Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 5, Issue 1, Pages 57-71, January-March 2021

Assessing the Conformity Level of Information Security Management System of the Higher Education Institutions: Basis for the Development of Policies and Guidelines

Jurly T. Torregosa, Markdy Y. Orong, Gretel T. Ricalde, Warnner D. Amin,
Herwina A. Lonzon & Richel B. Alcontin

Misamis University, Ozamiz City, Philippines.

DOI: http://doi.org/10.46382/MJBAS.2021.5105

Article Received: 24 September 2020 *Article Accepted: 28 January 2021* *Article Published: 14 February 2021*

ABSTRACT

Data is considered as the main asset in every organization. Hence, security management is important in order to protect the important information of the organization. The study assesses the higher education institutions (HEI) information security management system and check if they conform to the ISO27001 standards. Standardized ISO27001 assessment questionnaire was the main tool in gathering the data needed for the study. The director of Management Information System department of the higher education institutions were the respondents of the study. Results showed that majority of the indicators of the ISO27001 standards were addressed by the HEI's. However, there is a need for the HEI's to conform to other indicators in the standards specially those indicators which were not practiced by the HEI's.

Keywords: *Conformance, Guidelines, Protection, Policies, Tools.*

I. Introduction

Information Technology is becoming more important in business [1, 2]; it is also noticeable to understand how far the IT performance revolutionizes the process within organizations and its effect on the efficiency as well as productivity [3, 4, 5] of the business establishments. Organizations make use of important information in day-to-day business processes [6]. In today's modern world of technology, information was kept within the organization through various information systems [7, 8]. Information becomes more synonyms of patrimony, currency, and future of the company: historical data, research and development, intellectual property rights, and patents, just to name some organization's assets which are critically dependant on the daily operation of information systems (IS) and the information and communication technology (ICT) infrastructure of the firm [9, 10]. Information security (IS) is actively developed by using various technologies which can provide the ensuring of the confidentiality [11], integrity [12, 13] and availability of information together with its non-repudiation, accountability, reliability, and authenticity [14]. In an academe setting, students and administrative information were kept with full of confidentiality to avoid illegitimate accessed [15].

Protecting sensitive information is imperative and must be properly managed [16] by Information Technology experts in an organization. Thus, compliance with information security standards be highly recommended to ensure all information is safe since securing information system resources is extremely important to ensure that the resources are well protected [17]. An information security management system (ISMS) provides controls to protect organizations their most fundamental asset, information [18, 19, 20]. Almost all security groups use the international information security management system (ISMS) standard which is ISO 27000 series. ISO 27000 series focuses on protection of confidentiality, integrity, and availability of information [21].

The ISO27001 is a widely used standard for information security [18]. In terms of usability of standards in global, indicated that ISO (27001) is leading than other standards, especially on ISMS, therefore it indicated that the standard is more easily implemented and well recognized by stakeholders (top management, staff, suppliers, customers/clients, regulators), the standard introduces a cyclic model known as the “Plan-Do-Check-Act” (PDCA) model, aims to establish, implement, monitor and improve the effectiveness of an organization’s ISMS [19], thus compliance with information security standard, ISO 27001, is highly recommended with a variety of reason. Moreover, the standard is designed in order to assure the confidentiality, integrity and availability of information assets. Implementation of information security management, especially ISO27001 is still rare in developing countries [22]. Hence, to continually improve the system security utilized by higher education institutions, an information security management assessment is conducted utilizing the ISO27001 standards. The proposed study aims to assess the level of implementation of the security measures in a university utilizing the ISO 27001 standards. Further, the proposed study aims to give input to the management information system personnel the security level with respect to the information in their respective organization allowing them to improve its technique with as to information security.

II. Related Literature

Business process modeling and security engineering are two significant concerns when developing an information system [23]. Nevertheless, current practices report that security is addressed in the later development stages [24]. Trends of IT and information security awareness (ISA) in society today, particularly within the business environment are quite interesting phenomenon [25]. However, with the current interconnection between information systems combined with the increasing regulation and compliance requirements, it is more and more difficult to achieve real information security governance [26]. Since information security has a very important role in supporting the activities of the organization [27, 28], there is an extreme need of standard or benchmark which regulates governance over information security, these policies and standard function as fundamental guidelines for corporate secure electronic commerce on the global scale. There are several standards for IT Governance which lead to information security awareness such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT [29]. However, some of these standards are underutilized by most organizations.

The ISO27001 is a widely used standard for information security. In terms of usability of standards in global, indicated that ISO (27001) is leading than other standards, especially on ISMS, therefore it indicated that the standard is more easily implemented and well recognized by stakeholders (top management, staff, suppliers, customers/clients, regulators), the standard introduces a cyclic model known as the “Plan-Do-Check-Act” (PDCA) model, aims to establish, implement, monitor and improve the effectiveness of an organization’s ISMS [30], thus compliance with information security standard, ISO 27001, is highly recommended with a variety of reason. Moreover, the standard is designed in order to assure the confidentiality, integrity and availability of information assets. A case study of Martins et al., [31] on information security with the Military Standards Versus ISO 27001 reveals that (1) information security within the military organization is built on the basis of physical and human attack vectors, targeted to the infrastructure that supports the flow of information in the organization, (2) the information security controls applied in the military organization are included in ISO 27001; (3) planning and selection of information security controls are made by decision makers and information security specialists, aiming to ensure the integrity of digital information. It appears that specialists impose their planning options essentially inferring knowledge from analogies, or rather, seek to select and retrieve past successful information security cases, scenarios similar to situations under planning and that may lead to the selection and implementation of the most efficient information security controls.

On the other hand, Susanto et al., [32] implement a novel practical approach framework for the development of an information security management system (ISMS) assessment and monitoring software, called by I-Sol Framework. The framework is expected to assist stakeholders in assessing the level of their ISO27001 compliance readiness. Further, the software help stakeholders understood security control or called by compliance parameters, being shorter, more structured, high precision and measured forecasting. Liao and Chueh [33] assessed the level of attention provided to information security management by medical personnel in Taiwan and developed an evaluation framework based on the ISO27001 standard for information security management. In the context of education, a recent security survey of 485 colleges and universities around the world with 1,000 or more public Internet Protocol addresses should that the Massachusetts Institute of Technology (MIT) earned just above an overall failing grade performed by the information security assessment company Security Scorecard putting the school in the basement below New Mexico State University and Cambridge University [34].

III. Research Framework

Figure 1 presents the framework of the study. As shown, the information security management of the higher education institutions serves as an input of the study. Based on the information from the higher education institutions pertaining to how they manage their information security, the study conducted an assessment on ISMS utilizing the ISO27001 standards questionnaire. Based on the results of the assessment, the study crafted policies that serve as baseline for the institutions in preparation for ISO27001 certification.

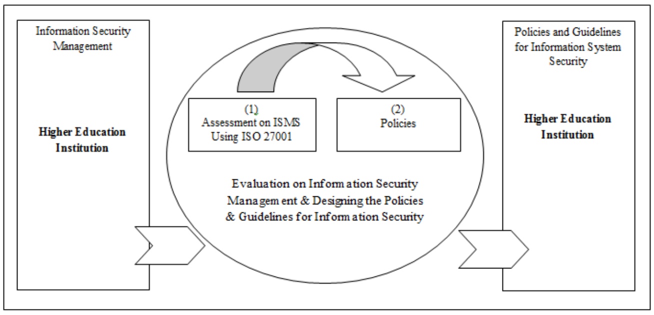
Information Security Management
Higher Education Institution
(1) Assessment on ISMS Using ISO 27001
(2) Policies
Evaluation on Information Security Management & Designing the Policies & Guidelines for Information Security
Policies and Guidelines for Information System Security
Higher Education Institution

Fig.1. Research Framework of the study

IV. Results and Discussions

A. ISO27001 Standards-Evaluation Results

Table 1 presents the results of an assessment on the information security management system of the higher education institution included in the study. Based on the data presented, seven (7) out of nineteen (19) indicators of

ISO27001 were all address in the higher education institutions included in the study. On the other hand, there were five (5) out of nineteen (19) indicators of ISO27001 standards were not clearly address by the higher education institutions. It is evident that that the higher education institutions must consider the following indicators of ISO27001 standards in crafting policies and guidelines such as information security policy, information security risk assessment, information security risk treatment, ISMS resources and competence, awareness and communication, documented information, operational planning and control, monitoring, measurement and evaluation, internal audit, management review, corrective action and continual improvement, and Security controls since it showed non-compliance based on the survey conducted.

Table 1. Assessment on the Information Security Management System Results

Indicators	**Assessment Results**			
	Yes	***%***	***No***	***%***
The organization and its context	10	100.00	0	0.00
Needs and expectations of interested parties	10	100.00	0	0.00
Scope of the ISMS	10	100.00	0	0.00
Leadership and management commitment	10	100.00	0	0.00
Information security policy	5	50.00	5	50.00
Roles and responsibilities	10	100.00	0	0.00
Risks and opportunities of ISMS implementation	10	100.00	0	0.00
Information security risk assessment	5	50.00	5	50.00
Information security risk treatment	0	0.00	10	100.00
Information security objectives and planning to achieve them	10	100.00	0	0.00
ISMS resources and competence	5	33.33	5	66.67
Awareness and communication	5	50.00	5	50.00
Documented information	7	70.00	3	30.00
Operational planning and control	2	20.00	8	80.00
Monitoring, measurement and evaluation	0	0.00	10	100.00

Indicators	Assessment Results			
	Yes	*%*	*No*	*%*
Internal Audit	0	0.00	10	100.00
Management Review	0	0.00	10	100.00
Corrective action and continual improvement	0	0.00	10	100.00
Security controls – as applicable, based on the results of your information security risk assessment	7	70.00	3	30.00

B. Suggested Information Technology Policies and Guidelines for Higher Education Institutions

Based on the results of the assessment on the level of readiness of the higher education institutions to the ISO27001 standards for information security management system, the following were the policies and guidelines designed that will help education institutions in preventing intruders of the different systems in the organization. Table 2 presented the policies and guidelines pertaining to the information security management system in line with the ISO27001 standards. The core principles for information security management are adapted to the higher education institutions for the following areas:

- Risk assessment
- Organizing information security
- Asset management
- Human resource security
- Communications and operations management
- Access control
- System development and maintenance
- Information security incident management
- Compliance

Table 2. Information Security Policies Crafted based on the ISO27001 Standards

Information Security Policies
Risk Assessment
a. HEI’s approach to security should be based on risk assessments.

b. HEI’s should continuously assess the risk and evaluate the need for protective measures. Measures must be evaluated based on HEI’s role as an establishment for education and research and with regards to efficiency, cost and practical feasibility.
c. An overall risk assessment of the information systems should be performed annually.
d. Risk assessments must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks.
e. Risk assessments are to be carried out when implementing changes impacting information security. Recognized methods of assessing risks should be employed, such as ISO/IEC 27001.
f. The Management Information System Director is responsible for ensuring that the risk management processes at the HEI’s are coordinated in accordance with the policy.
g. The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.
h. Risk management is to be carried out according to criteria approved by the management of the HEI’s.
i. Risk assessments must be approved by the management.
j. If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.
Security organization in the HEI’s
a. The University/College President is primarily responsible for the security.
b. The Management Information System Director has executive responsibility for information security in connection with IT systems and infrastructure.
c. The human resource director has executive responsibility for information security according to the Personal Data Act and is the controller on a daily basis of the personal information of the employees.
d. The human resource director has executive responsibility for information security related to employee’s information systems.
e. The Vice President for Academic Affairs and Research Director has executive responsibility for research related personal information.
f. Projects should be organized according to HEI's project manual, where information security should be defined.

g. HEI's information security will be revised on a regular basis, through internal control and at need, with assistance from an external IT auditor.
Asset Management
a. "Assets" include both information assets and physical assets.
b. Information and infrastructure should be classified according to security level and access control.
c. Information of the assets should be classified as one of three categories for confidentiality: 1. **Sensitive -** Information of a sensitive variety where unauthorized access (including internally) may lead to considerable damage for individuals, the university college or their interests. 2. **Internal -** Information which may harm HEI's or be inappropriate for a third party to gain knowledge of. The System owner decides who may access and how to implement that access. **3. Open –** Other information is open.
d. HEI's shall carry out risk analyses in order to classify information based on how critical it is for operations (criticality).
e. Routines for classification of information and risk analysis must be developed.
f. Users administrating information on behalf of the HEI's should treat said information according to classification.
g. Sensitive documents should be clearly marked.
h. A plan for electronic storage of essential documentation should be developed.
i. Information that is vital for operations should be accessible independent of which systems the information was created or processed in.
Human resource security
Prior to Employment
a. Security responsibility and roles for employees should be described.
b. A background check is to be carried out of all appointees to positions at HEI's according to relevant laws and regulations.
c. A confidentiality agreement should be signed by employees, contractors or others who may gain access to sensitive and/or internal information.

d. IT regulations should be accepted for all employment contracts and for system access for third parties.

During Employment

e. The IT regulations refer to HEI's information security requirements and the users' responsibility for complying with these regulations.

f. The IT regulations should be reviewed regularly with all users and with all new hires.

g. All employees and third party users should receive adequate training and updating regarding the Information security policy and procedures. The training requirements may vary.

h. Breaches of the Information security policy and accompanying guidelines will normally result in sanctions.

i. HEI's information, information systems and other assets should only be utilized for their intended purpose. Necessary private usage is permitted.

j. Private IT equipment in HEI's infrastructure may only be connected where explicitly permitted. All other use must be approved in advance by the IT department.

k. Use of HEI's IT infrastructure for personal commercial activities is [under no circumstances] permitted.

Termination or change of employment

a. The responsibility for termination or change of employment should be clearly defined in a separate routine with relevant circulation forms.

b. HEI's assets should be handed in at the conclusion of the need for the use of these assets.

c. HEI’s should change or terminate access rights at termination or change of employment. A routine should be present for handling alumni relationships.

d. Notification on employment termination or change should be carried out through the procedures defined in the personnel system.

Communications and operations management

a. Purchase and installation of IT equipment must be approved by the MIS department.

b. Purchase and installation of software for IT equipment must be approved by the MIS department.

c. The MIS department should ensure documentation of the IT systems according to HEI's standards.

d. Changes in IT systems should only be implemented if well-founded from a business and security standpoint.
e. The MIS department should have emergency procedures in order to minimize the effect of unsuccessful changes to the IT systems.
f. Operational procedures should be documented. Documentation must be updated following all substantial changes.
g. Before a new IT system is put in production, plans and risk assessments should be in place to avoid errors. Additionally, routines for monitoring and managing unforeseen problems should be in place.
h. Duties and responsibilities should be separated in a manner reducing the possibility of unauthorized or unforeseen abuse of HEI's assets.
i. Development, testing and maintenance should be separated from operations in order to reduce the risk of unauthorized access or changes, and in order to reduce the risk of error conditions.
j. All contracts regarding outsourced IT systems should include • information security requirements, including confidentiality, integrity and availability • a description of the agreed security level • requirements for reporting security incidents from third parties • a description of how may ensure that third parties are fulfilling their contracts • a description of HEI's right to audit third parties.
k. Requirements for information security must be taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes. Routines must be developed for change management and system development/maintenance.
l. IT systems must be dimensioned according to capacity requirements. The load should be monitored in order to apply upgrades and adjustments in a timely manner. This is especially important for business-critical systems.
m. Computer equipment must be safeguarded against virus and other malicious code. This is the responsibility of the IT security manager.
n. The IT department is responsible for carrying out regular backups and restore of these

backups, as well as data storage on HEI's IT systems according to their classification.

o. Backups should be stored externally or in a separate, suitably protected zone.

p. The MIS department has the overall responsibility for protecting HEI's internal network.

q. There should be an inventory containing all equipment connected to HEI's wired networks.

r. All access to HEI's networks should be logged.

s. There should be procedures in place for the management of removable storage media. Implementation is the responsibility of each employee.

t. Storage media should be disposed of securely and safely when no longer required, using formal procedures.

u. Procedures and controls should be established for protecting exchange of information with third parties and information transfer. Third party suppliers must comply with these procedures.

v. HEI's has the right to access personal e-mail and other personal data stored on HEI's computer networks.

w. Storage and transfer of sensitive information should be encrypted or otherwise protected.

x. Information exchanged across public networks in connection with e-commerce, should be protected against fraud, contractual discrepancies, unauthorized access and changes.

y. The MIS department should ensure that publicly accessible information, e.g. on HEI's web services, is adequately protected against unauthorized access.

z. Access and use of IT systems should be logged and monitored in order to detect unauthorized information processing activities.

aa. Usage and decisions should be traceable to a specific entity, e.g. a person or a specific system.

bb. The MIS department should register substantial disruptions and irregularities of system operations, along with potential causes of the errors.

cc. Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.

dd. The MIS department should log security incidents for all essential systems.

ee. The MIS department should ensure that system clocks are synchronized to the correct time.

Access Control
a. Written guidelines for access control and passwords based on business and security requirements should be in place. Guidelines should be re-evaluated on a regular basis.
b. Guidelines should contain password requirements (frequency of change, minimum length, character types which may/must be utilized, etc.) and regulate password storage.
c. Users accessing systems must be authenticated according to guidelines
d. Users should have unique combinations of usernames and passwords.
e. Users are responsible for any usage of their usernames and passwords. Users should keep their passwords confidential and not disclose them unless explicitly authorized by the MIS Director.
f. Access to information systems should be authorized by immediate superiors in accordance with the system owner directives. This includes access rights, including accompanying privileges. Authorizations should only be granted on a "need to know" basis, and regulated according to role.
g. The immediate superior should alert the system administrator about granting access and changes in accordance with the directives from the system owner.
h. Roles and responsibilities with accompanying access rights should be described based on the following classifications. • Internal (several roles) • External (several roles) • Student • Public • Others
i. The MIS department is responsible for ensuring that network access is granted in accordance with access policy.
j. Users should only have access to the services they are authorized for.
k. The access to privileged accounts and sensitive areas should be restricted.
l. Users should be prevented from accessing unauthorized information.
m. Remote access to HEI's computer equipment and services is only permitted if the security policy has been read and understood and the IT regulations signed.

n. Remote access to HEI's network may only take place through security solutions approved by the IT department.
o. Mobile units should be protected using adequate security measures.
p. Information classified as sensitive must be encrypted if stored on portable media, such as memory sticks, PDAs, DVDs and cell phones.
System development and maintenance
a. Definitions of operational requirements for new systems or enhancements to existing systems must contain security requirements.
b. Guidelines for administration and use of encryption for protecting information should be in place.
c. All changes to production environments should comply with existing routines.
d. The implementation of changes to the production environment should be controlled by formal procedures for change management, in order to minimize the risk of damaged information or information systems.
e. Systems developed for or by HEI’s must satisfy definite security requirements, including data verification, securing the code before being put in production, and use of encryption.
f. All software should be thoroughly tested and formally accepted by the system owner and the IT department before being transferred to the production environment.
g. Prior to new systems classified as “high”, or substantial changes in systems classified as “high” are put in production, a risk assessment must be carried out.
Information security incident management
a. All breaches of security, along with the use of information systems contrary to routines, should be treated as incidents.
b. All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to management or directly to the MIS Director.
c. Routines are to be developed for incident management and reporting. The routines should contain measures for preventing repetition as well as measures for minimizing the damage.
d. The MIS director should ensure that routines are in place for defining the cost of security incidents.
e. A plan for continuity and contingencies covering critical and essential information

systems and infrastructure should exist.
f. The continuity plan(s) should be based on risk assessments focusing on operational risks.
g. The continuity plan(s) should be consistent with HEI's overall contingencies and plans.
h. The continuity plan(s) should be tested on a regular basis to ensure adequacy, and to ensure that management and employees understand the implementation.
Compliance
a. All employees must comply with the Information security policy and guidelines. Enforcement is the responsibility of line management. Students must comply with IT regulations.
b. Employees and students should be aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following court orders.
c. Audits should be planned and arranged with the involved parties in order to minimize the risk of disturbing the activities of HEI’s.

V. Conclusions and Recommendations

Higher Education Institutions conform to majority of the indicators of the ISO27001 standards. However, there is a need for the HEI’s to closely monitor and continue their conformance and perform corrective actions on the other indicators that showed non-conformity. Moreover, the study crafted the policies and guidelines for the HEI pertaining to information security. These crafted policies will have served as baseline of the HEI’s for the improvement of their security measures on their different information system. Higher Education Institutions may utilize the designed policies and guidelines crafted based on the ISO27001 standards in preparation for ISO certification.

References

[1] Howell, R., van Beers, C., & Doorn, N. (2018). Value capture and value creation: The role of information technology in business models for frugal innovations in Africa. Tech. Forecasting & Social Change, 131, 227-239.

[2] Schwertner, K. (2017). Digital transformation of business. Trakia Journal of Sciences, 15(1), 388-393.

[3] Tagaram, P. (2018). The Effect of Organizational Factors and IT on Productivity in Valve Manufacturing. Australian Journal of Basic and Applied Sciences, 12(9), 73-77.

[4] Gunasekaran, A., Subramanian, N., & Papadopoulos, T. (2017). Information technology for competitive advantage within logistics and supply chains: A review. Transportation Research Part E: Logistics and Transportation Review, 99, 14-33.

[5] Angioha, P. U., Enukoha, C. U., Agba, R. U., & Ikhizamah, G. U. (2020). Information Technology Predictor Variables and Employee Productivity in Commercial Banks. JINAV: Journal of Information and Visualization, 1(1), 44-52.

[6] Yabe, T., Zhang, Y., & Ukkusuri, S. V. (2020). Quantifying the economic impact of disasters on businesses using human mobility data: a Bayesian causal inference approach. EPJ Data Science, 9(1), 36.

[7] Intezari, A., & Gressel, S. (2017). Information and reformation in KM systems: big data and strategic decision-making. Journal of Knowledge Management.

[8] Temirbekov, N., Baigereyev, D., Temirbekov, A., & Omirzhanova, B. (2019, December). Development of an information system for storing digitized works of the Almaty Academgorodok research institutes. In AIP Conference Proceedings (Vol. 2183, No. 1, p. 080005). AIP Publishing LLC.

[9] Ritz, W., Wolf, M., & McQuitty, S. (2019). Digital marketing adoption and success for small businesses. Journal of Research in Interactive Marketing.

[10] De La Hoz-Rosales, B., Ballesta, J. A. C., Tamayo-Torres, I., & Buelvas-Ferreira, K. (2019). Effects of Information and Communication Technology Usage by Individuals, Businesses, and Government on Human Development: An International Analysis. IEEE Access, 7, 129225-129243.

[11] Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. Security and Communication Networks, 2017.

[12] Mohd, K. B. (2019). The Integrity of Fintech In Information Security From Islamic Perspective. Editorial board, 61.

[13] Bateni, H., & Saeidi, P. (2019). The effect of information quality integrity on information security risk management.

[14] Fu, Y., Zhu, J., & Gao, S. (2018). CPS information security risk evaluation based on blockchain and big data. Tehnički vjesnik, 25(6), 1843-1850.

[15] Peddy, A. M. (2017). Dangerous Classroom Aptitude: Protecting Student Privacy from Third-Party Educational Service Providers. BYU Educ. & LJ, 125.

[16] Stankov, I., & Tsochev, G. (2020). Vulnerability and protection of business management systems: threats and challenges. Problems of Engineering Cybernetics and Robotics, 72, 29-40.

[17] Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.

[18] Achmadi, D., Suryanto, Y., & Ramli, K. (2018, May). On developing information security management system (isms) framework for iso 27001-based data center. In 2018 International Workshop on Big Data and Information Security (IWBIS) (pp. 149-157). IEEE.

[19] Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information Security Management System. International Journal of Computer Applications, 158(7), 29-33.

[20] Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. Information & Computer Security.

[21] Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. Network Security, 2018(5), 9-11.

[22] Candiwan, C. (2014, November). Analysis of ISO27001 implementation for enterprises and SMEs in Indonesia. In Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), Kuala Lumpur, Malaysia (Vol. 1719, p. 5058).

[23] Nguyen, P. H., Ali, S., & Yue, T. (2017). Model-based security engineering for cyber-physical systems: A systematic mapping study. Information and Software Technology, 83, 116-135.

[24] Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. computers & security, 70, 663-674.

[25] Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review.

[26] Mayer, N., Grandry, E., Feltus, C., & Goettelmann, E. (2015, June). Towards the ENTRI framework: security risk management enhanced by the use of enterprise architectures. In International Conference on Advanced Information Systems Engineering (pp. 459-469). Springer, Cham.

[27] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29.

[28] Alhassan, M. M., & Adjei-Quaye, A. (2017). Information Security in an Organization. International Journal of Computer (IJC), 24(1), 100-116.

[29] Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. International Journal of Engineering and Technology. IJET Publications UK, 2(1).

[30] Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International J.al of Electrical Computer Sciences IJECSIJENS, 11(5), 23-29.

[31] Martins, J., dos Santos, H., Rosinha, A., & Valente, A. (2013). Information Security–Military Standards Versus ISO 27001: A Case Study in a Portuguese Military Organization. Information Warfare and Security, 191.

[32] Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement. arXiv preprint arXiv:1203.6622.

[33] Liao, K. H., & Chueh, H. E. (2012). Medical Organization Information Security Management Based on ISO27001 Information Security Standard. JSW, 7(4), 792-797.

[34] Gallagher, S. (2015). MIT ranks high in bad security at major universities. New York: Condé Nast Publications, Inc. Retrieved from http://search.proquest.com/docview/1711125337?accountid=149218