



# SECURITY QUALITY INSTRUMENT

## IAIN PALOPO

---

**Submission date:** 15-Jan-2020 09:18AM (UTC+0700)

**Submission ID:** 1075690313

**File name:** EDIT\_SECURITY\_QUALITY\_INSTRUMENT.docx (112.97K)

**Word count:** 3737

**Character count:** 21344

# Quality Security Instrument For Academic Information System Based on Quality Model

## Abstract

The currently available academic information system software are not fully secure and provides quality assurance of academic information system software (AISS). Required quality instruments derived from the quality model as a determinant of the quality of academic information system software. The ISO/IEC 25010 quality model is a security quality instrument that must be contained in an academic information system software. ISO/IEC 25010 Quality Model Questionnaire is the most appropriate method of describing the ISO/IEC 25010 quality model as an instrument of the quality model required by an academic information system (AISS) software consisting of Basic Quality Questionnaire Method for AISS, Basic Quality Model Questionnaire Method, and Security Questionnaire Method. Five quality instruments that must be contained in an academic information system software (AISS) to create security are confidentiality, integrity, accountability, authenticity, and security compliance. The ISO / IEC 25010 quality model instrument is a guarantee of safe and high-quality software that is needed by an academic information system software (AISS).

**Key Words:** academic information system software, security quality instrument, quality model ISO/IEC 25010

## 1. Introduction

Academic information system software (AISS) is an information system in the form of software that provides academic services in an educational institution, college, or high school [1]. AISS helps users manage the operations of an educational institution that includes its activities so that it impacts the marketing of the educational institution. Based on its objectives, AISS has some differences with e-learning systems, which are educational systems that utilize information technology that uses electronics or computers that support the learning and teaching process. AISS is a software in electronic form or integrated computer system that supports learning, teaching, and organizing the business processes of a college or school. AISS is important because it can improve the operational efficiency and effectiveness of an educational institution specifically universities and high schools. The current AISS does not fully adopt the quality model as its systemic instrument [2]. Each of the quality models has different instruments [2]. The ISO/IEC 25010 quality model provides safety quality [3]. Safety is one important quality aspect that is highly considered. In academic information system software (AISS) security aspects related to data and information security, therefore an implemented security quality instrument must be able to provide security quality in the academic information system domain (AIS). Academic information systems (AIS) are currently being built using website-based applications [4]. Implementation of a website-based application quality model (WBAQM) is an implementation of the bottom up approach.

## 2. Teory

### 2.1. Software Quality Assurance

Software quality assurance is a match between functional and needs, software quality standards and the implicit characteristics expected of professional software developers. Based on IEEE software quality assurance is a plan and systematic pattern needed to produce products that meet the requirements, and a series of activities

created to carry out an evaluation process based on the product being built. The objectives of software quality assurance in software development are as follows:

1. Ensure the level of software confidence is based on requirements
2. Ensuring the level of confidence that the software will be in accordance with the specified time and development funds that have been determined to determine the requirements.
3. Initiation and management activities to increase and increase the efficiency of software development and software quality assurance.

### 2.2. Web-Based Applications Quality Model (WBAQM)

The Academic Information System (AISS) software implements WBAQM as the main framework for its system quality instrument. The academic information system software quality instrument is a quality measurement tool specifically implemented at AISS. At present, many AISSs are built using web-based applications [6]. WBAQM is built on different programming models, technologies and languages and is used to implement highly interactive applications that have very high quality requirements. ISO / IEC 25010: 2011 is a software quality standard that is widely used, especially in the security of an information system [7]. ISO / IEC 25010 is a quality model that improves the previous quality model ISO / IEC 9126 [8] by adding safety characteristics [3]. In addition, ISO / IEC 25010 is used because of its flexibility and generality. Implementation of the quality factors of the ISO / IEC 25010 quality model that has a security quality standard is the reason why the Web Based Application Quality Model (WBAQM) is the main framework of a Software Academic Information System (AISS).

### 3. Quality Model Questionnaire Method

Quality Model Questionnaire Method is a research method in the form of questions in the form of choices consisting of Basic Quality Questionnaire Method for AISS, Basic Quality Model

Questionnaire Method, and Security Questionnaire Method

*1. Basic Quality Questionnaire Method for AISS Attractiveness*

1. Annoying/Enjoyable
2. Bad/Good
3. Unlikeable/Pleasing
4. Unattractive/Attractive
5. Unfriendly/Friendly

Efficiency

1. Slow/Fast
2. Inefficient/Efficient
3. Impractical/Practical
4. Cluttered/Organized

Perspicuity

1. Not understandable/Understandable
2. Difficult to learn/Easy to learn
3. Complicated/Easy
4. Confusing/Clear

Dependability

1. Unpredictable/Predictable
2. Obstructive/Supportive
3. Not secure/Secure
4. Does not meet expectation/Meet expectation

Stimulation

1. Interior/Valuable
2. Boring/Exiting
3. Not interesting/Interesting
4. Demotivating/Motivating

Novelty

1. Dull/Creative
2. Conventional/Inventive
3. Usual/Leading edge
4. Conservative/Innovative

*2. Basic Quality Model Questionnaire Method*

*A. The choice of parameters below is the most appropriate parameter describing the ISO / IEC 25010 quality model as a quality model.*

\* The ISO / IEC 25010 quality model is a quality model that enhances the ISO / IEC 9126 quality model / The 25010 quality model is the opposite of the ISO / IEC 9126 quality model.

\* ISO / IEC 25010 quality models have safety quality instruments / ISO / IEC 25010 quality models focus on usability quality instruments.

\* Protection of data and information contained in a system is a function of quality confidentiality instruments / ISO / IEC 25010 unable to protect data and information.

\* Ability to maintain and maintain data and information so that data integrity is compatible with the safety documentation of the ISO / IEC 25010 quality model / Inability to maintain data integrity.

\* The ability to assess how far an entity's activities (users or systems) can be traced back to the entity itself / ISO / IEC 25010 does not have the ability to instrument quality accountability.

\* ISO / IEC 25010 is able to assess how far the identity of the subject (system or user) can be

verified / ISO / IEC 25010 does not have authenticity quality instruments.

\* The security compliance quality instrument is the ability of the ISO / IEC 25010 quality model to follow applicable standards and regulations / The ISO / IEC 25010 quality model does not have a security compliance quality instrument.

\* ISO / IEC 25010 security quality model functions to guarantee the quality of security / The instrument of security quality does not guarantee the quality of security.

\* Safety is one of the important quality aspects that must be considered and not found in other quality models besides ISO / IEC 25010 / ISO / IEC 25010 is a quality model that is not focused on security.

*B. Security Questionnaire Method*

*1. The parameter selection below is the parameter that best describes the confidentiality of an instrument of security quality based on an ISO / IEC 25010 quality model on an AISS*

\* Ability to maintain the confidentiality of data for certain purposes and is only allowed for certain purposes / Confidentiality of data only for certain people.

\* Confidentiality is a protection of data and information / Confidentiality is a limitation of data and information.

\* Protection of data and information from unauthorized disclosure / Ignorance of data and information from unauthorized disclosure.

\* Data and information can only be accessed by authorized people / Data and information cannot be accessed and changed.

\* Confidentiality relates to data provided to other parties for certain purposes and is only allowed for certain purposes / Confidentiality does not relate to access to information.

\* The basic aspects of information security / Confidentiality are not basic aspects of system security.

*2. The choice of parameters below is the most appropriate parameter to describe the integrity of a security quality instrument based on the AISS ISO / IEC 25010 quality model*

\* Information may not be changed without the permission of the owner of the information / Information may be changed without the permission of the owner of the information

\* Information received must be exactly the same as when the information was sent / Information received does not have to be the same as when the information was sent.

\* Viruses, Trojan horses, other users are an integrity problem / Integrity problems lie in the system.

\* Access to change data and information can only be done by the rightful owner of the data and information / Anyone who has access to change data and information is the owner of the data and information.

\* Appropriate data integrity is needed to maintain and maintain data and information / Data integrity is not required from people who are not entitled to access information.

\* Ability to maintain and maintain data and information / Inability to maintain and maintain data and information.

3. The choice of parameters below is the most appropriate parameter describing an AISS-based ISO / IEC 25010 quality safety instrument

\* Data and information on AISS can only be accessed by stakeholder owners of AISS universities / AISS provide access to data and information to each user.

\* Some information has limitations so that only users with certain authority can access data / All information can be accessed without limitations by each system user.

\* Accountability is assessing the extent to which an entity's activities (users or systems) can be traced back until the entity itself / accountability is an assessment of user or system entities

4. The choice of parameters below is the parameter that best describes the authenticity of a security quality instrument based on the AISS ISO / IEC 25010 quality model

\* AISS has many users with different interests / AISS limits access because of the large number of users.

\* Users need to prove the user's identity so that data and information can be protected from unauthorized disclosure / AISS does not require verification when using the system.

\* Authenticity is an assessment of how far the identity of a subject that can be either a user or a system, can be proven true.

5. The choice of parameters below is the most appropriate parameter to describe the security compliance instrument of a quality security based on the AISS ISO / IEC 25010 quality model

\* The nature of AISS often changes according to applicable regulations / AISS is not flexible in responding to changes in regulations or regulations.

\* Security compliance is an assessment of the extent to which AISS follows applicable standards and regulations, especially those related to system security / System security is very important in AISS

\* AISS regulations refer to university academic rules and statutory rules / AISS rules in accordance with system rules.

#### 4. Results and Discussion

##### A. Academic Information System Software Quality Model.

The quality model is a quality instrument model that is implemented in an academic information system. A quality model whose quality instruments implement safety characteristics. The ISO / IEC 25010 quality model

is a quality model that implements the safety characteristics of the instrument. The structure of the security quality model in the academic information system is focused on the ISO / IEC 25010 quality model with five quality instruments namely confidentiality, integrity, accountability, authenticity, and security compliance.



Figure 1. Structure Model of Academic Information System Software Quality Security Based on ISO/IEC 25010 Quality Model

TABLE I  
QUALITY SECURITY INSTRUMENT SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 9126 QUALITY MODEL

Quality Instrument	Description
Confidentiality	Attempts to safeguard information by providing AISS data to other parties for certain purposes and are only allowed for that particular purpose.
Integrity	Quality that emphasizes that information must not be changed without seizing the information owner. The information received must be exactly the same as when the information was uploaded into AISS.

Accountability	Quality that emphasizes the extent of the activities of an entity (user or system) AISS can be traced back to the entity itself.
Authenticity	Efforts to assess how far the identity of the subject of an AISS, which can be a user or a system, can be proven true.
security compliance.	Quality that emphasizes the extent to which AISS follows applicable standards and regulations, especially those related to system security.

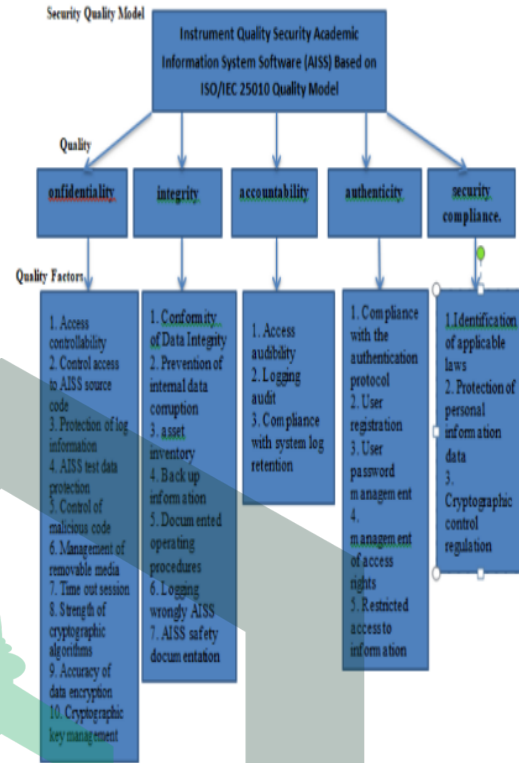


Figure 2. Quality Structure and Quality Factors of Security Instrument Quality Based on Quality Model ISO/IEC 25010

**B. Quality Structure and Instrument Quality Security Academic Information System Software (AISS) Based on ISO/IEC 25010 Quality Models**

In Figure 2 there is a quality structure and quality factor of the security quality of the instrument based on the quality of the ISO / IEC 25010 model which consists of three levels viz:  
 Level 1: Identify the quality perspective of the safety quality model  
 Level 2: Quality categorization of the instrument perspective on the quality of the model  
 Level 3: Mapping of quality factors against the perspective of the model quality instruments

The identification of the model quality instrument perspective is the first level of the quality security instrument based on the quality of the ISO / IEC 25010 model. The second level of security structure for instrument quality based on quality based on the ISO / IEC 25010 model is quality. There are 5 types of quality contained in the security quality instrument based on quality models, namely confidentiality, integrity, accountability, authenticity, and security compliance. The third level is the mapping of quality factors to the perspective of the model quality instruments namely the quality factors that become requirements, considerations, and the nature of each quality instrument.

**C. Security Quality Instrument Based on Quality Model ISO/IEC 25010**

Security quality instrument based on quality model ISO/IEC 25010 is a security quality model that implements five ISO / IEC 25010 based security instruments namely confidentiality, integrity, accountability, authenticity, and security.  
 1. Confidentiality  
 Confidentiality is an effort to safeguard information by providing AISS data to other parties for certain purposes and is only allowed for that particular purpose.

TABLE II  
 QUALITY CONFIDENTIALITY AS A QUALITY INSTRUMENT OF SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL

Quality Factor	Description
Access control	AISS access control is under user control
Control access to AISS source code	Restrict users to access information using the AISS source code
Log	Protect

<i>Confidentiality</i>	information protection	information against unauthorized access from an attacker.
	AISS test data protection	Protect AISS test results
	Control of malicious code	Limiting codes of unknown functions and benefits which can be active at any time and cause harm to AISS.
	Removable media management	The process of regulating removable media is computer storage media designed to be inserted and removed from AISS
	Session time out	The time the user is logged in but with no activity at all, consequently the user is logged out automatically
	The power of cryptographic algorithms	The functions of cryptographic algorithms are encryption, decryption and keys. This algorithm functions to hide information from people who are not entitled to the information.
	Data encryption accuracy	Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood.
	Cryptographic	The process of

	key management	regulating data security by private key and public key when doing encryption and decryption.
--	----------------	--

2. *Integrity* is a quality that emphasizes that information must not be changed without the permission of the owner of the information. The information received must be exactly the same as when the information was uploaded into AISS.

TABLE III  
QUALITY INTEGRITY AS A QUALITY INSTRUMENT OF SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL

Quality Factor	Description
Conformity of data integrity	The information or data that is received must match and exactly the same as when the information or data was sent.
Prevention of internal data corruption	Actions that prevent damage or loss of data
Asset inventory	Management of data and information to avoid damage or loss caused by viruses, Trojan horses, or other users who change information without permission.
Back up information	The process of backing up data by copying or archiving computer data so that the data can be reused if there is damage or loss.
Documented operating procedures	AISS operating procedures are created, documented, implemented and maintained
Logging is wrong AISS	Incorrect reports or records that

IAIPALOPC

		occur on AISS are caused by viruses, Trojan horses and hackers.
	AISS safety documentation	The process of collecting, selecting, processing and storing information and data from AISS as a security procedure.

4. *Accountability* is a quality that emphasizes the extent to which the activities of an entity (user or system) AISS can be traced back to the entity itself.

TABLE IV  
QUALITY ACCOUNTABILITY AS A QUALITY INSTRUMENT SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL

	Quality Factor	Description
Accountability	Access audibility	Access audibility is the possibility to assess whether a log system in an academic information system software (AISS) is functioning properly and is working properly
	Audit logging	Chronological records relevant to the security of access to an academic information system software (AISS)
	System log retention matches	Password compatibility when logging in the system.

4. *Authenticity* is an attempt to assess how far the entity of the subject of an AISS, which can be a user or a system, can be proven true.

TABLE V

QUALITY AUTHENTICITY AS A QUALITY INSTRUMENT OF SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL

	Quality Factor	Description
Authenticity	Authentication protocol compliance	Appropriate types of computer communication protocols or cryptographic protocols specifically designed for the transfer of authentication data between two entities
	User registration	User registration on an academic information system software.
	User password management	Better management of user passwords.
	Access rights management	Management of all user access rights
	Restricted access to information	Restrictions on accessing information are based on the access rights of each user.

5. *Security compliance* is an AISS effort that follows applicable standards and regulations, specifically those related to system security.

TABLE VI  
QUALITY SECURITY COMPLIANCE AS A QUALITY INSTRUMENT OF SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL

	Quality Factor	Description
Security compliance	Identification of applicable laws	Reviewing regulations regarding academic information systems from both educational institutions or laws
	Data protection for personal information	The method used to protect the user's personal

		information
	Cryptographic control regulation	The rules used check or supervise the security of the system

The academic quality security instrument based on the ISO / IEC 25010 quality model is a quality instrument contained in the ISO / IEC 25010 quality model consisting of confidentiality, integrity, accountability, authenticity, and security compliance.

The structure of academic quality information system security instruments based on the ISO / IEC 25010 quality model consists of three levels, namely:

Level 1: Identify the quality perspective of the safety quality model

Level 2: Quality categorization of the instrument perspective on the quality of the model

Level 3: Mapping of quality factors against the perspective of the model quality instruments

The identification of the instrument quality model perspective is the first level of the instrument quality security based on the ISO / IEC 25010 model quality. The instrument quality security based on the ISO / IEC 25010 model quality is a perspective that contains quality. The second level of security structure for instrument quality based on quality based on the ISO / IEC 25010 model is quality. There are 5 types of quality contained in the security quality instrument based on quality models, namely confidentiality, integrity, accountability, authenticity, and security compliance. The third level is the mapping of quality factors to the perspective of the model quality instruments namely the quality factors that become the requirements, considerations, and the nature of each quality instrument.

Academic Information System Software (AISS) is a software-based information system that is implemented in educational institutions, the implementation of which greatly benefits the university or school. AISS in operation really needs security. By implementing an ISO / IEC 25010 quality model based on security, it will create an academic information system software (AISS) that has quality security.

## 5. CONCLUSION

This paper examines a study of academic information system software security instruments based on ISO / IEC 25010 quality models. Quality Model Questionnaire is the most appropriate method of describing the ISO/IEC 25010 quality model as an instrument of the quality model required by an academic information system (AISS) software consisting of Basic Quality Questionnaire Method for AISS, Basic Quality Model Questionnaire Method, and Security Questionnaire Method. Where the academic information system software that is built

will have five security instruments namely confidentiality, integrity, accountability, authenticity, and security compliance. By implementing the five security quality instruments based on the ISO/IEC 25010 quality model, an academic information system (AISS) software that has quality security will be created.

## 6. REFERENCES

- [1] R.J. Salaki, Analysis and Design of Service Oriented Architecture Based in Public Senior High School Academic Information System, 2017 5<sup>th</sup> International Conference on Electrical, Electronics and Information Engineering (ICEEIE), p 180-186, DOI: 10.1109/ICEEIE.2017.8328785, (2017)
- [2]. I. Sulistiani, S. Syarif, Yusran, and Dewiani, Quality Models Engineering for Evaluation for Evaluation of Academic Information System Quality Instrument (AISQI), 2018 International conference on Applied Science and Technology (iCAST), p30-34. DOI:10.1109/iCAST.2018.8751525 (2018)
- [3]. B. Muthusenthil, C. Vijayakumar, H. Kim, Security and Privacy Framework for Academic Monitoring System, 2015 8<sup>th</sup> International Conference on Security Technology, p. 5-8, DOI: 10.1109/Sec—Tech.2015.9, (2015)
- [4]. M. L. Pandini, Z. Arifin, and D. M. Khairina, Design Web Service Academic Information System Based Multiplatform, 2014 1<sup>st</sup> International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), p. 297-302, DOI: 10.1109/ICITACEE.2014.7065760, (2014)
- [5]. IEEE, Standard Glossary of Software Engineering Terminology, The Institute of Electrical and Electronics Engineers, New York, IEEE Software Engineering Standards Collection 1991
- [6]. A.N. AbuAli, H.Y. Abu-Addose, A Comparative Study of Techniques Used for Evaluating Web Page Quality of the Public Organizations in Jordan, International Journal of Academic Research 3 (2), p. 65, (2011)
- [7]. ISO/IEC 25010:2011 System and Software Engineering-System and Software Quality Requirements and Evaluation (SQuaRE) System and Software Quality Models, Switzerland : BSI, (2011)
- [8]. ISO/IEC TR 9126-3, Software Engineering – Product Quality – Part 3: Internal Metrics. Japan: International Organization for Standardization, (2003)





**IAIN PALOPO**

# SECURITY QUALITY INSTRUMENT

## ORIGINALITY REPORT

16%

SIMILARITY INDEX

0%

INTERNET SOURCES

15%

PUBLICATIONS

15%

STUDENT PAPERS

## PRIMARY SOURCES

- 1** Ino Sulistiani, Syafruddin Syarif, Yusran, Dewiani. "Quality Models Engineering for Evaluation of Academic Information System Quality Instrument (AISQI)", 2018 International Conference on Applied Science and Technology (iCAST), 2018 9%

Publication
- 2** Siti Rochimah, Hanifa I. Rahmani, Umi Laili Yuhana. "Usability characteristic evaluation on administration module of Academic Information System using ISO/IEC 9126 quality model", 2015 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2015 1%

Publication
- 3** Submitted to University of Sheffield 1%

Student Paper
- 4** Submitted to Higher Education Commission Pakistan 1%

Student Paper
- 5** Sun, Yang, Hongbing Qian, and Xiaochen Liu.

"Evaluation and Measurement of Software Testing Process Quality Applicable to Software Testing Laboratory", 2015 Asia-Pacific Software Engineering Conference (APSEC), 2015.

Publication

1%

6

Garcia-Mundo, Lilia, Marcela Genero, and Mario Piattini. "Towards a Construction and Validation of a Serious Game Product Quality Model", 2015 7th International Conference on Games and Virtual Worlds for Serious Applications (VS-Games), 2015.

Publication

1%

7

Submitted to City University of Hong Kong

Student Paper

<1%

8

Submitted to University of Malaya

Student Paper

<1%

9

Lecture Notes in Computer Science, 2007.

Publication

<1%

10

Hela Hakim, Asma Sellami, Hanene Ben Abdallah. "Evaluating Security in Web Application Design Using Functional and Structural Size Measurements", 2016 Joint Conference of the International Workshop on Software Measurement and the International Conference on Software Process and Product Measurement (IWSM-MENSURA), 2016

Publication

<1%

11

Guerra, Ana Cervigni, and Marcelo Schneck de Paula Pessoa. "Models for Measuring Access Security of Web Application: Security Reference Model", 2013 International Conference on Social Computing, 2013.

Publication

<1%

12

Submitted to Itä-Suomen yliopisto

Student Paper

<1%

13

Neuman, Michael. "Biomedical Sensors", Electrical Engineering Handbook, 1997.

Publication

<1%

14

Submitted to The University of Manchester

Student Paper

<1%

15

file.scirp.org

Internet Source

<1%

16

Submitted to Coventry University

Student Paper

<1%

17

Submitted to Universiti Teknologi MARA

Student Paper

<1%

18

Software Product Quality Control, 2013.

Publication

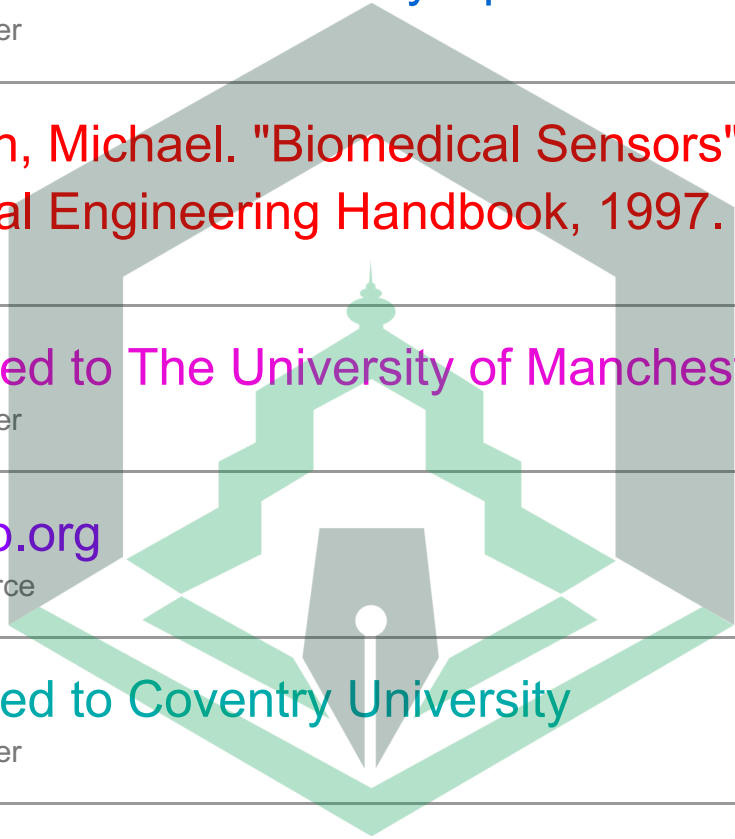
<1%

19

Daniel Galin. "Software Quality Factors (Attributes)", Wiley, 2018

Publication

<1%



---

Exclude quotes Off

Exclude matches < 5 words

Exclude bibliography On



**IAIN PALOPO**