KnE Social Sciences
ASABEC 2023
Annual Symposium on Applied Business Economics and Communication 2023
Volume 2024

Research Article

Securing Accounting Information Systems (AIS)

Ali Masjono Muchtar[1]*, Rahmanita Vidya Sari[1], and Stefanus Heru Santoso[2]

[1]Accounting Department, Politeknik Negeri Jakarta, Jakarta, Indonesia
[2]KAP Stefanus Heru Santoso, Jakarta, Indonesia

ORCID
Ali Masjono Muchtar: https://orcid.org/0000-0003-0247-3437

Abstract.
Top management needs to ensure that the company's operations run well and without interruption, but on the other hand, achieving the company's vision is a priority for top management, so that for operational matters, it is handed over to sub-management, for example, one of them is the responsibility of the information system security. Ideally, the company has a function to secure information systems, then the company can focus on the security. Top management will periodically receive reports on information system security. This ideal situation is difficult for some companies to implement, generally, these companies focus on operations, security issues are not yet a top priority, if information system security disturbances occur, for example, password theft by hackers, then they realize that information system security is very important. This research aims to design a security model and convert it to an instrument to determine the level of information system security. Top management is not only given a security report but also knows the level of security of the information system used. Whether the level is very secure, secure, relatively secure, unsecure, or totally not secure. The results of this study are normative measuring model and instrument. The company can regularly evaluate its information security condition by using this instrument and then taking action to anticipate the result.

Keywords: top management, information security, operational management, instruments, models

Corresponding Author: Ali Masjono Muchtar; email: ali.masjonomuchtar@akuntansi.pnj.ac.id

Published: 29 August 2024

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ASABEC 2023 Conference Committee.

1. Introduction

The number of cases of hacking of company data by unauthorized access increasingly shows that the security of accounting information systems is very important for management to pay attention to. The last case in 2023 was the hacking of BSI bank customer data which was hacked by the Lockbit 3.0 hacker group [1]. Cases like this happen almost every year, so it can be a question mark as to what companies or organizations are doing to secure their information systems so that they cannot be hacked.

Of the several hacking cases that occurred, almost all of them hacked customer or user data. If there is a breach in the account, the company manager/owner still

be sure that the error is not due to a weak company/organization system, because the company has ensured the strength of the system's defense against attacks from outside parties [2]. Generally, outside parties try to enter a system through an unauthorized access mechanism, there are outside parties involved. So, in many cases, bank account breaches occur outside the banking system, for example criminals who take advantage of customers' weaknesses and carelessness, or trick customers into sharing their PIN with irresponsible parties [2,3].

The development of information and communication systems has brought an organization or company to a very high dependence on the reliability of information systems. How much dependence does one get from the available information system, if the information system cannot provide reliable information, it means that the system is useless, or the simple question is why use an information system if it cannot provide information when needed [4].

On the other hand, the intangible nature of information systems means they are prone to being infiltrated by irresponsible individuals. In fact, in some cases, applications downloaded from illegal sources contain major threats because they are prone to being infiltrated by algorithms that function incompatible with the application's use [4].

From a management perspective, securing information systems refers to the level of confidence that assets; data, information and the systems that accommodate them remain safe and useful. Management has used a lot of funds to maintain these assets, if there is no threat then management can use them exclusively. However, threats to information systems are always constant and the need to secure information systems grow in line with the sophistication of attacks [4].

The main key to securing information systems lies in setting access rights to assets (data and supporting systems). Setting authorized users to have legal access to a system is very important, whereas on the other hand, hackers (unauthorized access) who access illegally always try to enter a system.

Second, there is an attack which refers to intentional or unintentional actions that can damage or endanger data/information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. A hacker trying to break into an information system is a deliberate attack. The lightning strike that caused the building fire was an accidental attack. Direct attacks are carried out by hackers who use a PC to break into the system. An indirect attack is where a hacker compromises a system using it to attack other systems—for example, as part of a botnet (robo network) [5].

Third is the existence of control and countermeasures or security mechanisms, policies, procedures that can counter attacks, reduce risks, resolve vulnerabilities. According to Weber, Ron [6] control in an information system can be categorized into general control and application control. These two controls can be implemented well if there is a management policy.

There are three parts of management whose function is to protect assets that require policies, the first is general management, the second is IT management and the third is Information Security Management [6]. Each section is responsible for facilitating an information system security program that can ensure that the information system used functions properly. Although many business managers avoid dealing with information security because they consider its a technically complex task, implementing information security actually has more to do with management than technology. Just as managing payroll involves management policy more than mathematical wage calculations [6]. Managing information security is more related to risk management, policy, and enforcement than to the technology of implementation.

The paragraph above implies that management requires assurance that its information systems are safe and can be used properly, regardless of complex technical problems that only certain people understand. To obtain this certainty, it is necessary to prepare methods and tools to help management feel certain that the information system is safe and can be used properly, without having to know about technical problems.

The main aim of this research is to create a model to provide information to management whether the information system (AIS) used in their company is in the safe category. The SIA security perspective uses theory [7]. One of the dimensions discovered is Overall Information System Security.

2. Literature Review

2.1. System reliability

Continuous developments in the field of technology have increased the need for methodologies and tools to assess information system performance in terms of reliability, conformance, and quality of service. Petrov [8], explains that from a methodological point of view, treating data or information is seen from the perspective of the probability of the information system components to provide their services. The first is seen from

the concept of entropy - to measure directly diversity, competition, uncertainty; second, concentration (hierarchy) – to measure order, dominance and certainty directly [8].

It was further explained that system reliability is a measurable, useful, and controllable property of an information system. Useful for management to support the decision-making process. Management needs to identify potential problems that are directly related to the system efficiency of all components supporting the information system. Information system reliability can be developed based on the Delone and Mclean theory, the Lyytinen model and the Technology Acceptance model [9].

Reliability of a system can be interpreted as the system used by an organization functioning in accordance with user needs, for example management and customers, other stakeholders. If customers are happy with the Reliability system used by the organization, it will bring goodness to the organization. Organizations can determine that system reliability is something important in order to please customers [10]. To determine system reliability, according to Romney, Marshal B; Steinbart, Paul John [7], you can use the concept of the Five Trust Services Principles for System reliability.

Based on theory of Romney, Marshal B; Steinbart, Paul John [7] there are five variables that can be used to determine System Reliability (Figure 1). The five variables are Security, Confidentiality, Privacy, Processing Integrity, Availability. The relationships between these variables are described by Romney, Marshal B; Steinbart, Paul John [7].

The performance of each variable and the relationship between these variables can reflect the System Reliability of an organization that uses ICT as a daily operational platform.

To ensure that something is reliable or not, from a management perspective it is necessary to know whether the existing security system can only be accessed by authorized people (controlled and restricted to legitimate users). Management, on the one hand, only knows that there is a strict control system and whether all employees are aware of this and take preventative action against unauthorized access attempts. Confidentiality, privacy, processing integrity and availability can all be categorized into security [7].

Company data and information are the most valuable assets among other information system assets. To ensure system reliability of the data, organizations are required to manage, secure and authorize only authorized persons (authorize persons only) [7].

Confidentiality ensures that sensitive information belonging to the company must be protected from access by unauthorized users. (Unauthorized disclosure). This means that all information regarding employees, customers, finances, products, trademarks can only be accessed by authorized people. This means that regulations and procedures need to be implemented so that confidentiality is maintained [7].

Privacy in this context, organizations are obliged to safeguard customer, employee, partner information that has been collected, used, exposed, and maintained only for the benefit of the organization in accordance with the organization's internal policies.

The data used by organizations needs to ensure that Processing Integrity complies with company policy. Data should be processed accurately, completely, available at all times and processed by only authorized persons [7].

The availability of information produced by the information system is in accordance with operational integrity and obligations in accordance with applicable regulations.

2.2. Measuring system reliability

Measuring System Reliability is something important [11], because it will influence decision making. Every decision taken is always based on the latest (updated) data. Organizations depend on the information systems used so that data is always up to date. To be sure of the reliability of the system used, it is recommended to carry out the measurement process yourself [12].

The measurement uses the concept of the security maturity model [12]. This model divides organizations into five levels of security maturity models. Level 0 is nonexistent where at this level it can be said that there is no control (lack of control). Level 1 ad hoc control can be said to be very weak or bad. Level 2 repeatable indicates concern for control. Level 3 defined which is characterized by starting automatic control. Level 4 managed is characterized by the existence or organization has begun developing the form and type of control and level 5 optimized, the organization has implemented automatic control.

Measuring system reliability can also use the Gage R&R method [11]. This method uses the Stochastic Method, where this method searching for various variations of reliability problems is carried out randomly to determine distributions or patterns that may indicate weaknesses in a system that is statistically measured and analyzed. The results may be accurate or inaccurate.

Confidentiality means protecting information so that only certain and authorized people can access the information. Company information has very high value, this is supported by the rules and regulations approved by management and complied with by the staff who manage the information. As technology advances today, information regarding customer bank accounts, credit card numbers, trade secrets, and confidential government documents needs to be protected so that it does not fall into the hands of irresponsible people [13]. Protecting confidentiality depends on establishing and implementing appropriate levels of access to information. In practice it often involves separating information into separate collections governed by who should have access to the information and how sensitive it is [14]. In the context of this research, management needs to know to what extent the information is protected and can be properly safeguarded. One method that is widely used includes applying encryption methods to stored data.

Privacy means that sensitive information about a person needs to be protected and must not be exposed to the public. To maintain this, companies need to establish strict procedures and rules that are adhered to by all those related to sensitive information. In this research, the instrument that will be created can determine that privacy issues have been implemented in accordance with company regulations.

In the context of processing integrity, organizations must have a level of confidence that data is processed accurately, completely and can be available at any time to authorized users [10]. The key word in processing integrity issues is protecting data from modification or deletion by unauthorized parties and ensuring that when authorized persons make changes that should not be made, the damage can be undone [14].

For this reason, organizations believe that distributed data can be integrated into a unified whole and can provide accurate information. Implementing processing integrity is very crucial because the data of an organization whose data is distributed requires a fast process (Communication), data is stored in a database that has a tight relationship (relationship). Using an encryption system in storage and transportation, having access rights that correspond to the level of obligations [15].

In the context of Availability, organizations must have a high level of confidence that the system used is always available and in accordance with operational needs. For certain types of organizations, availability must apply a 24/7 scheme, meaning the system must be accessible to customers 24 hours and 7 days a week. For example, banks, online shops and others. To ensure this, Information System Management (IMS) must ensure that data availability, system operations, access channels, and authentication

mechanisms must all function properly so that the information they provide and protect is available when needed.

The CIA triad concept explains that the triad, Confidentiality, Integrity and Availability. This concept describes an information system security model developed to assist Information System Management (IMS) in creating information system security policies to identify problem areas and find the necessary solutions [14].

The value of information is a slippery concept, because information has no universal value, it really depends on who uses it, when and for what. Each evaluation of information is related to the value given when making decisions [13].

Some research looks at the value of information from various points of view. Research that uses various variables to determine the success (reliability) or failure of an information system uses the variables System Quality, Information Quality, Use, User Satisfaction and their effects on individuals and their impact on companies [14]. apotheon [14], further explains that SERVQUAL, which is widely used in marketing research, is also used to measure. SERVQUAL is used to measure IT Department Quality by measuring and comparing user expectations and perceptions of IT Department Quality.

3. Methods

This research uses a qualitative method that describes and understands the phenomena experienced by research subjects, for example behavior, perceptions, motivations, actions, holistically and still supported by scientific methods. In the context of this research, describing and understanding the needs of an organization's management for information system security.

In this research, understanding of the phenomenon is evaluated from various information on cybercrimes that have occurred in Indonesia in order to obtain general phenomena and important indicators that are targets of intruders. The result is a weighting of the resulting indicators.

Based on the paragraph above, the object of this research is the information system used by an organization. The sub-objects that are targeted for identifying information system security problems are in the Overall Information system Security domain [7].

To answer the research objectives, the Overall Information system security domain is used as the main reference for developing models/tools that can help management understand the level of information system security [7].

3.1. Research stages

Table 1: Stages of research implementation.

Research Stages	Activity	Methos	Result
1	Identify the dimensions of information system security	*Review literature*	Dimensions of information system security
2	Determine the types of threats/errors that often occur in information systems	*Focus Group Discussion with industry (KAP). KAP Heru Santoso*	Types of threats and errors that often occur in information systems
3	Develop information system security indicators	Focus Group Discussion and literature review of various security cases	Approval of the general form of the model
4	Preparation of information system security measurement models	Focus Group Discussion and literature review with KAP Heru Santoso	Draft model
6	Indicator weighting	Focus Group Discussion and literature review	Model with weighting
7	Model Preparation	Focus Group Discussion	Evaluation results and adjusted model

Source: Prime data. 2023

Table 2: Weighting of each indicator as a result of analysis.

Weight of each indicator	Existence (required or not)	Description
5	Must, urgent	where a weight of 5 means that this indicator must be present and if it is not there it will endanger the company's operational security
4	Must,	Weight 4, must be present but its nature is to support operations and if it is not there, it will endanger the company's operations.
3	In Between	weight 3 in doubt, between presence and absence.
2	Not Must but important	Weight 2, if present, will provide support for security and operations, if not, the impact on company operations is not significant.
1	Not Must but less likely	weight 1. The existence of this indication has no influence the company's operations

Source: Prime data. 2023

The instrument uses two alternative answers, namely Yes, which means the related indicator is really implemented and Not, which means the indicator does not exist or is not implemented. If the respondent answers Yes, they are given a value of 1 and no is given a value of 0. Each answer is multiplied by a weight, the result is a reference value to provide a normative value for the information system security situation.

This instrument does not measure the security situation for all organizations but only applies to the companies or respondents who answered.

The final result of the model is a determination of whether the information system used by the company falls into three categories, namely Very Secure. Secure. Relatively secure. Unsecure. Totally Not Secure.

4. Result and Discussion

The following presentation is the result of discussions by the research team. This presentation shows two important things, namely indicators of overall information system security and errors that often occur in the Accounting Information System (AIS). Indicators are used as a basis for constructing models and types of errors are used as a reference for model creation, so both are sources for model development.

Establishment of a Model based on Comprehensive Security Indicators Basics of Model Preparation.

It is important for a model to be explained because the focus of management work is on strategic planning and how to achieve goals in accordance with the company's vision and mission. On the other hand, management needs data and information support from various places. The easiest data to obtain is internal data and structured data stored in the company database. If the information system used is not able to support the decision-making process by management then the information system is useless. With today's technological support, getting internal data support has become a minimum standard that must be available and can be accessed at any time.

4.1. Purpose of model making

The main aim of creating this model is to help management obtain certainty that the system they use is safe from various disturbances, for example internal hardware, software and other supporting devices, hacker attacks (unauthorized access) and other disturbances that can be anticipated.

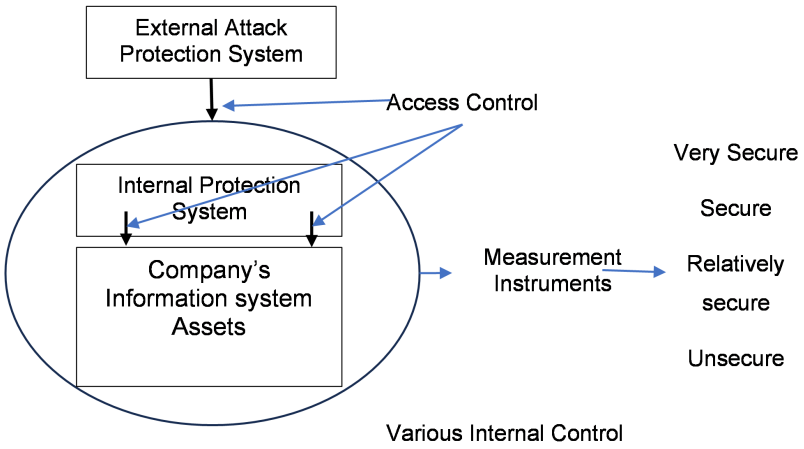
4.2. Benefit of model

The benefit of this model is that it can provide an early warning to management which provides information that there are parts of the company's information system that have weaknesses that need to be improved to make it very safe.

4.3. How models work

This model will produce a tool or way to determine the security level of the information system used by a company. All indicators indicated in this model will be converted into a questionnaire with the answer options provided being Yes-None. The assumption is that respondents who are companies that use information systems will answer according to the existence of these indicators in the company and will answer honestly. Honesty in answering really depends on the person answering because if something contrary happens it will reveal the true situation.

The instrument is designed using a simple mathematical formula, the final result of which is to provide security status in 5 security categories, namely Very Secure. Secure. Relatively secure. Unsecure. Not Secure. Each category reflects the information system situation owned by a company. From the answers given there will be an explanation of why the information system security system used falls into this category.



Source: Research Team Design

Figure 1: Research team design.

According to Romney [7], there are several types of errors that need to be anticipated to secure the information system as a whole (overall Information System Security), including theft of hardware or intentionally or unintentionally damaging hardware (Theft of or accidental or intentional damage to hardware). Loss, theft or unauthorized access to applications, data and other information system resources. (Loss, theft, or unauthorized access to programs, data, and other system resources). Loss, theft or disclosure of confidential data to the public by unauthorized persons or applications. (loss, theft, or unauthorized disclosure of confidential data). modification of applications and data by

unauthorized application parents. (Unauthorized modification or use of programs and data files). Interruption of crucial business activities occurs.

In general, if the above never happens in a company's information system, it can be categorized as a secure information system. If you ask management about this, you can be sure that the person who will answer is the Information Security Management section [6]. This is where the importance of the models and instruments produced from this research lies. This instrument is controlled by general management, once every six months this instrument is filled in/answered by Information Security management. Consistency of answers and explanations each time asked indicates something about the security of the information system, which can be very safe, safe, relatively safe, unsafe or not very safe. Regularly top management will evaluate the results and take anticipatory action.

In practice, if there is an answer of no and it is included in the weight of 5, then further action is needed in the form of deepening the case and taking preventive action.

4.4. Main factors in securing accounting information systems

The following table describes the variables, dimensions and indicators designed by the research team used in the instrument.

TABLE 3: Variables, dimensions and indicators for information systems security.

Variable	Type of Error and Fraud (dimension):	No	Indicators
Overall Information System security	*unauthorized access to programs, data, and other system resources*	1	Have policies and procedures regarding access to AIS and are well documented.
		2	Apply complex and systemized password combinations.
		3	Implement a two-media system to authenticate each access rights change.
		4	Implement a systemized user selection/user determination system.
		5	Using User Matrix Control to control access.
		6	Implement an encryption system when accessing hardware systems and applications.
		7	Implement an encryption system on storage media, either on company servers or on backup media.
		8	Implementing levels of supervision if there is a change in authorization (every change must be known by the direct superior in stages).

Table 3: Continued.

Variable	Type of Error and Fraud (dimension):	No	Indicators
		9	Implement strict and consistent methods of restricting access to computers hardware and software.
		10	Apply strong password combinations to have access to information systems.
		11	Implement password changes periodically.
	Theft of or accidental or intentional damage to hardware	12	Have policies and procedures regarding access to Hardware and are well documented.
		13	Access to hardware and computer space controlled by the system
		14	Strict controls for access to computer systems (hardware and storage media, libraries and applications)
		15	Arrangement and control of the room; anti-smoke/fire, water sprinkler, access control, CCTV.
	(Unauthorized disclosure of confidential data.	16	The organization/company has policies and procedures to protect confidential data from unauthorized disclosure and is well documented.
		17	Implement the latest (updated) encryption system on data storage media.
		18	The encryption system used is always updated and has a high level of difficulty.
		19	Has there been a disclosure of confidential data due to unauthorized actions?
	Unauthorized *modification or use of programs and data files)*	20	The company/organization has well-documented policies and procedures for application modification
		21	Companies/organizations implement copyright protection by using only licensed applications or programs.
		22	Every company/application modification used by the company gets approval from the leadership and there is a description of the changes and the expected results after the changes are made.
		23	So far, application changes/modifications have been carried out by programmers who have full authority.
	Interruption of crucial business activities.	24	Companies/organizations have policies to anticipate System Downtime, Network Disruption, Natural Disasters. Disaster Recovery Plan.
		25	All employees or staff know what actions must be taken if business operational disruption occurs.
		26	Companies train employees or staff on how to deal with operational disruptions.
	Information security protection plan	28	Companies/organizations have policies in dealing with computer system security disturbances (hacker attacks)
		29	Disaster Recovery Plan that is well documented and always updated
		30	Are there aspects that must be met in planning the protection of a system to ensure information security?

TABLE 3: Continued.

Variable	Type of Error and Fraud (dimension):	No	Indicators
		31	The company has experienced security breaches, for example misuse of access rights, hackers/viruses that managed to enter the system and resulted in operational disruption.
		32	Does the company have a way to limit access to computers?
		33	Does the company use strong passwords to access computers?
		34	Are password changes done regularly?
		35	Limiting of physical access to computer equipment
	Limiting of logical access to system using authentication and authorization controls	36	Are there controls that can be used to quickly detect that a system is under attack?
		37	Are there controls in place to prevent unauthorized access to the system?
		38	Are there procedures in place to respond to security incidents?
	Data storage and transmission controls	39	Is there a warning system if storage is almost full?
		40	Is there a system for storing or searching data that is arranged systematically?
		41	Is there a way to reduce the size of the data file so that storage is more efficient?
		42	Is there a transmission medium that is used without the need for cables?
	Virus protection procedures	43	Is there any security if it is detected that the web browsing you are visiting is dangerous?
		44	Are there steps in place to prevent attacks from occurring?
		45	Are there regular system scans and updates to ensure that the computer is protected from the latest virus threats?
	File backup and recovery procedures	46	Is there a scheduled backup system when moving to secondary storage?
		47	Is there a data recovery strategy implemented if data is accidentally deleted or lost?
		48	Is there software for data recovery on the server available?
	Fault-tolerant systems design	49	Can a company implement a fault-tolerant design system to minimize downtime associated with system repairs or maintenance due to failures that occur in the company?
		50	Does the company face challenges in implementing a fault-tolerant system design?
		51	Has the company implemented a system that automatically routes traffic to a backup server without human intervention if the primary server fails?
	Disaster recovery plan	52	Has the company ever experienced a disaster or incident that disrupted the system?

Table 3: Continued.

Variable	Type of Error and Fraud (dimension):	No	Indicators
		53	Does the company have a recovery plan for IT and business applications after a disaster?
		54	Is there regular testing and monitoring of the company's disaster recovery plan?
	Preventive maintenance	55	Companies/organizations have policies regarding system maintenance procedures and methods
		56	Has the company carried out appropriate and routine preventive maintenance?
		57	Is the preventive maintenance carried out by the company effective in reducing losses?
		58	Can the company ensure that the preventive maintenance program can be developed and managed optimally?
		59	Is there a way for the company to ensure that the preventive maintenance program can improve the performance of the machines it owns?
	Casualty and business interruption insurance	60	Companies/organizations have policies regarding disruption to business operations caused by malfunctioning information systems
		61	Companies/organizations insure all the most important parts of company operations, including information systems

Source: Prime Data. 2023

These sixty-one indicators were converted into instruments to be asked of companies and each answer item became the main key in determining the level of information system security.

5. Conclusion

The result of this research is a model for securing information systems that is equipped with an instrument design that normatively measures information system security, but in this article the instrument is not included. From the use of instruments, top management can find out whether the information system used falls into the Very Secure, Secure category. Relatively secure, Unsecure or Totally Not Secure. Then what actions need to be taken by top management to secure the information system that supports company operations.

5.1. Theory Implications

This research applies information system security theories. There are many theories that support information system security, these theories only point to ideal situations

that companies still need to implement. This ideal situation will only be beneficial to the company if the company implements it wisely or follows the recommended “best practices”.

5.2. Managerial Implications

Top managers can use it as a method or tool to control company operations, especially security issues of the information systems used which have a direct impact on operations. The model or tool can be used to anticipate information system security by regularly filling out questionnaires for staff and information system leaders and/or all staff. Analysis of the results is carried out by the information system leader to be reported to the leadership and what action to take if irregularities are found.

References

[1] Fajarlie NI. Kompas. 2023. 15 Juta Data Bank Syariah Indonesia Diduga Diretas, Direktur Utama: Perlu Pembuktian. Available from: www.kompas.tv/article/406513/15-juta-data-bank-syariah-indonesia-diduga-diretas-direktur-utama-perlu-pembuktian?page=all

[2] Hamapu A. Detik.com. 2023. 4 Karyawan Bank di Batam Bobol Rekening Nasabah, Berhasil Gasak Rp 25,6 M.

[3] Hermantoro B. Optimizing financial technology literacy in minimizing phishing threats (Case Study of Indonesian Sharia Bank Customers). In: Proceeding of International Conference on Islamic Philantrophy. 2023. p. 38–52.

[4] Theintactone. heintactone.com. 2019. Evaluation of information system,. Available from: theintactone.com/2022/03/06/evaluation-of-information-systems/.

[5] Whitman ME, Mattord HJ. Principles of information security. Thomson Course Technology Boston, MA; 2009.

[6] HF Tipton MKN. Information security management handbook. CRC Press; Taylor and Francis Group. 2012;

[7] Romney PJ. Accounting information system. Pearson. 2017.

[8] Petrov II. Information systems reliability in traditional entropy and novel hierarchy. Cybernetics and Information Technologies. 2022;22(3):3–17.

[9] Tworek K. Reliability of information systems in organization in the context of banking sector: Empirical study from Poland. Cogent Business & Management.

2018;5(1):1522752.

[10] N. Sevim EEH. Consumer trust impact on online shoping. Internet Application and Management. 2014;5(2).

[11] Kłos R. Measurement system reliability assessment. Polish Hyperbaric Research. 2015;51(2):31–40.

[12] Al-Matari OMM, Helal IMA, Mazen SA, Elhennawy S. Adopting security maturity model to the organizations' capability model. Egyptian Informatics Journal. 2021;22(2):193–9.

[13] Chia T. security.blogoverflow.com. 2016 [cited 2022 Feb 4]. IT Security Community Block. Available from: security.blogoverflow.com

[14] Apotheon. echRepublic. 2008 [cited 2022 Apr 6]. The CIA Triad. Available from: www.techrepublic.com/article/the-cia-triad

[15] Weber R. Information, NJ 07458: Prentice Hall, 1999.