Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11205

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Analysis and Evaluation of Academic Information System Security Using NIST SP 800-26 Framework

Poningsih[1)*], **Muhammad Ridwan Lubis** [2)]
AMIK Tunas Bangsa Pematangsiantar
[1)] poningsih@amiktunasbangsa.ac.id, [2)] ridwanlubis@amiktunasbangsa.ac.id

Submitted : Nov 4, 2021 | **Accepted** : Feb 1, 2022 | **Published** : Feb 3, 2022

Abstract: Along with the development of technology and information that is growing rapidly, currently the competition between educational institutions is getting stronger. If an institution is not able to keep up with the progress of information technology which is developing very quickly, it is certain that the institution will be left very far behind from all sides. However, there are things that really need to be considered due to the development of information technology, namely the consideration of the security of information systems owned by the Institution. For that we need an analysis and evaluation of the information system used to identify security in the information system. If the analysis and evaluation is not carried out, problems will arise related to the security of an information system such as data that is vulnerable to threats such as damaged and lost data so that the data becomes invalid. If the data is not valid, it is certain that the information generated will also not be reliable. Evaluation of information system security can be done with the framework. NIST is a framework that can be used to evaluate and identify security and risks in information systems. The information system security evaluation process is carried out by distributing questionnaires to the academic community in accordance with the NIST SP 800-26 framework and the data is managed to obtain the final result. The results of the academic information system security evaluation have an overall final score of 91.6%.

Keywords: Academic Information System, Evaluation of information system security, Questionnaire, NIST SP 800-26.

INTRODUCTION

Background

The development of technology and information that is growing very rapidly requires an institution, especially a university, to be able to balance the facilities and infrastructure related to the existing academic information system, considering the competition between universities is very fast at this time (Ogundoyini et al. 2021). The quality of information system services in universities is required to be better from various sides, one of which is in terms of information system security (Tohidi 2011). The number of community demands related to the quality of graduates and the service system in higher education requires the leadership to think about strategies for how the demands of the various communities (Bayo Olushola 2020). One of the strategies that can be carried out by higher education leaders is to provide an academic information system that is fast, precise, relevant and guaranteed its security (Gadhari and Jadhav 2016). The development of technology and information provides many positive impacts (Syafitri 2016). With the development of information technology, the academic world shows a significant change.

Starting from the teaching method for lecturers, positive competition among students by how students compete to get the best grades, and so on (Ki-Aries et al. 2017). Because now distance and time are no longer a problem or obstacle. Science is getting wider, the competition is getting higher. Integration between lecturers and students can be achieved well through a good information system (Muthukrishnan and Palaniappan 2016). The purpose of building an academic information system is to facilitate service and provide the best service to the entire academic community, so that the academic community can obtain information that is fast, accurate, relevant and guaranteed its security (Muthukrishnan and Palaniappan 2016). With a good information system, universities are able to

*name of corresponding author

survive and compete in the midst of a fairly tight competition today due to the impact of the development of information technology, because information systems have a very important role in improving the quality and services in an organization (Muthukrishnan and Palaniappan 2016). NIST is a framework published by the National Institute of Standard Technology (NIST). NIST takes measurements, sets standards and technology to optimize the role of Institutional facilities and infrastructure, especially in the IT field (Sandy and Solihin 2021). NIST has many versions and topics but are related to each other. One of the NIST versions for evaluating information system security is “NIST Special Publication 800-26: Security self-Assessment Guide for Information Technology System”. The NIST framework is expected to improve the ability of universities to overcome current and future academic information system security problems (Hoffmann et al. 2020).

Formulation of the Problem

Based on the background of the problems above, it can be concluded that the security of academic information systems is one of the very important pillars in improving the quality of information services and how to maintain the security of the information system so that it is necessary to analyze and evaluate the information system (Mailloux et al. 2015).

Research Purposes

The aim is to answer the above problems, namely to analyze and evaluate the security of the academic information system currently used at AMIK Tunas Bangsa Pematangsiantar.

LITERATURE REVIEW

System Basis Concept

There are 2 approaches in defining a system, namely from the procedural approach and its components (Mohd Sharudin Mat Deli; et al. 2017). When viewed in terms of procedures, the system is a network of procedures that are interconnected to carry out activities to complete a certain goal. The definition of the system in terms of its components, the system is a collection of elements that interact to achieve certain goals. These components / subsystems cannot stand alone, but are interrelated with one another to form a single unit so that the goals and objectives of the system can be achieved (Muthukrishnan and Palaniappan 2016).

Information System

An information system is a system within an organization that brings together the daily transaction processing needs to support operations, managerial and strategic activities of an organization and provides certain outside parties with the required reports (Santoso and Ernawati 2017). An information system can be defined as a collection of elements or resources and a network of procedures that are interrelated in an integrated manner, integrated in a certain hierarchical relationship, and aims to process data into information (Supriyanto, Aknuranda, and Putra 2019). Information systems in general can be formed with several operating activities, namely:

1. Data collection
2. Data grouping
3. Data calculation
4. Analyze topic data
5. Report presentation

Information System Components

The information system consists of components called the Building Block, namely (Putro, Ambarwati, and Setiawan 2021):

1. Input Block
   Input represents data that enters the information system.
2. Block Model
   This block consists of a combination of procedures, logic and mathematical methods that will manipulate the input data.
3. Output Block
   The product of the information system is quality and documented information that is useful for all levels of management.
4. Technology Block
   Technology is used to carry out all the processes that exist in the information system
5. Database block
   A collection of related data, stored on computer hardware and using software to manipulate it.
6. Control block

*name of corresponding author

Several controls need to be designed and implemented to ensure that things that can damage the system can be prevented or if something goes wrong can be addressed immediately.

Academic Information System

Academic information system is a method used to regulate how to collect, enter and process data and store it, manage, monitor and report it so that it can support companies or organizations to achieve goals (Santoso and Ernawati 2017).

Academic information system is a system that is used to provide information and manage the administration of all academic-related activities (Perdana 2018).

Management of data on fields of study and curriculum makes it easier to find information about one field of study. A good provision of certain and interesting classifications (criteria) will be able to accommodate larger data and produce more useful information. If this method is chosen, some additional information should be included or provided with a link to the host College (Ki-Aries et al. 2017). For example, about the teaching and learning process (PBM) related to the material. In a distributed manner, the data is managed by each, but there is a gateway or presentation that is mutually agreed upon for the convenience of the reader. The Ministry of Education or the government also has access rights. If needed, data collection for archives can be done via the internet at any time and reduces the need for data exchange through print media. Lecture activities are carried out every semester including a) filling out the KRS; b) attendance, materials, and coursework; c) assessment (Izatri, Rohmah, and Dewi 2020).

Information System Security

Information system security is something that needs to be considered when building an information system. Information system security is used to prevent someone who does not have access rights to enter the system. There are 3 things that become aspects of the information system security audit assessment, namely confidentiality, integrity and availability (Mohd Sharudin Mat Deli; et al. 2017).

Information System and Evaluation

The purpose of analyzing and evaluating this academic information system is to secure assets and all forms of information related to academic activities both in terms of system efficiency, system effectiveness, service availability, reliability, confidentiality and maintaining system integrity (Bayo Olushola 2020).

NIST SP 800-26

NIST SP 800-26 reveals that there are 17 assessment sub categories which are divided into 3 control groups, namely (Chopra, Kumar Jha, and Jain 2017):

1. Management Control (Management Control)
    1. Risk Management (Risk Management)
    2. Review of Security Control (Review of Security Control)
    3. Circle of life (Life Cicle)
    4. Authorize Processing
    5. System Security Plan
2. Operational Control
    1. Personnel Security
    2. Physical Security
    3. Production, input and output control (Production, Input and Output Control)
    4. Contingency Planning
3. Hardware and software system maintenance (Hardware and system software maintenance)
    1. Data Integrity (Data Integrity)
    2. Documentation
    3. Security awareness, training and education
    4. Incident response capability
4. Technical control
    1. Identification and Authentication (Identification and Authentication)
    2. Logical Access Control
    3. Audit Trials
5. NIST SP 800-26 also states that there are 5 security levels in information technology, namely:
    1. Level 1 – Documented Policy
    2. Level 2 – Documented Procedures
    3. Level 3 – Implemented Procedures and Controls

*name of corresponding author

4. Level 4 – Tested and Reviewed Procedures and Controls
5. Level 5 – Fully Integrated Procedures and Controls

METHOD

Object of research

The object of research is the Academic Information System at AMIK Tunas Bangsa Pematangsiantar.

Research methodology

The research method is an arrangement of work steps that are made sequentially. His research methods are as follows:

Initial research preparation

Analyzing problems, determining the background, formulating problems, conducting literature studies and reviewing theories as the theoretical basis

Designing a questionnaire

The assessment criteria are made in accordance with those that have been determined based on those listed in the NIST SP 800-26 framework. The number of criteria used is 17 criteria which are divided into 3 control groups. These criteria were used to prepare the assessment questionnaire. Each assessment criteria has 2 number of statements, so that the total data for each criterion is 90 data and uses a rating scale of 1 – 5.

Determine Respondents

Respondents who were appointed to fill out the questionnaire were structural members consisting of Directors, Deputy Directors, Head of Study Programs and their staff, finance, student affairs, HR and general sections, Laboratory Coordinator, Head of UPT related to the Academic Information system, several students . The total number of respondents totaled 45 people.

Data analysis and discussion

The data obtained from the results of the questionnaire were then processed and analyzed to obtain conclusions regarding the object of research

RESULT

Research Result

The results of this research are in the form of questionnaire data obtained from the assessment of 45 respondents. All the data is processed to get the final result of the assessment.

Based on the calculation of the questionnaire data, the results of the management control assessment are at 3,164. Referring to the level of information system security contained in the NIST SP 800-26 framework used, management control is at level 3, namely implemented procedures and controls. This means that the procedures and controls planned by the Institution relating to management control have been implemented.

Management Control Assessment

Table 1. Management Control Assessment

No	Criteria	Average	Final Average	Persentase (%)
1	1.a	3,244	3,164	63,3%
2	1.b	3,222		
3	1.c	3,044		
4	1.d	3,289		
5	1.e	3,022		

Based on the calculation of the questionnaire data, the results of the management control assessment are at 3,164. Referring to the level of information system security contained in the NIST SP 800-26 framework used, management control is at level 3, namely implemented procedures and controls. This means that the procedures and controls planned by the Institution relating to management control have been implemented.

Operational *Control Assessment*

*name of corresponding author

Table 2. Operational Control Assessment

No	Criteria	Average	Final Average	Persentase (%)
1	2.a	2,711	2,565	51,3
2	2.b	2,489		
3	2.c	2,678		
4	2.d	2,922		
5	2.e	2,433		
6	2.f	2,333		
7	2.g	2,533		
8	2.h	2,489		
9	2.i	2,500		

From the processed questionnaire data, the results for the Operational Control assessment are 2,565 out of 5. Referring to the information system security level contained in the NIST SP 800-26 framework used, that Operational Control is at level 2, namely Documented Procedures.). This means that the procedures planned by the Institution have been documented.

Technical Control Assessment

Table 3. Technical Control Assessment

No	Kriteria	Rata-Rata	Rata-Rata Akhir	Persentase (%)
1	3.a	2,478	2,515	50,3
2	3.b	2,756		
3	3.c	2,311		

From the questionnaire data that has been processed, the results for the Technical Control assessment are 2.515 out of 5. Referring to the information system security level contained in the NIST SP 800-26 framework used, that technical control is at level 2, namely Documented Procedures.). This means that the procedures planned by the Institution have been documented.

Overall Rating

Table 4. Overall Rating

No	Kriteria Pengendalian	Rata-Rata	Rata-Rata Akhir	Persentase (%)
1	1	3,164	2,748	91,6
2	2	2,565		
3	3	2,515		

Based on the results of the overall questionnaire assessment, the score is 2,748 out of 5. Referring to the information system security level contained in the NIST SP 800-26 framework used, that technical control is at level 2, namely Documented Procedures. This means that the procedures planned by the Institution have been documented.

Data Validity

Validity is a measure that allows researchers to assume that the measuring instrument can be used to measure the character to be measured. Validity is a measure that shows the level of accuracy of the measuring instrument. A measuring instrument is declared valid if the measuring instrument produces the right size in a measurement of a

*name of corresponding author

particular problem, and is not valid for measuring other problems. Valid and accurate measuring instruments have high validity. On the other hand, less valid measuring instruments have low validity. In general, the validity of measuring instruments depends on logical factors and statistical evidence. Determination of the validity of the data in this study using Ms. Excel.

Table 5. Questionnaire Data Validity

No	Criteria	Validity
1	1.a	Valid
2	1.b	Valid
3	1.c	Valid
4	1.d	Valid
5	1.e	Valid
6	2.a	Valid
7	2.b	Valid
8	2.c	Valid
9	2.d	No Valid
10	2.e	Valid
11	2.f	Valid
12	2.g	Valid
13	2.h	No Valid
14	2.i	Valid
15	3.a	Valid
16	3.b	Valid
17	3.c	Valid

DISCUSSION

Based on the evaluation results of the security of the academic information system in AMIK Tunas Bangsa Pematangsiantar, it can be concluded that the security of the information system is at level 2, namely Documented Procedures. This indicates that the procedure and the control applied at AMIK Tunas Bangsa is still in a documented procedure. This is obtained based on the results of the overall final assessment which is 2,748 out of 5.

CONCLUSION

NIST is a framework that can be used to evaluate and identify security and risks in information systems. The information system security evaluation process is carried out by distributing questionnaires to the academic community in accordance with the NIST SP 800-26 framework and the data is managed to obtain the final result. The results of the academic information system security evaluation have an overall final score of 91.6%.

REFERENCES

Chopra, G., Jha, R. K., & Jain, S. (2017). A survey on ultra-dense network and emerging technologies: Security challenges and possible solutions. *Journal of Network and Computer Applications*, *95*, 54-78.

Deli, M. S. M., Ahmad, J. F., Hassan, N. H., Maarop, N., Samy, G. N., Abdullah, M. S., & Yaacob, S. (2018). Understanding User Participation in Information Security Risk Management. *Open International Journal of Informatics*, *5*(1), 1-8.

Gadhari, S. P., & Jadhav, P. S. A Detailed Review on Cybercrime and Cyber Security. *Journal of Android and IOS Applications and Testing*, *1*(2).

*name of corresponding author

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Measurement models of information security based on the principles and practices for risk-based approach. *Procedia Manufacturing*, *44*, 647-654.

Izatri, D. I., Rohmah, N. I., & Dewi, R. S. (2020). Identifikasi risiko pada perpustakaan daerah Gresik dengan NIST SP 800-30. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 50-55.

Ki-Aries, D., Dogan, H., Faily, S., Whittington, P., & Williams, C. (2017, September). From requirements to operation: components for risk assessment in a pervasive system of systems. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)* (pp. 83-89). IEEE.

Mailloux, L. O., Garrison, C., Dove, R., & Biondo, R. C. (2015, October). Guidance for working group maintenance of the Systems Engineering Body of Knowledge (SEBoK) with systems security engineering example. In *INCOSE International Symposium* (Vol. 25, No. 1, pp. 1004-1019).

Muthukrishnan, S. M., & Palaniappan, S. (2016, May). Security metrics maturity model for operational security. In *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (pp. 101-106). IEEE.

Ogundoyin, I. K., Olajubu, E. A., Akinboro, S. A., Akanbi, C. O., & Aderounmu, G. A. (2017). A computational framework for computer networks novel threats management. *Uniosun Journal of Sciences*, *1*(2).

Omoyiola, B. O. (2020). The evolution of information security measurement and testing. *IOSR Journal of Computer Engineering*, *22*(3), 50-54.

Perdana, R. S. (2018). Audit Keamanan Sistem Informasi Akademik Menggunakan Framework NIST SP 800-26 (Studi Kasus: Universitas Sangga Buana YPKP Bandung). *Infotronik: Jurnal Teknologi Informasi dan Elektronika*, *3*(1), 9-14.

Putro, A., Ambarwati, A., & Setiawan, E. (2021). Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1. *Jurnal Teknologi Dan Informasi*, *11*(2), 125-136. https://doi.org/10.34010/jati.v11i2.5314

Sandy, S., & Solihin, H. H. (2021). Audit Keamanan dan Manajemen Risiko pada e-Learning Universitas Sangga Buana. *Jurnal Manajemen Informatika (JAMIKA)*, *11*(1), 1-14.

Santoso, H. B., & Ernawati, L. (2017). Manajemen Risiko Pada Pusat Data Perguruan Tinggi Dengan Kerangka Kerja NIST 800-30 (Studi Kasus: Universitas Kristen Duta Wacana). *Jurnal Informatika Dan Sistem Informasi (JUISI) Universitas Ciputra*, *3*(02), 8-17.

Supriyanto, A., Aknuranda, I., & Putra, W. H. N. (2019). Penyusunan Disaster Recovery Plan (DRP) berdasarkan Framework NIST SP 800-34 (Studi Kasus: Departemen Teknologi Informasi PT Pupuk Kalimantan Timur). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X.

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, *2*(2), 8-13.

Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science*, *3*, 881-887.