Security Quality Measurement Framework for Academic Information System (AIS) Based on ISO/IEC 25010 Quality Model

Istiningdyah Saptarini[1], Siti Rochimah [2], Umi Laili Yuhana [3]

***Abstract*— Academic Information System (AIS) is a CASE tool that can improve efficiency and operational effectiveness of a university. It is necessary to guarantee its security quality. In addition, AIS has different characteristics from other software. This study aims to establish a framework to measure the quality of security on the AIS application domain. The framework is built based on ISO/IEC 25010 quality model. The resulting framework showed that it can measure 20 additional security aspects and produce an aggregated security value compared to the existing quality measurement standard. It is also able to improve the quality of the case study system by an increase in security value of 15.6%.**

***Keywords*—Academic Information System, ISO/IEC 25010, security, quality measurement framework, AHP.**

I. Introduction

Information system is one means of supporting the activities of a particular organization or institution especially universities. Information systems at universities in Indonesia, or the Academic Information System (AIS) itself included to the quality assessment criteria of Universities [1]. Thus, the existence of Academic Information Systems at Universities is important. Therefore, quality assurance for AIS is needed. One step that can be done to ensure its quality is to do an evaluation using existing standard measures of quality to know the maturity level of the system. Through evaluation, software developers, users, or maintainer of the system can find out the shortcomings of the system so they will be able to improve the system. That way, hopefully the system can be used continuously.

There are many aspects of software quality that can be evaluated. McCall [2] states that softwares generally have 11 quality factors which then grouped into three categories. In addition to McCall, other quality models such as Boehm, Dromey, FURPS, Ghezzi, and Kazman [3] see the quality of software from various aspects and attributes. Whereas the quality standard such as ISO divides software quality aspects into several characteristics and sub characteristics [4][5].

Security is one important quality aspect to be considered. In software, the security aspect related to data and information security. AIS itself has different characteristics from other software. Although business processes in universities are the same, the implementation depends on the academic regulations applied. Academic regulations in each university vary in its application and can be changed at any time to comply with government or the university's regulations. As a result, the AIS may change at any time to follow the regulations. This also applies to the security needs such as the access rights to information on the system.

Due to the characteristic differences of AIS, a certain quality standard that is capable of measuring the quality of security in AIS application domain is needed. This research aims to establish a new security quality measurement framework that is capable of measuring the security quality in AIS application domain in a comprehensive manner. ISO/ IEC 25010 have been selected as the basis for the establishment of the framework because ISO/ IEC 25010 is an improvement of ISO/ IEC 9126. One such improvement is the addition of the security characteristics. Moreover, ISO/ IEC 25010 is used due to its flexibility and generality, which makes it convenient to adapt the quality model to measure a specific application domain.

II. Academic Information System Security Quality Measurement Framework

The development phases of this framework consists of determining the measurement properties, measurement attributes mapping, assigning weights, and testing. The proposed security quality measurement framework has 5 sub characteristics that are considered as important in AIS application domain.

To determine the measurements' properties, measurement objective of each sub characteristic on the security quality is defined. The objective can be defined by identifying what we want to know and what information needs to be represented by the measurement of each sub characteristic. Target entity to be measured is also determined at this stage. The target entity can be a product, system behavior, or stakeholders such as AIS user, developer, or maintainer. Then the properties of the target entity associated with each subcharacteristic measurement objective are determined. The property must be able to be represented using numbers [6].

The next step is to determine the measurement method which provides a step to transform the property values that have been obtained in the preceding stage so as to produce a value that represents the purpose of measuring the quality of each security sub characteristic. The method is generated in the form of a mathematical function with a standard unit of measurement. Limitation of measurements was also specified at this stage. Measurement parameters are determined by mapping AIS's needs on security quality standards ISO / IEC 25010 and ISO / IEC 27002.

[1]Istiningdyah Saptarini, Siti Rochimah, Umi Laili Yuhana are Siti Rochimah with Departement of Informatics Engineering, Institut Teknologi Sepuluh Nopember, Surabaya, 60111, Indonesia. E-mail: istiningdyah.057@gmail.com; siti@its-sby.edu; yuhana@cs.its.ac.id.

The proposed framework has a hierarchical measurement method, where measurement metrics are at the lowest level that will form the sub characteristic values. Each metric and sub characteristic is weighted on a scale from 0 to 1 in accordance with the security requirements in the AIS application domain. Weighting on the measurement method of the proposed framework is done by using Analytical Hierarchy Process (AHP) that used by Bekhamal, Kahani, and Kazem [7]. The weighting process is conducted by determining the level of importance of each metric and sub characteristic using questionnaires. Questionnaires were distributed to six experts who include scholars and practitioners in the field of software security and/ or the AIS. Each of the sub characteristics and the weighting is explained below.

A. Confidentiality

Confidentiality assesses how much protection from unauthorized disclosure the AIS given to the data/ information contained in the system. Data/ information on AIS of a university can only be accessed by the university's stakeholders. In this case the students, faculty and academic staff. Confidentiality has 11 metrics which consist of access controllability, Access control to AIS source code, protection of log information, protection of AIS test data, controls against malicious code, management of removable media, session time-out, strength of cryptographic algorithms, data encryption correctness, and cryptographic key management. Confidentiality has weighting value of 0.21. The weighting of each confidentiality metrics is shown in "**Table 1.**"

B. Integrity

Integrity assesses how accurate and complete AIS assets can be maintained. In AIS, the asset in question is data/ information related to academic processes at universities such as student academic data. Integrity has 7 metrics which consist of data integrity conformance, internal data corruption prevention, inventory of assets, information back-up, documented operating procedures, AIS fault logging, and security of AIS documentation. Integrity has weighting value of 0.22. The weighting of each metric in integrity sub characteristic is shown in "**Table 2.**"

C. Accountability

Accountability assesses how far the activities of an entity (user or system) can be uniquely traced back to the entity itself. Data/ information on AIS can only be accessed by the stakeholder of the University's AIS owner. Some information has restrictions so that only the user with a certain authority is able to access the data. Accountability has 3 metrics which consist of access auditability, audit logging, and system log retention conformance. Accountability has weighting value of 0.13. The weighting of each metric in accountability sub characteristic is shown in "**Table 3.**"

D. Authenticity

Authenticity assesses how far the subject's identity, which can be either a user or system, can be proven true. In AIS, there are various users with different interests and access rights. So it is necessary to prove the identity of users so that the data/ information can be protected from unauthorized disclosure. Authenticity has 5 metrics which consist of authentication protocol conformance, user registration, user password management, privilege management, and information access restriction. Authenticity has weighting value of 0.23. The weighting of each authenticity metrics is shown in "**Table 4.**"

E. Security Compliance

Security compliance assesses the extent of AIS following the standards and regulations in force, in particular those relating to system security. This sub characteristic is important because of the nature of AIS itself that change according to regulations applicable, both legislation and academic regulations of each university. Security compliance has 3 metrics which consist of identification of applicable legislation, data protection of personal information, and regulation of cryptographic controls. Security compliance has weighting value of 0.21. The weighting of each metric in security compliance sub characteristic is shown in "**Table 5.**"

III. EVALUATION

The proposed security quality measurement framework is used to measure the security quality of a case study. Quality measurements using existing security quality metrics against the same case study is also conducted. Quality metrics being used is the security sub characteristic of ISO/ IEC DIS 25023. The measurement results are then compared. Moreover, AIS case study is then reengineered based on the recommendations of proposed framework's measurement results. Then the quality measurement results are compared and analyzed.

AIS tested is a prototype of Institut Teknologi Sepuluh Nopember (ITS) AIS's assessment module. The prototype was developed using ASP.NET programming language. While the database management system used is Microsoft SQL Server 2008. The functionality provided, among others, are as follows:

1) Students grading
2) Lecturers performance evaluation
3) Lecturers questionnaire
4) Grades reporting
5) Lecturers grades (Indeks Prestasi Dosen) reporting

A. Quality Measurement using Proposed Security Quality Measurement Framework and ISO/IEC DIS 25023

AIS study case's security quality is measured using the proposed framework and ISO/IEC DIS 25023. Comparison of the measurement results can be seen in "**Table 6.**" and "**Table 7.**" The proposed framework measures some aspects that are not considered by ISO/ IEC DIS 25023. This is manifested by the presence of 20 additional metrics which consist of access control to AIS source code metric, protection of log information metric, protection of AIS test data metric, control against malicious code metric, management of removable media metric, session time-out metric, cryptographic key management metric, inventory of assets metric, information back-up metric, documented operating procedures metric, AIS fault logging metric, security of AIS documentation metric, audit logging metric, user registration metric, user password management metric, privilege management metric, information access restriction metric, identification of applicable legislation metric, data protection of personal information metric, and regulation of cryptographic controls metric.

Measuring the security quality using ISO / IEC 25023 cannot generate sub characteristics values and a security value. That is because ISO/ IEC 25023 do not have weighting so the metrics values cannot be aggregated. So the measurement results can only be compared to the metrics level without weight. The results of measurements with the proposed framework can generate security value of 0.896384. Security value resulting from measurement using measurement framework security quality is ranged from 0 to real infinite positive numbers. The greater the security value, the better the security quality of AIS tested.

Furthermore, because of its generality, not all metrics are applicable to measure the case study. For instance, the utilization of digital signature metric was not used. Utilization of digital signature metric deals with the systems' connection and data delivery to outside parties or third parties. University's AIS does not have much to do with the system outside of the scope of the university itself. So it does not need security protection in the form of digital signatures in the data transmission.

B. Quality Measurement on Existing System and Reengineered System

After measuring the quality of ITS AIS's security using proposed framework, the system was then reengineered. The reengineered system subsequently re-measured using the proposed framework and compared with the results of measurements of the old system/ the existing system. Comparison of the existing system's measurements with the re-engineered system's measurements can be seen in "**Table 8.**", "**Table 9.**", and "**Table 10.**" The re-engineered system has increase values in some metric that causes an increase in the value of sub characteristics. Such improvements appeared in four sub characteristics. Security compliance sub characteristic cannot be measured because when the systems were tested, there were no specific regulations about the security of AIS. "**Figure 1.**" illustrates the comparison of sub characteristics measurement values between the existing system and the reengineered system. The improvement in sub characteristics values caused an increase in the system's security value from 0.896384 to 1.036912. The percentage increase then can be calculated using the following equation:

$$\%increase = (B - A) \div A \times 100 \quad (1)$$

where A is the old security value and B is the new security value. The calculation results show that the security value of AIS study case is increased by 15.6%.

IV. CONCLUSION

The evaluation results indicate that the proposed framework has several advantages from the existing security quality measurement metrics. Proposed framework can generate sub characteristic values and a security value using a weighting system that has been tailored to the needs of AIS application domain. Proposed framework also able to assess some aspects of security that are not considered by the existing security quality standard. Additional security aspects can be measured with 20 additional metrics in the proposed framework. In addition to the security value, measuring AIS using the proposed framework also reveals AIS's weakness so that it can be used next as a recommendation to update the system. Proposed framework can improve the security quality of AIS case study. It is shown by an increase in the security value of 15.6% on the system that has been reengineered according to recommendations resulting from previous measurements.

Due to limitations of the data set, the proposed framework is only tested on a prototype of ITS AIS. There are some metrics relating to the operational security of the system that cannot be measured. Measuring AIS which already is in the operational phase can be a consideration for future research. That way, the security quality measurement result can even be more comprehensive.

TABLE 1.
CONFIDENTIALITY METRICS WEIGHTING

Metric name	Weight
Access controllability	0.11
Access control to AIS source code	0.11
Protection of log information	0.09
Protection of AIS test data	0.08
Controls against malicious code	0.1
Management of removable media	0.09
Session time-out	0.11
Strength of cryptographic algorithms	0.1
Data encryption correctness	0.11
Cryptographic key management	0.1

TABLE 2.
INTEGRITY METRICS WEIGHTING

Metric name	Weight
Data integrity conformance	0.16
Internal data corruption prevention	0.16
Inventory of assets	0.14
Information back-up	0.15
Documented operating procedures	0.16
AIS fault logging	0.13
Security of AIS documentation	0.12

TABLE 3.
ACCOUNTABILITY METRICS WEIGHTING

Metric name	Weight
Access auditability	0.36
Audit logging	0.32
System log retention conformance	0.32

TABLE 4.
AUTHENTICITY METRICS WEIGHTING

Metric name	Weight
Authentication protocol conformance	0.21
User registration	0.19
User password management	0.19
Privilege management	0.21
Information access restriction	0.21

TABLE 5.
SECURITY COMPLIANCE METRICS WEIGHTING

Metric name	Weight
Identification of applicable legislation	0.35
Data protection of personal information	0.35
Regulation of cryptographic controls	0.3

TABLE 6.
COMPARISON OF SECURITY QUALITY MEASUREMENT

Metric name	Proposed framework result	ISO/IEC DIS 25023 result
Confidentiality		
Access controllability	1	1
Access control to AIS source code	0.6	-
Protection of log information	N/A	-
Protection of AIS test data	N/A	-
Controls against malicious code	1	-
Management of removable media	0.66	-
Session time-out	30	-
Strength of cryptographic algorithms	N/A	N/A
Data encryption correctness	0	0
Cryptographic key management	0	-
Integrity		
Data integrity conformance	1	1
Internal data corruption prevention	N/A	N/A
Inventory of assets	0	-
Information back-up	N/A	-
Documented operating procedures	N/A	-
AIS fault logging	0	-
Security of AIS documentation	N/A	-
Validity of array accesses	-	N/A
Non-repudiation		
Utilization of digital signature	-	N/A
Accountability		
Access auditability	0	0
Audit logging	0	-
System log retention conformance	N/A	N/A

TABLE 7.
COMPARISON OF AUTHENTICITY AND SECURITY COMPLIANCE QUALITY MEASUREMENT

Metric name	Proposed framework result	ISO/IEC DIS 25023 result
Authenticity		
Authentication protocol conformance	0.5	1
User registration	0.4	-
User password management	0.2	-
Privilege management	1	-
Information access restriction	0	-
Authentication rules conformance	-	N/A
Security compliance		
Identification of applicable legislation	N/A	-
Data protection of personal information	N/A	-
Regulation of cryptographic controls	N/A	-

TABLE 8.
COMPARISON OF CONFIDENTIALITY AND INTEGRITY ON REENGINEERING MEASUREMENT RESULT

Metric name	Existing system result	Existing system result with weight	Reengineered system result	Reengineered system result with weight
Confidentiality				
Access controllability	1	0.11	1	0.11
Access control to AIS source code	0.6	0.066	0.6	0.066
Protection of log information	N/A	N/A	0.67	0.0603
Protection of AIS test data	N/A	N/A	N/A	N/A
Controls against malicious code	1	0.1	1	0.1
Management of removable media	0.66	0.0594	0.66	0.0594
Session time-out	30	3.3	30	3.3
Strength of cryptographic algorithms	N/A	N/A	N/A	N/A
Data encryption correctness	0	0	0	0
Cryptographic key management	0	0	0	0
Integrity				
Data integrity conformance	1	0.15625	1	0.15625
Internal data corruption prevention	N/A	N/A	N/A	N/A
Inventory of assets	0	0	0	0
Information back-up	N/A	N/A	N/A	N/A
Documented operating procedures	N/A	N/A	N/A	N/A
AIS fault logging	0	0	1	0.12
Security of AIS documentation	N/A	N/A	N/A	N/A

TABLE 9.
COMPARISON OF ACCOUNTABILITY, AUTHENTICATION, AND SECURITY COMPLIANCE ON REENGINEERING MEASUREMENT RESULT

Metric name	Existing system result result	Existing system result with weight	Reengineered system result	Reengineered system result with weight
		Accountability		
Access auditability	0	0	1	0.37
Audit logging	0	0	0.7	0.224
System log retention conformance	N/A	N/A	N/A	N/A
		Authentication		
Authentication protocol conformance	0.5	0.105	1	0.21
User registration	0.4	0.076	0.4	0.076
User password management	0.2	0.038	0.2	0.038
Privilege management	1	0.21	1	0.21
Information access restriction	0	0	0	0
		Security compliance		
Identification of applicable legislation	N/A	N/A	N/A	N/A
Data protection of personal information	N/A	N/A	N/A	N/A
Regulation of cryptographic controls	N/A	N/A	N/A	N/A

TABLE 10.
COMPARISON OF SUB CHARACTERISTICS ON REENGINEERING MEASUREMENT RESULT

Sub characteristics	Existing system result	Existing system result with weight	Reengineered system result	Reengineered system result with weight
Confidentiality	3.6354	0.7634	3.6957	0.7761
Integrity	0.16	0.0352	0.28	0.0608
Accountability	0	0	0.594	0.0772
Authenticity	0.425	0.0977	0.53	0.1228
Security compliance	N/A	N/A	N/A	N/A
Security value	0.896384		1.036912	

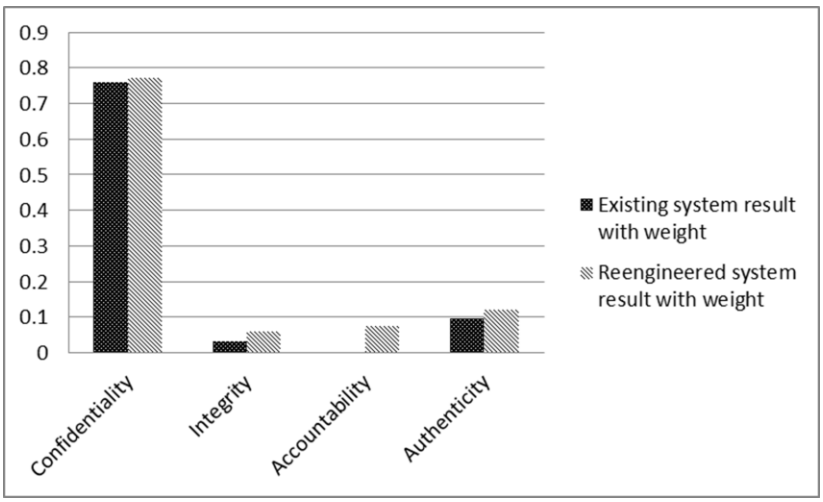

Figure. 1. Comparison between existing system sub characteristics measurement result and the reengineered system sub characteristics measurement result

REFERENCES

[1] BAN-PT, Buku II Standar dan Prosedur AIPT. Jakarta, Badan Akreditasi Nasional Perguruan Tinggi, 2011.

[2] Galin, D., Software Quality Assurance: From theory to implementation. London, Pearson, 2004.

[3] Suman and Wadhwa, M., "A Comparative Study of Software Quality Models," International Journal of Computer Science and Information Technologies, pp.5634–5638, 2014.

[4] ISO/IEC JTC 1, "9126-1 Information Technology - Software Product Quality - Part 1 : Quality Model." Geneva, ISO/IEC, 2000.

[5] ISO/IEC JTC 1, "Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Software and quality in use models". ISO/IEC, 2008.

[6] ISO/IEC JTC 1, "Systems and Software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality measure elements". ISO/IEC, 2011.

[7] Behkamal, B., Kahani, M., & Kazem Akbari, M., "Customizing ISO 9126 quality model for evaluation of B2B application," Information and Software Technology, vol. 51, pp.599–609, 2009.