International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 11, November 2021, pg.29 – 46

ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORKS

Mohammad Abdu Al-esaïy^{*1}; Dr. Nagi Ali Al-Shaibany^{*2}

^{*1}IT Student, IT Management, Sana'a University, Yemen.

^{*2}Assistant Professor, IT Management, Sana'a University, Yemen.

DOI: 10.47760/ijcsmc.2021.v10i11.005

ABSTRACT

ISMS is a set of policies, activities, and procedures implemented by the Information Security Department to maintain the confidentiality, integrity, and availability of information from threats and risks. Activities and procedures include identifying security needs, strategies required for implementation, and measuring results for security improvement. This paper aims to review the previous literature to verify the factors that affect information security management. Examination of current information security frameworks and standards, and this paper concluded that, for an organization to adopt a specific framework, this framework must be evaluated based on the security needs of the organization. The framework must include all factors that affect information security from all organizational aspects, people, and technology. Otherwise, the organization will face difficulties and obstacles in implementing the framework and improving security.

Keywords: Information Security, Framework, Information Security Management System

1.1 INTRODUCTION

Information today has become an essential part of the modern economy, and modern organizations today depend in their commercial activities on information to survive in the markets [1], this means that information is one of the most important resources that the organization possesses, so organizations need this information to be accurate, reliable, ready at any time the user requests and in the correct format because the information has become the lifeblood of the organization [7, 8, 10, 12].

The current technological acceleration has provided companies with many factors such as saving time, competition, customer service, and opening up new investment opportunities for organizations. This technology requires companies to put in place security policies and procedures to ensure their safety and ability to provide services to the public and gain their trust [11].

Technological development has opened new markets, and keeping pace with development has become necessary for organizations, so today information security has become one of the biggest problems that threaten organizations, and it is a source of concern for organizations, because the organizations economy depends on technology, so many organizations develop policies and procedures to reduce security risks that You may face it, for fear of economic collapse [2].

With organizations relying on technology, capital or leadership are no longer the only essential elements for the success of the organization, but a new element has appeared here, which is information security. The information security component of organizations and made it a priority for organizations, because organizations have become aware that this element may have a significant negative impact on the value and reputation of the organization in the markets, and that it has become necessary to protect organizations from security risks and threats that develop every day [13]. This interest in the security component, in turn, has led to an increase in organizations' interest in information security management [17].

Information security management is the planning, coordination, implementation, and control activities with the aim of protecting the organization's information [18]. ISMS is concerned with securing information, whatever its form, and the organization's information assets, through an ordered and continuous sequence of operations that aim to achieve the organization's goals. These operations are comprehensive framework for establishing, operating, implementing, monitoring, reviewing, maintaining, and improving information security [9]. It helps the organization to avoid risks and penalties, mitigate security incidents, overcome weaknesses and ensure business continuity by implementing proactive security measures to reduce risks [16]. Therefore, many bodies have developed many standards that meet the information security needs of organizations regardless of the size, type, and activity of the organization, and any organization can adapt to these standards, as well as there are many security frameworks that have been established to meet the needs of a particular organization. These frameworks may not be Feasible enough with an organization of a different type or activity [4]. This paper analyzes and compares the information security management frameworks and standards mentioned in the previous literature.

1.2 PROBLEM STATEMENT

With the expansion of the activities of organizations, the need for organizations to share information and the increase in security threats. This matter called for organizations to create a comprehensive ISMS information security management system to contain all security risks that may harm the organization. With the different activities of organizations and their need to implement security controls according to the expertise of their employees and their budget, there are many frameworks and standards to improve information security management systems. This paper analyzes the frameworks for improving information security management systems.

2.1 OVERVIEW OF INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORKS

The standards and frameworks for managing information security systems are a summary of the findings of experts and academic researchers regarding the mechanisms, methods, and correct security controls that organizations must follow in managing information security systems, to ensure the best security controls, maintain unified information security between organizations, and ensure the proper and correct use of resources available.

These standards are not obligatory for organizations to follow, but they are considered the best approach to managing information security systems, as these standards provide a large number of control objectives and leave room for organizations to add controls that the organization deems appropriate [9]. Here we will discuss several standards and frameworks for information security management.

2.1.1 BS 7799

In 1995 the British Standards Institution (BS) in cooperation with the British Ministry of Industry and Trade and a number of organizations published a standard for information security management called BS7799, and in 1999 published the next version of BS7799 which was divided into two parts (BS7799-2) covering ISMS requirements and Part The second is code of practice (BS7799-1), and in the year 2000 BS7799-2 was issued. . [21, 8]

From the point of view of (BS), this standard clarifies the basic requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving ISMS., which is part of the organization's general system with the aim of protecting information assets. BS7799 defines 10 security controls as necessary for any organization, this standard clarifies the basic requirements that it considers indispensable, namely:

Establishing and managing the ISMS

Management responsibility

Management review of the ISMS

ISMS improvement

2.1.2 COBIT

The International Information Technology Association (ISACA) has developed the COBIT Standard for Information Technology Governance, in which information security has been integrated as an essential part of it, in the name of COBIT 5 for Information Security, in order to help organizations to reduce risks, achieve the strategic goals of the organization by adapting ISMS to support strategic goals, ensuring the survival of systems and services Available, customer satisfaction and decision-making assistance. COBIT 5 Information Security focuses on planning the creation, implementation, and maintenance of ISMS. It provides the organization with guidance on policies, principles, processes, organizational structures, security culture, types of information, skills, and competencies [22]. It contains some principles such as:

- Strategic Alignment
- Delivery Value Resource Management
- Risk Management
- Performance Measure

2.1.3 NIST SP 800-14

NIST SP 800-14: A framework developed by the National Institute of Standards and Technology (NIST), that provides organizations with key practices and principles for creating and improving information security systems. Practices are a list of security controls, objectives, and procedures described in NIST SP 800-12, principles used when developing a security policy or system where security is viewed from a high level such as cost, accountability, and jealousy. This means that practices are derived from principles because it is principles that set restrictions on practices. This standard describes 8 principles and 14 practices. The principles used here are derived from the principles of the Organization for Economic Cooperation and Development (OECD) and are as follows [15,3,14]:

Security Supports the Mission of the Organization

- 1- Security is an Integral Element of Sound Management
- 2- Security Should Be Cost-Effective
- 3- Systems Owners Have Security Responsibilities Outside Their Own Organizations
- 4- Security Responsibilities and Accountability Should Be Made Explicit
- 5- Security Requires a Comprehensive and Integrated Approach
- 6- Security Should Be Periodically Reassessed
- 7- Security is Constrained by Societal Factors

2.1.4 ISO/IEC 27001

ISO/ IEC 27001: This standard was published in 2005 with the title:

- Information technology - Security techniques - Information security management systems – Requirements.

ISO27001 provides a comprehensive framework, guidelines, and requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving Information Security Management Systems (ISMS) in the context of an organization's general business risk. ISO27001 provides requirements for assessing and addressing risks through the application of security controls. These requirements are scalably Applicable to all organizations [9], this means that ISO27001 clarifies the requirements for ISMS that are applicable internationally, and this is the original standard that was developed from the BS7799 2- standard [7]. This standard focuses on the risk assessment approach and is considered the most widely used standard. ISO/ IEC 27001 follows the PDCA model in implementing all ISMS processes with the aim of ensuring continuous improvement and ensuring the effectiveness and efficiency of ISMS so that ISMS outputs are the expectations of interested parties [7,8]. This standard sets out a set of requirements for ISMS. These requirements are necessary and indispensable for any organization [20,4]:

- Context of the organization
- Leadership

- Planning
- Support
- Operation
- Performance evaluation
- Improvement

2.1.5 PCI DSS

PCI DSS: is an information security standard developed by the Payment Card Industry Security Standards Council to improve information security in organizations that deal with credit cards, and contains a set of security controls related to securing credit and payment card data. These security controls discuss network security, software, Data protection, vulnerability management, access control, network monitoring, and security policies [19]. Table (2.4) shows the most important security controls in the previously mentioned frameworks and standards.

Table (2.4) Comparison of control objectives for the six ISMS Standards and Frameworks

No	Element	ISO/IES 27001	BS 7799	COBIT	PCIDSS	NIST
1	Information security policies	✓	✓	✓	✓	✓
2	Organization of information security	✓	✓	✓	✓	✓
3	Human resource security	✓	✓	✓	✓	✓
4	Asset management	✓	✓	✓	✓	✗
5	Access control	✓	✓	✓	✓	✓
6	Cryptography	✓	✓	✓	✓	✓
7	Physical and environmental security	✓	✓	✓	✓	✓
8	Operations security	✓	✓	✓	✓	✓
9	Communications security	✓	✓	✓	✓	✗
10	System acquisition, development and maintenance	✓	✓	✓	✓	✓
11	Supplier relationships	✓	✗	✓	✗	✗
12	Information security incident management	✓	✗	✓	✗	✓
13	Information security aspects of business continuity management	✓	✓	✓	✓	✗
14	Compliance	✓	✓	✓	✓	✗

3.1 OVERVIEW OF INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORKS

In this study, many previous studies that were published regarding the development of a framework for improving the information security management system were reviewed. This section of the study presents a summary of the most important scientific studies in this subject.

Kauspadiene, Cenys, Goranin, Tjoa, and Ramanauskaite (2017) designed a High-level self-sustaining ISMS framework (HISMF) for small and medium enterprises. The framework was created through a variable (stakeholders), where stakeholders were classified into seven categories. Each category covers an area of information security management and these categories are:- Legislatures (to ensure control of cyberspace), Professionals (to manage security at the system level), corporate governance (to ensure infrastructure), Developers (to ensure the development of systems), Third parties (for external communications), IT companies (to supply hardware) and Universities (to provide university experts), shown in Fig [3.1]. However, this framework does not take into account the budget and management support [34].

Fig. 3.1: High-level self-sustaining Information Security Management Framework [34]

Achmadi, and others, (2018), presented a special framework for the data center based on ISO 27001, the goal is to reduce threats, and maintain the confidentiality, integrity, and availability of information, and the framework consists of three aspects: people, processes, and technology. This framework covers only 21 control objectives. This framework discusses the Issue-Specific policies and does not discuss the Roles and Responsibilities of the Policy Development Team. This framework does not discuss the budget and culture [29].

Teresa. P, Henrique.S, (2010), presented an approach to improve information security management through developing a conceptual framework for security auditing, verifying the efficiency of security controls and policies in organizations. The framework aimed to assist organizations to classify attacks. The framework focused on specific audit components: security controls to detect events, protect assets, protect information

properties, reduce threats, detect attacks and protect vulnerabilities, shown in Fig [3.2]. The framework was based on the relevant ISO/IEC_JTC1 standards. The framework did not focus on security controls to audit awareness and training programs. In other words, the framework discussed the technological aspect [30].

Fig. 3.2: Concepts and relationships defined in the conceptual framework [30]

Sohail S., and others (2012), Designed a framework for information security management, for companies in South Africa. This framework discusses information security management from the security governance aspect, shown in Fig. [3.3]., This framework examines four issues related to information security within an organization: policy documentation, employee awareness, management support, and access control. The framework discussed the importance of the human element. This framework discussed awareness only and did not discuss other factors such as culture, motivation, communication, and training [31].

Fig. 3.3: Conceptual Model for Enterprise Information System Security [31]

R. Werlinger (2008), and others, provided a framework for human, technological, and organizational challenges in implementing information security in academic and private organizations. The framework in Fig. [3.4] illustrates the interactions between the different factors. The framework identified four human factors: culture, security tools, risk perception, and communication. The framework identified three technological factors: mobile access, technology compatibility, and vulnerabilities. The framework identified eight organizational factors: budgeting, scheduling, risk assessment, interaction with other organizations, access control, distributed management, infrastructure, and security priorities. However, the study sample was limited, only 27 cases [25].

Fig. 3.4: framework for human, technological and organizational challenges [25].

M. Zammani, and others, (2019), discussed the success factors of information security management that effect on ISM implementation. This study has confirmed fourteen factors are Top Management, IS Coordinator Team, ISM Team, IS Audit Team, Employees, Third Parties, IS Policy, IS Procedures, Resource Planning, Competency Development, and Awareness, Risk Management, Business Continuity Management, IS Internal Audit, and IT infrastructure. This study divided the success factors of information security management into four categories are Human, Organizational Documents, Process, and Technology. Each category includes a group of factors. This study did not discuss the budget and vulnerabilities [28]

Ismail, and others, (2010), presented a framework for ISM in Higher Education Institutions in Malaysian. This framework is based on a set of standards such as ISO 27001 and COSO. This study discusses a set of information security factors such as policies, risks, awareness, access control, Compliance, and management Support, shown in Fig. [3.5]. Management support and awareness had a fundamental and important role in the information security management of the Malaysian academies. The sample of this study is small, as the study was based on only four institutions. This study did not discuss other technological factors such as security tools and mobile access [32].

Fig. 3.5: Conceptual Information Security Framework for HEI [32]

Kazemi, M., and others, (2012), this study presented a model for the most important factors for the success of the information security management system in the Iranian municipal environment. This model discussed a group of success factors in implementing ISMS such as management support, information security policy, responsibilities, motivation, awareness and training programs, compliance, and using the services of the information security external advisors. The study found that management support, information security policy, awareness, and training programs are the most important success factors in implementing ISMS. However, this framework did not discuss all factors such as communications, culture, security tools, and mobile access [33].

W. Basri and others, (2017), in Fig. [3.6] presented a framework for establishing and improving information security policy in higher education institutions in Malaysia. This framework focused on the development of public security policies. The proposed framework has three stages: 1) Before development, it includes defining the policy team and defining the content of the policy. 2) The development stage includes risk assessment, policy preparation, policy writing, and policy approval. 3) The implementation stage includes publishing the policy, maintaining the policy. However, this framework did not take into account the development team's understanding of stakeholder expectations as well as the external factors that drive management to develop security policies [27].

Fig. 3.6: A Generic Framework for Information Security Policy Development [27].

A. I. Al-darwish and P. Choe, (2019), presented an information security framework that interacts with human factors. This framework aims to improve information security from the human factor only. This framework divided human factors into two groups; the first group is direct human factors: errors, ease of use, awareness, skills, experience, employee participation, motivations, ignorance, and security behavior. The second group is indirect factors and includes budget, return on investment in information security, organizational culture, information security integrity, communication, Enforce security policies, management support, risk awareness, and auditing. The researchers found that the indirect factors had an effect on the direct factors. However, this framework does not discuss the technological factors [23].

T. Tuyikeze and S. Flowerday, (2014), presented a model for implementing, developing, and enforcing security policies. This module is divided into ten categories: risk assessment, policy construct, policy implementation, compliance, policy update, management support, employee participation, security standards, legislative requirements, and stakeholders as shown in Fig. [3.7]. However, this study does not take into account existing policies in the organization and previous security events before developing security policies and does not take the policy team into account [26].

Fig. 3.7: Information security policy development model [26].

A.Alhogail, and others (2015), presented a framework for the issues of the human factors that affected on information security. This framework divided human factors into four fields: 1) the environment field, including national culture, organizational culture, and standards and regulations. 2) The field of administration includes security policy, practices, and communications. 3) The field of readiness, which includes awareness and change. 4) The scope of responsibility includes the employee's acceptance of responsibility, monitoring and control, and sanctions, as shown in Fig. [3.8]. However, this study does not provide the necessary security controls to improve the behavior of the human factor [24].

Fig. 3.8: The Human Factor Diamond (HFD) framework [24]

Aginsa, A., Yosef, I., & Edward, M. (2016). The study aims to design a framework that can be used by companies to manage information security, Designed framework adopts on ISO 27001 standard for ISMS and Zachman Framework, the framework it consisting of human, technical and process factors as shown in Fig. [3.9], the framework contains on guidelines, the author's seen that the processes and policy are the

important factors to implement ISMS. However, the framework did not discuss the budget for the implementation of ISMS [5].

Fig. 3.9: Enhanced ISMS Framework Design [5].

3.2 Summary of previous literature

Authors \year	Main Objectives	Study factors	pros and cons	Results of study
Werlinger. (2010)	Challenges of Implementing IT Security in Organizations	culture, security tools, risk perception , communication, mobile access, technology compatibility, vulnerabilities, budgeting, scheduling, risk assessment, interaction with other organizations, access control, distributed management, infrastructure, security priorities	pros : framework focused on Human, Organizational and Technological factors cons : the study sample was limited	framework that illustrates the interactions between human, technological and organizational challenges

A. Alhogail . (2015)	Attempts to integrate human factors that affected on IS in comprehensive framework	National culture, Organizational culture, Standards and regulations, Security policy, Practice, Communications, Awareness, Change, Employees' acceptance, Monitoring & control, Reward & deterrence	pros : integrate a lot of human factors cons: does not provide the necessary security controls to improve the behavior of the human	comprehensive framework for human factors that affects on IS in Saudi organizations
Al-darwish. (2019)	Classification of IS system challenges	Error, Usability, Awareness, Training, Education, Skills, Experience, Employee Engagement, Incentive Disincentive, Policy, Ignorance Negligence, Stress, Behavior, Budget, investment, Culture, Safety Climate, Communication, Policy Enforcement, Management Support, Business Dashboard, Risk Perception, Audit, Compliance	Pros: the framework focused on Human factors. Divided the impact of human factors into two forms, they are direct and indirect influence. Cons: This study is based on general concepts of the IS systems and did not simulate the reality of organizations to solve an existing problem.	presented a framework for improving information security on the part of human factors and their impact on the information security system in Qatar
Achmadi. (2018)	design framework for data center to Identify, reduce and manage security threats in the data center	21 controls from Annex A ISO27001, that related to people, technology and process	pros : the framework uses the PDCA concept that ensures continuous improvement. Cons: The framework does not discuss the budget and culture	proposed ISMS framework for data center to manage CIA
Teresa . (2010)	improve security management to assist organizations to classify attacks	security controls , protect assets, protect information properties, reduce threats, detect attacks, event, incident and protect vulnerabilities	pros : comprehensive framework to address attacks Cons: the framework discussed the technological aspect only	Conceptual framework to manage and audit IS

Sohail. (2012)	present Conceptual framework to secure organization's data	policy documentation, employee awareness, management support and access control	<p>pros : This framework discusses information security management from the security governance aspect.</p> <p>Cons: This framework did not discuss other factors such as culture, motivation and communication.</p>	Designed a framework for information security management, for companies in South Africa
Zammani. (2019)	identify ISM success factors in public and private organization in Malaysia.	Top Management, IS Coordinator Team, ISM Team, IS Audit Team, Employees, Third Parties, IS Policy, IS Procedures, Resource Planning, Competency Development and Awareness, Risk Management, Business Continuity Management, IS Internal Audit, and IT infrastructure	<p>pros : The study in included the public and private sector</p> <p>Cons: This study did not discuss the budget and vulnerabilities</p>	The results indicate that there are 14 factor. All factors are classified into four aspects are Human, Organizational Documents, Process and Technology that ensure the effectiveness of ISM implementation
Ismail .(2010)	Assesses ISM in Higher Education Institutions in Malaysian	Policy, Risk, Access control, Compliance and Awareness program & training	<p>pros : The framework is comprehensive and Risk Assessment is basic process in framework</p> <p>Cons: This study did not discuss other technological factors such as security tools and mobile access</p>	presented a framework for ISM in Higher Education Institutions in Malaysian
Kazemi .(2012)	identify the priority of key success factors in implementing ISMS in Iranian Municipal Organization	Management support, Policy, Responsibilities, Motivation, Awareness and training programs, Compliance, and ISMS external advisors	<p>pros : The most important success factors are ranked and identified.</p> <p>Cons: The model dose not discuss all factors such as security tools</p>	model that identify the priority of key success factors in implementing ISMS

Basri .(2017)	development of security policies in institutions of higher education	Team Development, Risk Assessment, Preparation, Writing Policy, Approval, Publish ,Monitoring Maintenance	pros : Security Policy Development process included a lot of factors. Cons : This study did not take into account management support and Awareness.	Framework for improve and establish Security Policy Development process
R. Alavi. (2014)	Understanding the impact of human factors on ISMS in organizations	Security Awareness, Communication, Management Support	pros : Meta-model illustrates the interaction of human factors cons : the proposed framework was not evaluated.	A Conceptual Framework to Analyze Human Factors of ISMS
A. Norman .(2013)	Determine the ISSM success factor that have an impact on business in Malaysia	Organization structure, Environmental influences, Security management practices, Culture	pros : four models of ISSM were analysis from three aspects: people, process and technology cons : the proposed framework was not evaluated.	ISSM success considerations theoretical model.

Table (2.5) Analysis of common isms frameworks in literature

CONCLUSION

By reviewing previous studies, it became clear that there is no 100% security system, and information security will remain a major challenge and worrying for all organizations, due to the organizations' need to share and secure information at the same time. The need for insurance and information sharing created a gap that constitutes a source of concern for organizations. Because security for organizations is a means to achieve an end, meaning that private sector organizations are keen on security in order to achieve profit, as is the case in service organizations, which consider security a secondary need in order to improve the service they provide, so security must serve the goal that the organization wants to achieve. In other words, the objectives of the organization create a need for information security in order to achieve the objectives, and this need for information security generates objectives for information security that serve the objectives of the organization, hence the role and importance of information security, as well as the importance of information security management .

Information security issues vary, they may take an administrative nature such as politics, or a human nature such as awareness and culture, or information security issues may take a technological nature such as software and hardware, and here shows the importance of a comprehensive approach to information security management in order to solve all information security issues .

The human being is the main focus in information security, and information security does not depend on technological solutions only. Rather, non-technological solutions such as security policies, training, and awareness programs for all employees of the organization must be reviewed in general and partially for each

according to his powers, or any other non-technological solutions that may The organization deems appropriate for it because information security has become a major player in the profitability of the organization and reduce insurance costs., and at the same time increasing the complexity of security controls for non-technological solutions that the organization does not need in the conduct of its business, it may increase the cost of operation and waste of time, so it must be Security controls cover security risks with the best available resources.

Information security must serve the goals of the organization, and the goals of the organization differ from one organization to another, and information security is affected by a number of factors such as policies, culture, awareness, effective communication, employees' sense of responsibility, administrative support, incentives, technology compatibility, wireless access, security tools, and management Security vulnerabilities. In order for the organization to adopt a specific framework, this framework must be designed based on a prior assessment of the security situation of the organization and includes all factors that affect information security from all organizational aspects, people, and technology. Otherwise, the organization will face difficulties and constraints to implement the framework. Hence the importance of allocating an adequate budget to provide all information security requirements.

References

- [1] Patiño, Susana & Mosquera, Carmen & Suárez, Franyelit & Nevarez, Ronnie, "EVALUACIÓN DE SEGURIDAD INFORMÁTICA BASADA EN ICREA E ISO27001", UNIVERSIDAD, CIENCIA y TECNOLOGÍA, 2017, Vol. 21, (pp. 129-139), ISSN 2542-3401.
- [2] K. I. Alshetri and A. N. Abanumy, Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia, *2014 International Conference on Information Science & Applications (ICISA)*, Seoul, 2014, pp. 1-4. doi: 10.1109/ICISA.2014.6847396
- [3] Michael E. Whitman, Herbert J. Mattord , Principles-of-Information-Security-4th- ed, 2011.
- [4] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements. International organization for standardization
- [5] A. Aginsa, I. Y. Matheus Edward and W. Shalannanda, "Enhanced information security management system framework design using ISO 27001 and zachman framework - A study case of XYZ company," *2016 2nd International Conference on Wireless and Telematics (ICWT)*, Yogyakarta, 2016, pp. 62-66. doi: 10.1109/ICWT.2016.7870853
- [6] E. Chisanga and E. K. Ngassam, "Towards a conceptual framework for information security digital divide," *2017 IST-Africa Week Conference (IST-Africa)*, Windhoek, 2017, pp. 1-8.
- [7]- COERTZE, Jacques Jacobus. "A framework for information security governance in SMMEs. 2013. PhD Thesis". Nelson Mandela Metropolitan University.
- [8]- DZAZALI, Suhazimah; ZOLAIT, "Ali Hussein. Assessment of information security maturity: An exploration study of Malaysian public service organizations", *Journal of Systems and Information Technology*, 2012. <https://doi.org/10.1108/13287261211221128>
- [9]- ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
- [10]- Abu-Musa, Ahmad. "Information security governance in Saudi organizations: an empirical study." *Information Management & Computer Security*, Springer-Verlag Berlin Heidelberg 2010, CCIS 122, pp. 18–28.

- [11]- Tarn, J. M., Raymond, H., Razi, M., Han, B. T., Rapids, G., & Raymond, H, "Exploring information security compliance in corporate IT governance", *Human Systems Management* 28.3,2009, 131–140. <https://doi.org/10.3233/HSM-2009-0698>
- [12]- Susanto¹², Heru, Mohammad Nabil Almunawar, and Yong Chee Tuan. "Information security management system standards: A comparative study of the big five." *International Journal of Electrical Computer Sciences IJECSIJENS* 11.5,2011, Vol: 11 No: 05
- [13]- ISO/IEC 27002:2013, Information technology — Security techniques Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- [14]- National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. SP 800-14. September 1996.
- [15]- National Institute of Standards and Technology. *An Introduction to Computer Security The NIST Handbook*. SP 800-12.
- [16]- Shojaie, Bahareh. "Implementation of information security management systems based on the ISO/IEC 27001 standard in different cultures". Diss. Staats-und Universitätsbibliothek Hamburg Carl von Ossietzky, 2018.
- [17]- Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. "Information security management needs more holistic approach: A literature review." *International Journal of Information Management* 36.2, 2016, 215-225.
- [18]- Alshaikh, Moneer. "Information security management practices in organisations." Diss. 2018. 1–294.
- [19]- Kitheka, Philip M. "*Information security management systems in public universities in Kenya: A gap analysis between common Practices and industry best practices*". Diss. University of Nairobi, 2013.
- [20]- Tipton, Harold F. and Micki K. eds . "*Information Security Management Handbook,*" 4th Edition. New York: Auerbach Publications. 2000.
- [21]- Siponen, M., & Willison, R. "Information security management standards: Problems and solutions." *Information & Management*, 46.5, 2009, 267-270.
- [22]- ISACA, "COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT", 2012.
- [23]- Al-Darwish, Ahmed I., and Pilsung Choe. "A framework of information security integrated with human factors." *International Conference on Human-Computer Interaction*. Springer, Cham, 2019.
- [24]- Alhogail, Areej, Abdurrahman Mirza, and Saad Haj Bakry. "A COMPREHENSIVE HUMAN FACTOR FRAMEWORK FOR INFORMATION SECURITY IN ORGANIZATIONS." *Journal of Theoretical & Applied Information Technology* 78.2 .2015. vol. 78, no. 2, pp. 201–211, 2015.
- [25]- Werlinger, R., K. Hawkey, and K. Beznosov. "Human, Organizational and Technological Challenges of Implementing Information Security in Organizations." *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)*. Lulu. com, 2008. no. section 2, pp. 35–147.
- [26]- Tuyikeze, Tite, and Stephen Flowerday. "Information Security Policy Development and Implementation: A Content Analysis Approach." *HAISA*. 2014., pp. 11–20.
- [27]- Ismail, Wan Basri Wan, et al. "A generic framework for information security policy development." *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. IEEE, 2017., no.pp. 19–21.
- [28]- Zammani, Mazlina, Rozilawati Razali, and Dalbir Singh. "Factors contributing to the success of information security management implementation." *Int. J. Adv. Comput. Sci. Appl.* 10.11 (2019): 384-391.
- [29]- Achmadi, Dedy, Yohan Suryanto, and Kalamullah Ramli. "On developing information security management system (isms) framework for iso 27001-based data center." *2018 International Workshop on Big Data and Information Security (IWBIS)*. IEEE, 2018.
- [30]- Pereira, Teresa, and Henrique Santos. "A security audit framework to manage Information system security." *International Conference on Global Security, Safety, and Sustainability*. Springer, Berlin, Heidelberg, 2010.
- [31]- Chaudhry, Peggy E., et al. "Enterprise information systems security: A conceptual framework." *Re-conceptualizing Enterprise Information Systems* (2012): 118-128.

- [32]- Ismail, Zuraini, et al. "Framework to manage information security for Malaysian Academic Environment." *Journal of Information Assurance & Cybersecurity* 2010 (2010): 1-16.
- [33]- Kazemi, Mehdi, Hamid Khajouei, and Hashem Nasrabadi. "Evaluation of information security management system success factors: Case study of Municipal organization." *African Journal of Business Management* 6.14 (2012): 4982-4989.
- [34]- Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. 'High-level self-sustaining information security management framework'. *Baltic Journal of Modern Computing*, 2017, 5(1), 107.<https://doi.org/10.22364/bjmc.2017.5.1.07>.