JOURNAL LA MULTIAPP

VOL. 05, ISSUE 05 (732-739), 2024
DOI: 10.37899/journallamultiapp.v5i5.1626

Security Quality Measurement Based on ISO/IEC 25023 Quality Model Case Study: Hospital Management Information System

Nungky Taniasari[1], Mohamad Shodikin[2]

[1]*Faculty of Health Science, Universitas Anwar Medika, Sidoarjo, Indonesia*
[2]*Faculty of Sciences and Technology, Universitas Anwar Medika, Sidoarjo, Indonesia*

**Corresponding Author: Nungky Taniasari*
Email: nungkytaniasari@yahoo.com

Article Info

Article history:
Received 7 September 2024
Received in revised form 16 October 2024
Accepted 5 November 2024

Keywords:
Hospital Management Information System
Security Audit

Abstract

Hospitals need to protect the security of data assets, where data assets are an important part of the continuity of hospital operations. In connection with the protection of data and information assets in the hospital, it has become a requirement for the hospital information technology team to carry out a security audit of the hospital management information system (HMIS). In this study, we measured the quality of the HMIS software in X Hospital using ISO 25023 which focused on the security aspects of the outpatient service module and drug services in the outpatient pharmacy unit. The security aspect based on the ISO 25023 standard consists of five main characteristics, namely: confidentiality, integrity, non-repudiation, accountability and authenticity. In the early stages, calculations are carried out to find the value of each measurement standard which is denoted by (X). The X value is based on the standard calculation range of values 0 and 1. The threshold value is determined at 0.80 to categorize the point quality whether it is not good or has met the ISO 25023 quality point. The results of software quality measurements show Internal Data Corruption Prevention is worth 0.75 and is at below a predetermined threshold value. Based on these results, it is recommended to improve one of them by replication the database to minimize the possibility of Internal Data Corruption Prevention. In this study, all aspects of software quality have an average value above the threshold, so it can be concluded that HMIS in RS X meets ISO 25023 standards.

Introduction

Along with the development of digital transformation in health care facilities such as hospitals that are getting bigger, the security risks inherent in information are also getting bigger. Hospitals really need to protect the security of data assets, considering that data assets are an important part of the continuity of the hospital's operational processes. In connection with the protection of data and information assets in the hospital, it has become a requirement for the hospital information technology team to conduct a security audit of the hospital management information system (HMIS), which has never been done before (Kemboi, 2020; Amankwah, 2019; Yuhana Ashikin, 2020).

An audit is needed to find out the current condition compared to the real condition. One of the latest standards published by the International Organization for Standardization (ISO) for Measurement of System and Software Product Quality is ISO 25023 (Nasional, 2009; Komiyama et al., 2020; Aziz et al., 2018). This standard is a guideline and principles for initiating, implementing, maintaining, and improving information security management

ISSN: 2716-3865 (Print), 2721-1290 (Online)

within an organization and to provide guidance on developing organizational security standards (Xu et al., 2013; Ganji et al., 2019; Ganji et al., 2019).

In this study we measure software quality using ISO 25023 with focusing on security aspects. We apply measurements to the HMIS that has been used by X Hospital located in Sidoarjo district in carrying out operational services to patients. This HMIS has been implemented in RS X since 2019 and until now there has never been a measurement of software quality on the security aspect. The service module that will measure the quality of the software is the outpatient service module and drug service in the outpatient pharmacy unit (Craig et al., 2001). This service module was chosen due to the high number of patients that must be served in one day and this module has implemented electronic prescriptions. This research is expected to provide recommendations for system improvement on security aspects according to the ISO 25023 standard which includes Confidentiality, Non-repudiation, Accountability and Authenticity (Saptarini et al., 2017; Correa et al., 2022).

HMIS in RS X uses the Hypertext Pre-processor (PHP) programming language with the CodeIgniter and PostgreSQL frameworks as databases. The CodeIgniter framework is one of the most widely used PHP frameworks for developing websites (Da-gang, 2009). CodeIgniter was chosen because it has very rich functionality to speed up website development and provides a lot of security to prevent applications from different attacks (Solanki et al., 2017; Adamu et al., 2020).

This research was conducted in several stages of the work process. The first stage includes the main roles and functions of each HMIS user. The second stage will define the aims and objectives of each security aspect measurement standard to calculate the system according to ISO 25023 standards. The calculation standards used are standard values of 0 and 1. The final stage is data analysis. The results of the study can be used to formulate recommendations for improving the quality of HMIS security in X Hospital.

Methods

The methodology used for measuring security quality at HMIS using ISO 25023 can be seen in Figure 1 below.

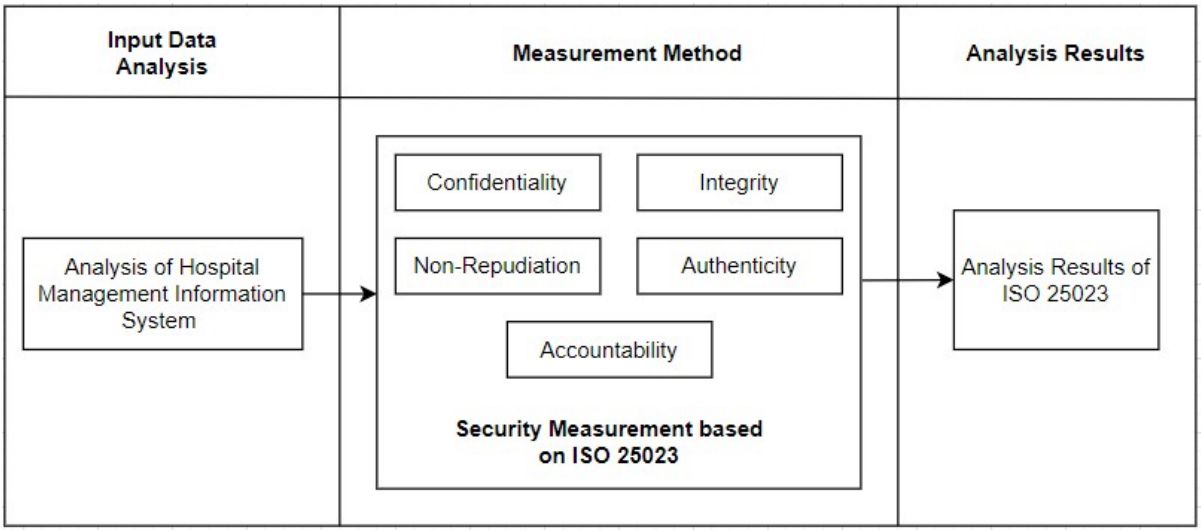


Figure 1. Research Methodology

Based on Figure 1, it shows that data collection through the HMIS direct observation method used in X Hospital is based on predetermined metrics. Measurement of the five aspects of HMIS security quality can be explained as follows:

Confidentiality

ISSN: 2716-3865 (Print), 2721-1290 (Online)

The confidentiality aspect has 3 quality points, namely: 1) Access Controllability which measures the proportion of data confidentiality that is protected from unauthorized access; 2) Data Encryption Correctness which measures the correctness of the application of encryption/description whether it is in accordance with the requirement specifications; 2) Strength of Cryptographic Algorithms which measures how many cryptographic algorithms have been used.

Integrity

The Integrity aspect has 3 quality points, namely: 1) Data Integrity conformance which measures the extent to which the destruction or modification of data is protected from unauthorized access; 2) Internal Data Corruption Prevention which measures the extent to which prevention methods are available in terms of data destruction; 3) Validity of Array Accesses which measures the extent to which each input is validated for user access rights.

Non-repudiation

The non-repudiation aspect has quality points, namely: the use of digital signatures which measures the proportion of events that are processed using digital signatures.

Accountability

The accountability aspect has 2 quality points, namely: 1) Access Auditability which measures how complete the system can monitor and record user access activities to certain resources or data; 2) System Log Retention Conformance which measures what percentage of log duration is stored with stable storage.

Authenticity

The authenticity aspect has 2 quality points, namely: 1) Authentication Protocol Conformance which measures how well the authenticate system can identify subjects or resources; 2) Authentication Rules Conformance which measures the proportion of authentication rules required to establish that a system is secure.

Results and Discussion

The initial stage of measuring HMIS security quality is by calculating the value of each measurement standard which is denoted by (X) (Nasional, 2009). The X value is based on the standard calculation range of values 0 and 1. The steps for measuring the quality of security based on ISO 25023 are divided into 5 main characteristics (Nasional, 2009).

Confidentiality

Confidentiality section, have 3 quality points which are the main focus of measurement, namely Access Controllability, Data Encryption Correctness, and Strength of Cryptographic Algorithm.

Access Controllability is measured by counting how many features on the HMIS menu can be accessed without access rights or login. HMIS uses the CodeIgniter framework which has standard security and session functionality which requires that access to features on the menu must already have a login and the session validity period has not expired.

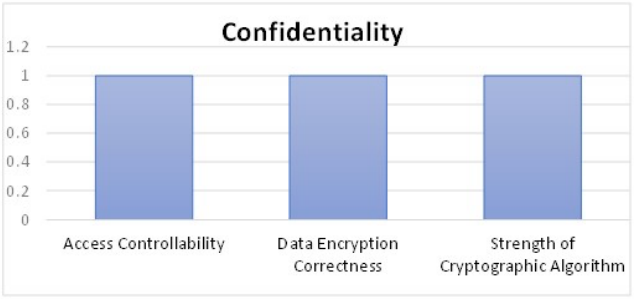
HMIS already has a feature for setting user access rights to each feature on the menu. From these data it can be calculated that the value of Access Controllability at HMIS has a value of:

Data Encryption Correctness is calculated by checking the correctness of the application of encryption in the process of exchanging data on the internet. One of the methods that can be used for encryption is the SSL method. SSL aims to provide public key authentication and

ISSN: 2716-3865 (Print), 2721-1290 (Online)

certificate-based private keys that are used to create session keys, and secret data traffic security based on symmetric keys (Das & Samdaria, 2014).

HMIS already has an SSL certificate so that website access uses the https protocol so that data exchange is not found without proper encryption. From this data it can be calculated that the Data Encryption Correctness value at HMIS has a value of 1. Strength of Cryptographic Algorithm can be measured by calculating how much the system has accommodated cryptographic needs. HMIS only uses algorithms cryptography to change password characters that have been stored in the database according to (Andress, 2014). So that the Strength of Cryptographic Algorithm has a value of 1 because no algorithm requirements are found other cryptography that has not been implemented.



Confidentiality	
Quality Points	**Value**
Access Controllability	1
Data Encryption Correctness	1
Strength of Cryptographic Algorithm	1

Figure 2. Confidentiality Measurement Result

Integrity

Integrity section, have 3 quality points which are the main focus of measurement, namely Data Integrity conformance, Internal Data Corruption Prevention, and Validity of Array Accesses.

Data integrity conformance can be measured by measuring the system's capability against data damage threats such as Cross-Site Scripting, Cross-site Request Forgery, Cookie Attack, Sql Injection. Prevention of these 4 types of threats can already be handled by the system by implementing the CodeIgniter framework library (Solanki et al., 2017).

HMIS was developed using the CodeIgniter framework and has implemented a library for prevention of these 4 types of threats, so Data Integrity conformance has a value of 1. Internal Data Corruption Prevention can be measured by the extent to which the availability of methods has been applied to several possible damages, such as damage to the hardware level and storage (Bairavasundaram et al., 2008) and damage to the Database Management System (DBMS) level (Bohannon et al., 2003). For damage prevention at the hardware and storage level, the HMIS server has implemented Redundant Array of Independent Disks (RAID) (Shooman & Shooman, 2012) level 5. Prevention at the DBMS level can be done with DBMS replication and data backup (Amrullah, 2023), in this case the HMIS database has been backed up. regularly on cloud servers, but have not implemented the DBMS replication method, so Data Corruption Prevention on HMIS has a value of 0.75. The validity of Array Accesses can be measured by measuring the extent to which user input is validated. According to (Saidhi et al., 2023) the Validity of Array Accesses can be measured by 11 kinds of input validity as can be seen in Table 1.

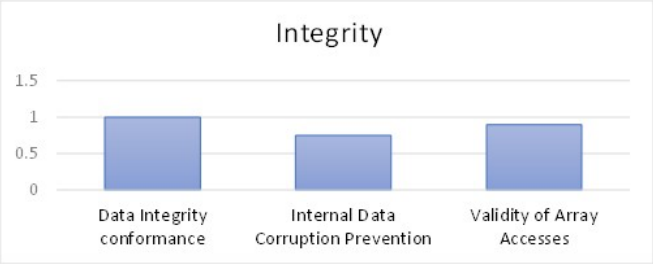
Table 1. Validity Of Array Accesses Measurement

Validity of Array Accesses	Available on system
Validate input attribute with value true or false	Yes
Implement code validators like required, in, date etc	Yes
The validation of the login attribute value is that the user is still valid	Yes
Validate attribute values according to table data types	Yes

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Validate if the attribute accepts a valid file upload	yes
Attribute value validation is in the specified parameter range	No
Attribute length validation has a certain length	Yes
Attribute value validation is a number	Yes
Validate attribute values with customizing error messages	Yes
Attribute value validation is not null or empty value	Yes
Attribute validation if it meets certain conditions	Yes

In Table 1 HMIS implements 10 of 11 types of input validity so that the Validity of Array Accesses has a value of 0.90.



Integrity	
Quality Points	**Value**
Data Integrity conformance	1
Internal Data Corruption Prevention	0.75
Validity of Array Accesses	0.9

Figure 3. Integrity Measurement Result

Non-repudiation

Non-repudiation measures the extent to which any action or transaction made by a user can be accounted for and cannot be rejected if necessary. Non-repudiation has a digital signature utilization quality point that measures the proportion of events that are processed using a digital signature. HMIS only applies digital signatures to electronic prescriptions. HMIS has limited access to making electronic prescriptions to doctors, dentists and veterinarians according to (Pravika, 2019). From these data it can be calculated that the Non-repudiation value has a value of 1.

Accountability

The Accountability section has 2 quality points which are the main focus of measurement, namely Access Auditability and System Log Retention Conformance.

Access Auditability can be measured by measuring the ability of the system to record all user access activities in each feature on the menu. The HMIS used for this study has recorded users accessing the features on the menu so that the Access Auditability value is 1. From these data it can be calculated that the Access Auditability value at HMIS has a value of 1. System Log Retention Conformance can be measured by measuring how long the log period is maintained in stable storage and the retention period required to maintain system logs in stable storage. All feature access on HMIS is recorded in the system log and data backup on the nas server without storage allocation limitations. So that the System Log Retention Conformance value is 1.

Accountability	
Quality Points	**Value**
Access Auditability	1
System Log Retention Conformance	1

Figure 4. Accountability Measurement Result

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Authenticity

Authenticity section, have 2 quality points which are the main focus of measurement, namely Authentication Protocol Conformance and Authentication Rules Conformance.

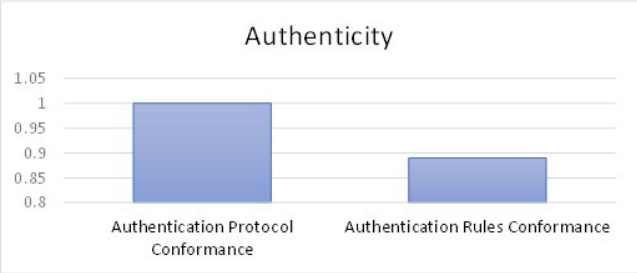
Authentication Protocol Conformance can be measured by measuring the system's ability to identify subjects or resources. HMIS has implemented a Password Authentication Protocol which validates the user's identity by comparing the password entered by the user with that stored in the database. So that Authentication Protocol Conformance on HMIS has a value of:

Authentication Rules Conformance can be measured by measuring the ability of the system to apply authentication rules to ensure that the system is secure. According to (Maulana et al., 2020) to secure the suitability of authentication it is proposed to use 9 kinds of authentication rules as can be seen in Table 2.

Table 2. Authentication Rules Conformance Measurement

Authentication Rules Conformance	Available on system
Defining identity class	No
Login and logout	Yes
Session based login	Yes
Access control filters	Yes
Handling of authorization results	Yes
Role-based access control	Yes
configuration permissions with permissions manager	Yes
Defines an authorization hierarchy	Yes
Using business rules	Yes

In Table 2 HMIS fulfills 8 out of 9 authentication rules so Authentication Rules Conformance has a value of 0.89.



Authenticity	
Quality Points	**Value**
Authentication Protocol Conformance	1
Authentication Rules Conformance	0.89

Figure 5. Authenticity Measurement Result

Conclusion

In this study, we measured the quality of software using the PHP programming language with the CodeIgniter framework and PostgreSQL as databases. Measurements were carried out using the ISO 25023 standard with limitations focusing on five security aspects, namely: Confidentiality, Integrity, Nonrepudiation, Accountability, and Authenticity. From the measurement results, a threshold value of 0.80 is determined to categorize the quality point whether it meets ISO 25023 quality points. From the results of software quality measurements, the Internal Data Corruption Prevention quality point is 0.75 and is below the predetermined threshold value. Based on these results, it is recommended to improve one of them by mirroring the database to minimize the possibility of Internal Data Corruption Prevention. In this study, all aspects of software quality have an average value above the threshold, so it can be concluded that HMIS in RS X meets ISO 25023 standards.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

References

Adamu, J., Hamzah, R., & Rosli, M. M. (2020). Security issues and framework of electronic medical record: A review. *Bulletin of Electrical Engineering and Informatics*, *9*(2), 565-572. https://doi.org/10.11591/eei.v9i2.2064

Amankwah, M. A. B. (2019). *Assessment of Electronic Health Management Information System at University of Ghana Hospital* (Doctoral dissertation, University of Ghana).

Amrullah, A. (2023). *BELAJAR CEPAT DATABASE NoSQL: Menggunakan Document Oriented Database (MongoDB) pada Pengaplikasian Big Data*. Penerbit Andi.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Aziz, M. N., Sapta, I. M., & Rochimah, S. (2018, October). Security characteristic evaluation based on ISO/IEC 25023 quality model, case study: Laboratory management information system. In *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)* (pp. 332-336). IEEE. https://doi.org/10.1109/EECCIS.2018.8692982

Bairavasundaram, L. N., Arpaci-Dusseau, A. C., Arpaci-Dusseau, R. H., Goodson, G. R., & Schroeder, B. (2008). An analysis of data corruption in the storage stack. *ACM Transactions on Storage (TOS)*, *4*(3), 1–28. https://dl.acm.org/doi/abs/10.1145/1416944.1416947

Bohannon, P., Rastogi, R., Seshadri, S., Silberschatz, A., & Sudarshan, S. (2003). Detection and recovery techniques for database corruption. *IEEE Transactions on Knowledge and Data Engineering*, *15*(5), 1120–1136. https://doi.org/10.1109/TKDE.2003.1232268

Correa, E. B. E., Sousa, J. C., Abelém, A. J. G., & Oliveira, S. R. B. (2022). An evaluation of Security Features based on Iso/Iec 25023 for a Distributed Autonomic Scientific Publisher Tool on a Permissioned Blockchain. *JISTEM-Journal of Information Systems and Technology Management*, *19*, e202219020. https://doi.org/10.4301/S1807-1775202219020

Craig, S., Crane, V. S., Hayman, J. N., Hoffman, R., & Hatwig, C. A. (2001). Developing a service excellence system for ambulatory care pharmacy services. *American journal of health-system pharmacy*, *58*(17), 1597-1606. https://doi.org/10.1093/ajhp/58.17.1597

Da-gang, G. (2009). Analysis of model-based mvc framework for php development codeigniter. *Jiangxi Sci*, *5*, 22.

Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. *Applied Computing and Informatics*, *10*(1–2), 68–81. https://doi.org/10.1016/j.aci.2014.02.001

Ganji, D., Kalloniatis, C., Mouratidis, H., & Gheytassi, S. M. (2019). Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review. *Int. J. Adv. Softw*, *12*(3).

Kemboi, L. (2020). *Security control model for electronic health records* (Doctoral dissertation).

Komiyama, T., Fukuzumi, S. I., Azuma, M., Washizaki, H., & Tsuda, N. (2020). Usability of software–intensive systems from developers' point of view: Current status and future perspectives of international standardization of usability evaluation. In *Human-Computer Interaction. Design and User Experience: Thematic Area, HCI 2020, Held as Part of the 22nd International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part I 22* (pp. 450-463). Springer International Publishing. https://doi.org/10.1007/978-3-030-49059-1_33

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Maulana, M. S., Sabaruddin, R., & Nurmalasari, N. (2020). Rancang bangun dashboard smart system manajemen rt/rw untuk mendukung society 5.0. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *8*(4), 328–332. http://dx.doi.org/10.26418/justin.v8i4.42586

Nasional, B. S. (2009). Pengantar standardisasi. *Jakarta: BSN*, *198*.

Pravika, U. H. (2019). *Implementasi hiperkes dan keselamatan kerja serta lingkungan di PT aNtam Tbk. Ubpe Pongkor*.

Saidhi, R., Derta, S., Musril, H. A., & Okra, R. (2023). PERANCANGAN APLIKASI VIDTORGA PADA MATAPELAJARAN PJOK KELAS X DI SMKN 1 AMPEK ANGKEK. *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, *6*(2), 222–246. https://doi.org/10.37792/jukanti.v6i2.1004

Saptarini, I., Rochimah, S., & Yuhana, U. L. (2017). Security Quality Measurement Framework for Academic Information System (AIS) Based on ISO/IEC 25010 Quality Model. *IPTEK Journal of Proceedings Series*, *3*(2), 128-135. http://dx.doi.org/10.12962/j23546026.y2017i2.2310

Shooman, A. M., & Shooman, M. L. (2012). A comparison of RAID storage schemes: Reliability and efficiency. *2012 Proceedings Annual Reliability and Maintainability Symposium*, 1–6. https://doi.org/10.1109/RAMS.2012.6175446

Solanki, N. V, Solanki, D. B., & Shah, R. R. (2017). Patient Satisfaction with Services in Out-Patient Department at Tertiary Care Hospital of Patan District, Gujarat. *National Journal of Community Medicine*, *8*(06), 334–337.

Xu, H., Heijmans, J., & Visser, J. (2013). A practical model for rating software security. *2013 IEEE Seventh International Conference on Software Security and Reliability Companion*, 231–232. https://doi.org/10.1109/SERE-C.2013.11

Yuhana Ashikin, G. (2005). *Hospital management information system/Yuhana Ashikin Ghazali* (Doctoral dissertation, Universiti Malaya).

ISSN: 2716-3865 (Print), 2721-1290 (Online)