Data Theft Partially.
R16	Damage to the computer but UIS continues to operate.
R21	UIS application error.
R23	Partially data is damaged.
R25	Student data partially damaged.
R27	Malicious code inserted.
R28	Natural Disasters damage computers that operate UIS.
R31	The user has experienced an error.
R26	Maintenance Error
R32	Usage is not in accordance with Ethics.

D. Risk Management

After the risks are ranked, the next step of this research is to establish controls for each risk. In this study, the type of control applied refers to NIST SP 800-30, which is prevention or detection, but because UIS is currently still in the development stage and has not been fully operational. The controls applied for each risk are based on ISO 27002 and NIST SP 800-53. The UIS development and implementation team in charge of the selection of controls and who is responsible for approving and implementing the controls is the UIS development and implementation coordinator.

E. Risk Acceptance

This process is carried out to accept the risks identified, whether those risks are accepted, mitigated, transferred, avoided or made an opportunity. The acceptance of risk is also based on the Risk Value in Table 4. In this study, the acceptance of risk is decided by the party to be able to make decisions related to the identified risks, in this case the coordinator of the development and implementation of UIS.

Table- VI. Risk Acceptance

No	Acceptance Status
R1	Mitigated
R2	Mitigated
R3	Mitigated
R5	Mitigated
R6	Mitigated
R7	Mitigated
R15	Mitigated
R17	Mitigated
R20	Mitigated
R29	Mitigated
R30	Mitigated
R4	Mitigated
R8	Mitigated
R10	Mitigated
R12	Mitigated
R14	Mitigated
R18	Mitigated
R19	Mitigated
R22	Mitigated
R24	Mitigated
R9	Mitigated
R11	Mitigated
R13	Mitigated
R16	Mitigated
R21	Mitigated
R23	Mitigated
R25	Mitigated
R27	Mitigated

R28	Mitigated
R31	Accepted
R26	Accepted
R32	Accepted

V. CONCLUSION

Based on the discussion that has been done, here are some things that can be concluded:

1. UIS has a very important role in supporting the process of university financial management, student administration and online student learning, so it becomes a necessity for UIS to have the tools to guarantee the availability of UIS services. One tool that can be used to ensure the availability of UIS services is the application of information security risk management.
2. The process of preparing information security risk management in UIS in the form of setting context, identifying assets, identifying vulnerabilities, identifying threats, identifying risks, and selecting controls for risks, guided by ISO 27005, NIST SP 800-26, NIST SP 800-53, and NIST SP 800-30.
3. The preparation of UIS information security risk management carried out in this study has succeeded in identifying 32 risk scenarios, prioritizing risks, providing direction in managing risks and accepting processes whether risks are acceptable or should be mitigated.

REFERENCES

1. F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1," vol. 02, no. 02, pp. 1–8, 2017.
2. J. S. Suroso, M. A. Fakhrozi, J. S. Suroso, and M. A. Fakhrozi, "ScienceDirect ScienceDirect Assessment Of Information System Risk Management with Octave Assessment Of Information Risk Management with Octave Allegro At System Education," Procedia Comput. Sci., vol. 135, pp. 202–213, 2018.
3. J. Slay and A. Koronios, Information technology, security and risk management. John Wiley & Sons Australia Ltd, 2005.
4. I. Fahmi, "Manajemen Risiko: Teori," Kasus dan Solusi, Bandung, Alf., 2010.
5. J. S. Suroso and B. Rahadi, "Development of IT risk management framework using COBIT 4.1, implementation in IT governance for support business strategy," in Proceedings of the 2017 International Conference on Education and Multimedia Technology, 2017, pp. 92–96.
6. F. Hartawan and J. S. Suroso, "Information Technology Services Evaluation Based ITIL V3 2011 and COBIT 5 in Center for Data and Information," in Asian Conference on Intelligent Information and Database Systems, 2017, pp. 44–51.
7. E. Wheeler, Security risk management: Building an information security risk management program from the Ground Up. Elsevier, 2011.
8. J. D. White, "Managing Information in the Public Sector, ME Sharpe," Inc, New York, 2007.
9. A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," in 2009 International conference on availability, reliability and security, 2009, pp. 726–731.

AUTHORS PROFILE

Monika Evelin Johan Information Systems Management Department, BINUS Graduate Program, Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia, 11480 monika.johan@binus.ac.id

Moh Fahrur Rizqon Information Systems Management Department, BINUS Graduate Program, Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia, 11480 moh.rizqon@binus.ac.id

Dr. Ir. Jarot S.Suroso, M.Eng. Information Systems Management Department, BINUS Graduate Program, Master of Information Systems Management, Bina Nusantara University Jakarta, Indonesia, 11480 jarot_suroso@binus.ac.id