

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 25014 quality model is a security quality instrument that must be contained in an academic information signer 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

1. Software Quality Assurance

Software quality assurance is a match between functional and needs, software qual standards and the implicit characteristics expected of profesional 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 TIEC 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 propriate parameter describing the ISO / IEC 25310 quality model as a quality model.
- * The ISO / IEC 25010 quality model is a quality model that enhances the O / IEC 9126 quality godel / The 25010 quality model is the opposite of the O / 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 assets 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 18 rity compliance quality instrument is the ability of the ISO / IEC 25010 quality model to allow applicable standards and regulations / The ISO / IEC 25010 quality model does not have a sea rity 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.
- * Authencity 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 11. 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

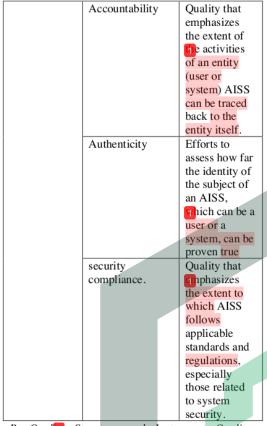
is a quality model that implements the safety characteristics of the instrument. The structure of the security quality model in the academic information system is focused on the ISO / IEC 25010 quality model with five quality instruments namely confidentiality, integrity, accountability, authenticity,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

	QUALITY MODEL	
	Quality	Description
	Instrument	
	Confidentiality	Attempts to
		safeguard
		information by
		providing
		AISS data to
		other parties
		for certain
		purposes and
		are only
		allowed for
		that particular
		purpose.
Security	Integrity	Quality that
Quality		emphasizes
Instrument		that
Based on		information
ISO/IEC		must not be
25010		changed
Quality		without
Model		seizing the
		information
		owner. The
		information
		received must
		be exactly the
		same as when
		the
		information
		was uploaded
		into AISS.



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 qual 13 tructure 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 3 e first level of the quality security instrument based on the quality of the ISO / IEC 25010 model. The second level of security 8 tructure 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 integrity, models, namely confidentiality, accountability, authenticity, and 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.

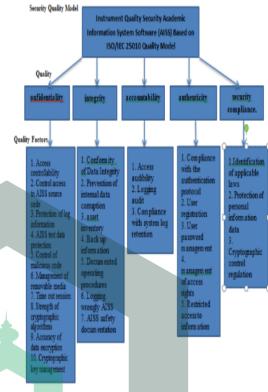


Figure 2. Quality Structure and Quality Factors of Security Institute 15 nent Quality Based on Quality Model ISO/IEC 25010

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

tecurity quality instrument based on quality model ISO/IEC 25010 is a security quality model that implements five ISO / IET 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.

,	BribED OIL BOTTEC 25010 QUITETT MODEL				
		Quality Factor	Description		
		Access control	AISS access		
			control is under		
			user control		
		Control access	Restrict users to		
		to AISS	access		
		source code	information		
			using the AISS		
			source code		
		Log	Protect		

information protection against unauthorized access from an attacker. AISS test data Protect AISS protection Control of malicious code malicious maliciou							
AISS test data protection Control of malicious code malicious code functions and benefits which can be active at any time and cause harm to AISS. Removable media management The process of regularing removable media is computer storage media designed to be inserted and removed from AISS. Session time out The time the user is logged out automatically the user is logged out automatically the user is logged out automatically algorithms The power of cryptographic algorithms are encryption, description and keys. This algorithms are encryption, as a quality that encourage information to avoid damage information to avoid damage information. Data encryption accuracy Data encryption accuracy Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not undetstood. The content of the composition of the compositi		information	information				regulating data
AISS test data protection Control of malicious code malicious computation confidentiality de media malicious code malicious co		protection	against			management	security by
ALSS test data protection best results Control of malicious code malicious code malicious code malicious code malicious code functions and benefits which can be active at any time and cause harm to ALSS. Removable media management Removable media management Confidentiality Removable media management Confidentiality The process of regulating emovable media is computer storage media designed to be inserted and removed from ALSS. Session time out The time the user is logged out automatically algorithms are encryption, description and keys. This algorithm functions to hide information Data encryption and securacy because the formation of more people who are not entified to the information. Data encryption and securacy more people who are not entificated to the information or data was sent. The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information. Data encryption and securacy who are not entificated to the plaintext (original message) is changed into codes that are not understood.		1	unauthorized				private key and
ALSS test data protection Control of malicious code of unknown functions and benefits which can be active at any time and cause harm to AISS. Removable media management Removable media management Confidentiality Confidentiality Confidentiality Confidentiality The process of regularing management of the information in the information was uploaded into AISS. Session time out The time the out "The time the user is logged out automatically algorithms are encryption, description and keys. This algorithm functions to hide information. Data encryption and accuracy Data encryption and active at any time and cause harm to AISS. Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. The limits code information must not be changed without the permission of the owner of the information. The information must not be changed without the permission of the owner of the owner of the information must not be changed without the permission of the owner of the information must not be changed without the permission of the owner of the information must not be changed without the permission of the owner of the information was uploaded into AISS. ALSE Integrity is a quality that emphasizes that the permission of the owner of the information must not be changed without the permission of the owner of the information was uploaded into AISS. ALSE INTEGRITY AS A QUALITY INTEGRIT			access from an				
AISS test data protection test results Control of malicious code of unknown functions and benefits which can be active at any time and cause harm to AISS. Removable media management Confidentiality Confident							
Control of Control of Control of Malicious code of unknown functions and benefits which can be active at any time and cause harm to AISS. Removable media is computer storage media designed to be inserted and removed from AISS		AISS test data					
Control of malicious code of unknown functions and benefits which can be active at any time and cause harm to AISS. Removable media management Confidentiality Confidentialit							
malicious code of unknown functions and benefits which can be active at any time and cause harm to AISS. Removable media management out of the management of the more of regulating removable media is computer storage media designed to be inserted and removed from AISS. Session time out out with no activity at all, consequently the user is logged out automatically. The power of cryptographic algorithms are encryption, description and keys. This algorithms are encryption accuracy where the plaintext (original message) is changed into codes that are not understood. Malicious code for the information. The information was uploaded into AISS. TABLE III QUALITY INTEGRITY AS A QUALITY MODEL Quality Pactor Description or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received must match and exactly the same as when the information or data that is received					2 Introduitor	is a quality that	
functions and benefits which can be active at any time and cause harm to AISS. Removable media management Confidentiality Conformity of Conformity of Conformity of Conformity of Conformity of Conformity of C							
Removable media is computer data designed to be inserted and removed from AISS Session time out The power of cryptographic algorithms The functions of information The functions to hinde information Data accuracy D		mancious code					
Removable media management Removable media is computer storage media designed to be inserted and removed from AISS. Session time out The process of regulating removable moved is computer storage media designed to be inserted and removed from AISS. Session time out The process of regulating removable moved is computer storage media designed to be inserted and removed from AISS. The time the user is logged in but with no activity at all, consequently the user is logged out automatically. The functions of cryptographic algorithms are encryption, description and keys. This algorithms are encryption, description and keys. This algorithm functions to hide information Data encryption accuracy Data encryption accuracy East up a continuation from people who are not entitled to the information accuracy or limited to the information accuracy or limited to the information accuracy or limited and an animatian confidentiality, where the plaintext (original message) is changed into codes that are not understood. Logging is wrong limited and maintained and main							
Removable media is computer storage media designed to be inserted and removed from AISS Session time out The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information from people who are not entitled to the information from people who are not entitled to the information from people who are not entitled to the information from people who are not entitled to the information accuracy Based on ISO/IEC 25010 QUALITY MODEL ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL Of the information or data was sent. 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 are encryption, description and keys. This algorithm functions to hide information Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Total Table II QUALITY INTEGRITY AS A QUALITY (INTEGRITY (INTEGRITY AS A QUALITY (INTEGRITY AS A QUALITY (INTEGRITY (INTEGRITY AS A QUALITY (INTEGRITY (INTEGRITY AS A QUALITY (INTEGRITY (INTEGRITY AS A QUALIT							
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 process of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information. Data encryption accuracy accuracy who are not entitled to the information. Data encryption accuracy who are not confidentiality, where the plaintext (original message) is changed into codes that are not understood. The grow of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information without permission. Data encryption accuracy who are not cancilled to the information witho					when the info		d into AISS.
Removable media management Confidentiality Conformation The time the user is logged in but with no activity at all, consequently the user is logged out automatically the user is logged out automatically consequently the user is logged out automatically the user is logged out automatically consequently the user is logged in the information or data was sent. Prevention of data integrity or data that is received must make and exactly the same as when the information or data was sent. Prevention of data integrity or data that is received must make and exactly the same as when the information or data was sent. Prevention of data integrity or data that is received must make and exactly the same as when the information or data was sent. Prevention of data was sent. Prevention of data sent on accurate and exactly the same as when the information or data was sent. Prevention of accurate and exactly the same as when the information or data was sent. Prevention of data sent on accurate an			-				
Removable media management Confidentiality Conformity of data that is received must match and exactly the same as when 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 prevent damage or loss of data Asset inventory Management of avoid damage or loss caused by viruses. Trojan horses, or of other users who change information without permission. Data the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Conformity of data integrity Integrity Asset inventory Management of avoid damage or loss caused by viruses. Trojan horses, or of other users who change information without permission. Back up information The process of peace and the information or data was sent. Actions that the data and information to avoid damage or loss caused by viruses. Trojan horses, or often users who change information without permission. Back up information backing up data by copying or archiving computer data so that the data en to be reused if there is damage or loss. Also yourselve the same and entered in the read of the data entered to the information. As the formation or data was the the information or data was the the inf			cause harm to				
media management media is computer storage media is computer storage media designed to be inserted and removed from AISS Session time out Session time out user is logged in but with no activity at all, consequently the user is logged out automatically The power of cryptographic algorithms algorithms algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Based Don So/IEC 25010 QUALITY MODEL. Quality Factor Description of Conformity of data that is received must match and exactly the same as when the information or data was sent. Prevention of internal data corruption of loss of data and integrity and the information of a Actions that internal data corruption or loss of data and integrity and internal data or loss of data and internal data integrity and exactly the same as when the information or data was sent. Prevention of internal data or loss of data and internal data integrity or data that is received must match and exactly the same as when the information or data was sent. Prevention of active must an internal data integrity or data that is received must match and exactly the same as when the information or data was sent. Prevention of internal data integrity or data was early the internal data integrity or data was early the must an internal data or loss of data and internal data or loss of data and internal d			AISS.		1 NSTRUM	ENT OF SECURITY	SOFTWARE
Confidentiality management 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 our automatically automatically algorithms are cryptographic algorithms The power of cryptographic algorithms The functions of cryptographic algorithms Data encryption accuracy Data encryption accuracy Data encryption accuracy Data encryption accuracy Employed and a integrity and integr		Removable	The process of		ACADEMIC	INFORMATION S	YSTEM (AISS)
Confidentiality management 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 our automatically automatically algorithms are cryptographic algorithms The power of cryptographic algorithms The functions of cryptographic algorithms Data encryption accuracy Data encryption accuracy Data encryption accuracy Data encryption accuracy Employed and a integrity and integr		media	regulating		BASED ON	ISO/IEC 25010 QUA	ALITY MODEL
media is computer storage media designed to be inserted and removed from AISS Session time out The time the out with no activity at all, consequently the user is logged in but with no activity at all, consequently the user is logged out automatically The power of cryptographic algorithms The increase or loss of data and information or data was sent. Prevention of internal data corruption or loss of data and information or data was sent. Prevention of internal data corruption or loss of data and information or data was sent. Prevention of actions that internal data corruption. 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 sen be reused if there is damage or loss of that the data sen be reused if there is damage or loss of that the data sen be reused if there is damage or loss caused and prevent damage or loss or other users who change information without permission. Data encryption accuracy Data encryption accuracy Asset inventory Management of data and internal data corruption Asset inventory Management of data and information without permission. The process of backing up data by copying or or loss. Documented operating procedures are created, documented, implemented and maintained. Logging is wrong Incorrect reports		management					
Confidentiality Computer storage media designed to be inserted and removed from AISS			media is				The information
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 Back up information without permission. Data encryption and keys. This algorithms are encryption and keys are not entitled to the information Data encryption accuracy Data encryption and keys are not entitled to the information confidentiality, who are not entitled to the information Confidentiality, where the plaintext (original message) is changed into codes that are not understood. Logging is wrong incorrect reports	Confidentiality		computer				
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 algorithms The functions of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption and confidentiality, where the plaintext (original message) is changed into codes that are not understood. Documented operating procedures are created, documented, implemented and maintained incorrect reports Logging is wrong in match and exactly the same as when the information or data was sent. Prevention of internal data corruption or loss of data prevent damage or loss caused by viruses. Trojan horses, or other users who change information without permission. Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained. Logging is wrong Incorrect reports						l line go wy	
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 algorithms The power of cryptographic algorithms algorithms Back up information backing up data by viruses, or other users who change information without permission. Back up information backing up data by copying or archiving computer data so that the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Logging is wrong incorrect reports							
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 The functions to hide information Data encryption and keys. This algorithm functions to hide information. Data encryption accuracy Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. The time the user is logged in the user is logged out at was sent. Prevention of internation or data was sent. Prevention of internation of or loss of data was sent. Prevention of internation of data and information 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 ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained and maintain							
Session time out			inscribe a tara				
Session time out with no activity at all, consequently the user is logged out automatically The power of cryptographic algorithms The functions of eryptographic algorithms are encryption, description and keys. This algorithm functions to hide information The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information The power of cryptographic algorithms are encryption and keys. This algorithm functions to hide information The time the user is logged in the internal data 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. The power of cryptographic algorithms are encryption, description and keys. This algorithm without permission. The power of cryptographic algorithms are encryption and keys. This algorithm without permission. The power of cryptographic algorithms are encryption and keys. This algorithm without permission. The power of cryptographic algorithms are encryption and keys. This algorithm without permission. The process of backup information without permission. The process of backup information without permission. The process of backup information without permission. The process of the complete of the process							
out user is logged in but with no activity at all, consequently the user is logged out automatically The power of cryptographic algorithms Integrity algorithms The power of cryptographic algorithms Integrity algorithms The power of cryptographic algorithms Integrity algorithms The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Data encryption accuracy Integrity algorithm Data encryption accuracy Integrity Data encryption accuracy Back up information Data encryption accuracy Da		0 1 1		Ч			
in but with no activity at all, consequently the user is logged out automatically The power of cryptographic algorithms The power of cryptographic algorithms are encryption, description at log information from people who are not entitled to the information. Data encryption Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Integrity Integrit							
activity at all, consequently the user is logged out automatically The power of cryptographic algorithms The functions of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Dota encryption accuracy Dota encryption accuracy Dota encryption accuracy Dota encryption accuracy 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 Back up 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 are created, documented, implemented and maintained Logging is wrong Incorrect reports		out				D 1 0	
consequently the user is logged out automatically The power of cryptographic algorithms algorithms are encryption, description and keys. This algorithm functions to hide information. Data encryption accuracy Data encryption accuracy Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Corruption 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 Back up information Back up information Back up information The process of backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports						110.0111101101	
the user is logged out automatically The power of cryptographic algorithms algorithms The functions of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information The process of part in the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. The power of The functions of cryptographic algorithms Integrity Asset inventory Management of data and information avoid damage or loss caused by viruses, Trojan horses, or other users who change information without permission. The process of backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained logged into codes that are not understood.							
Integrity automatically The power of cryptographic algorithms algorithms algorithms algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Back up information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Back up information Back up information Back up information Back up information Computer data so that the data can be reused if there is damage or loss. Documented operating procedures or loss. Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports							
The power of cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information. Data encryption accuracy Data encryption accuracy Data encryption accuracy Data encryption encryption accuracy Data encryption accuracy Data encryption accuracy Documented operating procedures Documented operating procedures Documented operating procedures Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports						Asset inventory	Management of
The power of cryptographic algorithms algorithms algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Documented operating procedures are created, documented, implemented and maintained codes that are not understood. Logging is wrong 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 sen be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained lincorrect reports			logged out		Integrity		data and
cryptographic algorithms algorithms algorithms algorithms cryptographic algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Data encryption accuracy Data encryption accuracy Documented the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Cryptographic algorithms are encryption, description and keys. This algorithm without permission. Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained locales that are not understood. Logging is wrong Incorrect reports			automatically				information to
algorithms algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Data encryption accuracy Documented accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Logging is wrong by viruses, Trojan horses, or other users who change information without permission. Back up information Back up information 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 are created, documented, implemented and maintained Logging is wrong Incorrect reports		The power of	The functions of				avoid damage
algorithms algorithms are encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Data encryption accuracy Documented accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Logging is wrong by viruses, Trojan horses, or other users who change information without permission. Back up information Back up information 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 are created, documented, implemented and maintained Logging is wrong Incorrect reports		cryptographic	cryptographic				or loss caused
encryption, description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data encryption accuracy Data encryption accuracy Documented (original message) is changed into codes that are not understood. Encounted to the information without permission. Back up information 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 are created, documented, implemented and maintained locorrect reports			algorithms are				by viruses,
description and keys. This algorithm functions to hide information from people who are not entitled to the information. Data encryption accuracy Data confidentiality, where the plaintext (original message) is changed into codes that are not understood. Doug information Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports			encryption,				
keys. This algorithm functions to hide information without permission. Back up information backing up data by copying or archiving computer data so that the data encryption accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports							
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. Back up information Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures Created, documented, implemented and maintained Logging is wrong Incorrect reports							
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. Back up information Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports							
hide information from people who are not entitled to the information. Data Safeguarding the data sent to accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. hide information Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented AISS operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports							
information from people who are not entitled to the information. Data encryption accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Back up information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures Created, documented, implemented and maintained Logging is wrong Incorrect reports							
from people who are not entitled to the information. Data Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Information backing up data by copying or archiving computer data so that the data ean be reused if there is damage or loss. Documented operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports			mae			Back up	1
who are not entitled to the information. Data Safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Who are not entitled to the information. Safeguarding the data sent to maintain computer data so that the data ean be reused if there is damage or loss. Documented AISS operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports						1	1
entitled to the information. Data Safeguarding the data sent to accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. entitled to the information. Safeguarding the data sent to ean be reused if there is damage or loss. Documented AISS operating procedures are procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports						miormation	
information. Data Safeguarding the data sent to accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Safeguarding the data sent to so that the data ean be reused if there is damage or loss. Documented operating procedures or created, documented, implemented and maintained Logging is wrong Incorrect reports							
Data safeguarding the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. Safeguarding the data sent to ean be reused if there is damage or loss. Documented AISS operating procedures are procedures created, documented, implemented and maintained Logging is wrong Incorrect reports							
encryption accuracy the data sent to maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. the data sent to maintain there is damage or loss. Documented AISS operating procedures are procedures created, documented, implemented and maintained Logging is wrong Incorrect reports		Data					
accuracy maintain confidentiality, where the plaintext (original message) is changed into codes that are not understood. maintain there is damage or loss. Documented AISS operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports							
confidentiality, where the plaintext (original message) is changed into codes that are not understood. confidentiality, where the plaintext (original message) is changed into codes that are not understood. confidentiality, where the plaintext (or loss. Documented AISS operating procedures are created, documented, implemented and maintained Logging is wrong Incorrect reports						-	
where the plaintext (original message) is changed into codes that are not understood. Where the plaintext (original message) is changed into codes that are not understood. Documented AISS operating procedures created, documented, implemented and maintained Logging is wrong Incorrect reports		accuracy					
plaintext (original message) is changed into codes that are not understood. plaintext operating procedures created, documented, implemented and maintained Logging is wrong Incorrect reports							
(original procedures created, documented, implemented and maintained look understood. Contained procedures created, documented, implemented and maintained look understood. Logging is wrong Incorrect reports							
message) is changed into codes that are not understood. message) is documented, implemented and maintained Logging is wrong Incorrect reports			•				procedures are
message) is changed into codes that are not understood. message) is documented, implemented and maintained Logging is wrong Incorrect reports						procedures	created,
codes that are not understood. codes that are not understood. Logging is wrong Incorrect reports							documented,
codes that are not understood. codes that are not understood. Logging is wrong Incorrect reports			changed into				implemented
not understood. Logging is wrong Incorrect reports			codes that are				
			not understood.			Logging is wrong	
		Cryptographic	The process of				
				'		1	

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

1 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 STRUMENT SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 OUALITY MODEL

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

4. Authenticity is an attempt to assess how far the flentity 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

1 NSTRUMENT OF SECURITY SOFTWARE
ACADEMIC INFORMATION SYSTEM (AISS)
BASED ON ISO/IEC 25010 QUALITY MODEL

BASED ON ISO/IEC 25010 QUALITY MODEL					
	Quality Factor	Description			
	Authentication	Appropriate			
	protocol	types of			
	compliance	computer			
		communication			
		protocols or			
		cryptographic			
		protocols			
		specifically			
		designed for the			
		transfer of			
		authentication			
		data between			
		two entities			
Authenticity	User	User registration			
	registration	on an academic			
		information			
		system software.			
	User password	Better			
	management	management of			
		user passwords.			
	Access rights	Management of			
	management	all user access			
		rights			
	Restricted	Restrictions on			
	access to	accessing			
	information	information are			
		based on the			
_		access rights of			
		each user.			
5. Security co	mpliance is an	AISS effort that			

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 INTRUMENT OF SECURITY SOFTWARE ACADEMIC INFORMATION SYSTEM (AISS) BASED ON ISO/IEC 25010 QUALITY MODEL

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

	information
Cryptographic	The rules used
control	check or
regulation	supervise the
	security of the
	syste 115

The academic quality security instrument based on the ISO / IEC 25010 10 ality model is a quality instrument contained in the ISO 1 IEC 25010 quality model consisting of confidentiality, integrity, accountability, authenticity, and security compliance.

The structure of academic 7 uality 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 2 odel quality. The instrument quality security based on the ISO / IEC 25010 model quality is a perspective that contains quality. The second level of security 8 tructure 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 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 op 5 tion really needs security. By implementing an ISO / IEC 250 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 1 formation system software security instruments based on ISO / IEC 25010 quality models. Quality Model Questionn 6 is the most appropriate method of describing the ISO/IEC 25010 quality model as 1 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 plementing 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 5th 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. Vijayakumaran, H. Kim, Security and Privacy Framework for Academic Monitoring System, 2015 8th 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 1st 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
- [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)



SECURITY QUALITY INSTRUMENT

ORIGINALITY REPORT

SIMILARITY INDEX

INTERNET SOURCES

15%

PUBLICATIONS

15%

STUDENT PAPERS

PRIMARY SOURCES

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

Publication

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 Publication

Submitted to University of Sheffield Student Paper

1%

Submitted to Higher Education Commission **Pakistan**

Student Paper

Sun, Yang, Hongbing Qian, and Xiaochen Liu.

1%

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.

1%

Publication

Submitted to City University of Hong Kong
Student Paper

<1%

Submitted to University of Malaya
Student Paper

<1%

9 Lecture Notes in Computer Science, 2007.

Publication

<1%

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

	Security of Web Application: Security Reference Model", 2013 International Conference on Social Computing, 2013. Publication	
12	Submitted to Itä-Suomen yliopisto Student Paper	<1%
13	Neuman, Michael. "Biomedical Sensors", Electrical Engineering Handbook, 1997. Publication	<1%
14	Submitted to Student Paper 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%

Guerra, Ana Cervigni, and Marcelo Schneck de

Paula Pessoa. "Models for Measuring Access

11

<1%

Exclude quotes Off Exclude matches < 5 words

Exclude bibliography On

