Sana'a University Journal of Applied Sciences and Technology

Vol. 1 | No. 1 | Page 1 – 12 | 2023 | https://jpurnals.su.edu.ye/jast

A Model for Enhancing the Information Security Management Systems in Yemen Banks

Nagi Ali Al-shaibany[1,*], Tariq A. Baqi Al-sofi [1], Ghaleb H. Al Gaphari [2]
[1]Department of Information Technology, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen
[2] Department of Computer Science, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen
*Corresponding author: E-mail: *shaibani@su.edu.ye*

ARTICLE INFO
Article history:
Received: October 20, 2022
Accepted: December 18, 2022
Published: January, 2023

Keywords
1. Security management
2. ISO 27002-2013
3. Yemen Banks
4. Security Model
5. Security evaluation

ABSTRACT: Exposure of valuable assets of Yemen banking sector to various attacks and threats may violate the privacy, confidentiality, integrity and accessibility (availability) of their data, information or computer systems resulting in financial and valuable loss. Such a violation may adversely affect the continuity of the business and the competitive advantages they seek to achieve. The objective of this paper is to evaluate the current security performance of banking systems in Yemen and to introduce a framework for improving information security management based on the ISO 27002-2013 benchmark and standards. The proposed framework includes important security factors which are people, technology and process. IBM SPSS AMOS is applied for testing framework hypothesis on complex variable relationships and gain new insight. Such framework shows that the process variable has obtained the most direct positive effect on improving information security management system with value (0.990), while the technology variable has obtained the second direct positive effect on improving the information security management system with value (0.930). Finally, the people variable has obtained the least direct positive effect on improving the information security management system with value (0.740). The research methodology includes: data collection, data analysis, reliability testing and computing results. The model validated and compared with other similar models available in the literature and the results were in valid range. Also, the research hypotheses were significant and deferent results of the proposed model were very promising.

CONTENTS

1.Introduction

The development of information and communication technology has created a significant leap in improving business's efficiency, accuracy and increasing its productivity. Moreover, IT assets include data, networks, hardware, and software are now considered as one of the resources and essential operators of successful business organizations in banking systems [5, 6]. At the same time, there is an emerged negative side of using technology since it opened the way for the development of the methods of informational threats such as breaching the safety, availability and confidentiality. Within the banks industry, it necessary to adopt the information security management systems (ISMS) for continuous operation and protection of asset and personal data. In this regards, numerous studies have concluded that exposure of valuable assets of banking institutions to various attacks and threats may violate the privacy, confidentiality, integrity and accessibility (availability) of their data, information or computer systems resulting in financial and valuable loss. Such a violation may adversely affect the continuity of the business and the competitive advantages they seek to achieve [1,2,3].

Like other international financial sectors, the Yemen banking sector will continue to be under heightened and persistent security threat and attacks unless it continually takes and committee to measure, apply, compile, and update the information security controls. These threads could adversely affect its functionality, reliability, and delivery of its services. Hence, protecting the financial institution's assets and application considered an essential point to guarantee business continuity and minimize business risk. [nada], so the evaluation of the security performance in banking systems and steps to improving it is the one of the critical steps required to achieve this goal, Therefore, this paper aimed to Evaluating security performance of banking systems in Yemen according to the ISO 27002-2013 standard and proposed the framework to improvement the vulnerable of information security operations. The proposed framework includes important factors which are people security, technology security and process security. This framework is tested and validated using Amos tools. It is also evident from the framework that the process variable was the most direct positive effect on improving the information security management system (0.990), followed by the Technology variable was the second direct positive effect on improving the information security management system (0.930). The people security variable was the least variable, direct positive effect on improving the information security management system (0.740).

2 Related work

A comprehensive review was conducted on current status related to information security management of banks for specifying the existing gaps in this area. The review covered available models and frameworks which help in figuring out the important factors for improving information security. Among the most prominent studies in this regard is indicated in [1] which used the ISO27001 standard to assess the performance of the financial institutions in information security management systems, he found some deficiencies in some control categories such as the organization of the Information Security. The researcher concluded that the information security management should be based on rules, policies or controls mandatory imposed by the high-level administration. Finally, the researcher recommended that different companies in the financial services sector should follow the directions provided by government officials. Authors in [2] proposed a framework for data centers security management on the bases of three aspects: confidentiality, integrity, and availability. The framework includes three factors: people, policies, and technology to manage and protect information for enhancing the

security in the data center. This framework was developed based on the ISO 27001 standard; the framework mainly concerned with people rather than budget. Author in [4] assessed the current (ISMS) of banking sector in Ethiopian banks, hence introduced a framework to improve information security management. The framework is a combination of two models, one of them is Entity Relation Model (ERM), while the other is the ISMS process model, this framework depends on ISO27001 standard and classified under three categories: administrative, Technical, and Physical & Environmental security. The suggested framework is still a general approach to ISM program. It requires detail policies and procedures formulation and comprehensive test in the real banking environment.

The author in [5] presented an intrusion detection framework for Rafi Dain_Bank, he concluded that the banks should have intrusion detection systems to prevent any threat and to increase their security performance.

Authors in [6] focused on the most important factors affecting the improvement of Information Security Management (ISM) in the banking industry in Nigeria. They proposed a framework consisting of the most important factors affecting the management of information security consisting of technological, organizational and environmental (TOE) factors, that can lead to improving the security of information systems (IS) among Nigerian banks, and the study focused on the human factor, but the study did not mention Budget allocated for information security and incident management.

Authors in [7] evaluated the cybersecurity in financial institutions, then he developed a framework for enhancing the performance based on NIST framework. This study focused on auditing of cybersecurity which might not be generalizable in terms of other fields.

Authors in [9], introduced a framework on the bases of the data security standard FFIEC, COBIT, ISO 27002 and PCI where the framework is categorized into strategic, tactical, operational and technical levels. Unfortunately, the study ignores the human factor, which is one of the most important factors influencing the governance of information security.

The research study in [10] proposed a model consisting of three factors: physical protection, employee protection, and software protection, which has significant impact on the security and confidentiality of information in banking performance in banks operating in Jordan. Unfortunately, the model has not indicated any organizational policy factors. Most frameworks and models covered in this section have lack of factors such as the national and organizational culture, environment and level of awareness and how these factors relate to generic attitudes towards information security and its management. Thus, this paper has introduced a comprehensive framework solution that addressed human awareness, organizational culture with technical solutions, policies and procedures which may improve the security systems in Yemen Banks.

3 The Conceptual Model

The main objective of the proposed model is to explore and evaluate the reality of information security management in Yemen banks on the bases of ISO27001 benchmark and stander. The model also, identify success factors that have a great impact on improving information security management systems in Yemen banks community as shown in Fig. 1. The model focused on the relationship between three independent variables: people security process, technology, and the dependent variable.

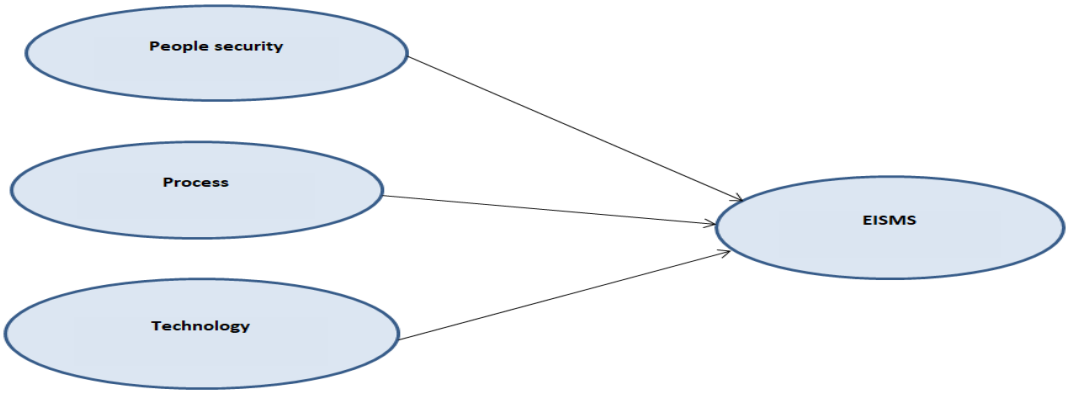

Fig. 1. The proposed study

3.1. Major Components of the Proposed ISMS Framework

Various factors affect the information security that comprises of three main components namely:

3.1.1. People Security Factors:

Human factors are considered the weakest ring in information security as long as they are not aware of their responsibility in that domain. Human error is the significant cause of information systems security threats such as poor awareness, boredom, lack of training, and lack of risk perception. Thus, it is necessary to state the hypothesis(H1)

H1: people security (PS) has a positive effect on enhancing information security management system (EISMS).

In this study, human security component is divided into three sub-components:

3.2.1.1. Management Support (MS)

The implementation of information security in organizations can be difficult when organizations do not get any support from the top management regarding the information security, So Top management is the backbone of implementing an effective information security management system [18].

3.2.1.2. Awareness Security (AS)

All employees should be aware of potential security threats. They should have enough IT literacy that provides a basic level of concept in information security [21]. On the other hand, raising awareness serves for focusing employee attention on information security in order to ensure their understanding of their roles and responsibilities in the protection of information [26, 27].

3.2.1.3. Communication and Connection (CC)

Utilizing users in the direction of compliance with security policy and exchanging of ideas and experience between people inside and outside of the organization that is an important issue of ISMS tolls and procedures.

3.2.2. Process Factor

ISMS process is a two-phase information security management system which focuses on planning and implementing management practices, procedures to establish and maintain information security, thus the hypothesis(H2) would be pressed.

H2: Process security (PS) has a positive effect on information security management system (EISMS) enhancement. In this section, the process factor consists of five sub-factors as follows:

3.2.2.1 Organization of Information Security (OIS)

Organization of information security concerns with higher management approval in terms of organization development that includes: policies, technologies and people role and responsibilities within the organizations.

3.2.2.2. Information Security Policy (ISP)

ISP is an important factor to guide and direct information security [29, 30] in the organization. It should be clear, compatible with legal and ethical norms, on the other hands, it should be effective in case the implementation.

3.2.2.3. Supplier Relationships (SR)

Supplier Relationship Management is a comprehensive control to manage banks interactions with the firms that supply the products and services. Such firms may expose partially or totally banks services to different security risks that validates confidentiality, integrity, and availability issues. This control mechanism ensures that supplier activities performed in a safe manner [33].

3.2.2.4. Business Continuity Management (BCM)

Business continuity management (BCM) is a predefined set of instructions that describe how an organization's mission-essential functions will be sustained [34]. Thus, achieving the availability of data is considered the primary objective of both business continuity as well as information security management [38, 40].

3.2.2.5. Information Security Incident Management (ISM)

Incident management is a series of sequential processes which includes six phases: preparatory, detection, containment, mitigation, recovery and a learning [42]. Banks are exposed to some kind of risks that may damage their business in different ways of attacks. It is necessary to develop and implement plans to prevent risk, minimize the damage and to recover from disaster [35].

3.2.2.6. Compliance (CO)

It is well known that cyber-attacks, information theft, and online fraud are becoming common in the banking industry as a result of non-compliance with policies and information security standards by the employees [40]. therefore, more attention has been directed toward the human compliance with information security policy, as a more important step towards effective information security management [41, 42].

3.2.3. Technology Factor

Information systems include hardware, software, technical expertise which is considered as important as managerial professionalism. It is divided into two major parts: technical and managerial expertise. thus, integration of these two aspects will ensure the effectiveness of information security (Ji, Wang, Min, & Smith Chao, 2007; Kayworth & Whitten, 2010; Young & Windsor, 2010).

Therefore, we can state the following hypothesis as:

H3: Technology security (TS) has a positive effect on the enhancing information security management system (EISMS).

Therefore, the technology component in this proposed framework comprised of two main sub-components: Software, and hardware. The software subcomponent itself is divided into six subcomponents. On the other hand, the hardware component consists of two sub-components, as indicated in the following subsections:

3.2.3 .1. Access Control (AC)

Access Controls Management is very important for allocating users responsibilities in terms of accessing their own tasks and protecting data and resources against unauthorized users [44, 45].

3.2.3.2. Cryptography (CR)

Authors in [46, 47] reported that encryption is a very important component for banks data privacy and communication with other organizations, they also concluded that encryption is important factor which improves information security management.

3.2.3.3. Operations Security (OS)

Authors in [48] emphasize that procedures and responsibilities for bank operations including information services document, tracking processes activities on records, risk assessment and auditing which enhance the information security.

3.2.3.4. Communications Security (CS)

The aim of CS is to set controls for protecting and securing the information network and exchanging information with other organizations, it is considered one of the success factors of information security management [49] in banks.

3.2.3.5. System Acquisition, Development and Maintenance (SADM)

Authors in [50] indicated that security is an integral part of information systems acquisition and development [50]. Thus, identifying security vulnerabilities of the system when developing, purchasing, or acquiring systems. Therefore, the SADM consider important for ISMS.

3.2.3.6. Asset Management (AM)

ISO / IEC 27001: 2013 defines the term assets as “anything of value to an organization”. Assets can range from data files to physical assets, such as removable media. However, the definition of ISO allows an organization to classify items as assets of a wider range including: intangibles, such as the reputation of the organization, utilities, and skill sets of the workforce can be categorized as assets. The main objective of asset management is to achieve and maintain appropriate protection of the organization's information assets [51].

3.2.3.7. Physical and Environmental Security (PES)

Author in [52] mentioned that physical infrastructure of information technology is important for banks, so it must be protected and secured from any potential danger such as destruction, modification and appropriate disclosure. The PES should be placed in a safe area with adequate security perimeter physical access to facilities is monitored and restricted.

Since people, processes, technology security factors and their sub-factors are very important in terms of improving and enhancing banks information management security as indicated above. Therefore, this research study proposed a hybrid model on the bases of two different original models introduced by A B, for improving and enhancing banks information security management. The new adaptive model combines two different types of parameters represent new factors which occur very important in securing banks information management as shown in Fig (1).

4 METHODOLOGY

4.1 Methodology description

This research study is applied descriptive and analytical methods in its process’s conduction:

1. Collecting data using questionnaire survey and staff interview where a number of surveys is distributed to 160 employee of Yemen banks. The

number of retrieved and valid questionnaires for the analysis were only 129 with response rate of 81.62% which is an acceptable response rate. On the other hand, a number of interviews with information technology team are held.

2. Analysing data using AMOS tool to:

- verify that model interrelated factors are fully integrated and capable for improving and enhancing the information security management in banks.

- testing all factors and selecting the most significant factors to be best representative factors in the adaptive model while those less significant are eliminated.

3.Reliability Test

Cronbach's alpha used to determine if the scale is reliable when using multiple Likert questions in a questionnaire. In order to confirm reliability and consistency, the values of Cronbach alpha must meet the minimum acceptable criteria, there are several reports of these values, ranging from 0.70 to 0.98[15] , Table 1 shows the reliability statistics table that provides the actual value of the Cronbach alpha for each sample.

Table [1]

Number of Items	Variable	Alpha	Alpha½
13	People Security	90.2%	94.8%
26	Process	95.7%	97.8%
48	Technology	97.3%	98.6%
87	All items	98.0%	99.0%

From the result, the above table shows the stability of the data collection tool and the credibility of answers, that the values of the Cronbach's alpha coefficient (α) for data collecting scale stability is 98% and the credibility of the answers Alpha½ is 99% which means a high degree of the credibility of the answers, and this means that the sample is homogeneous in responding to the questionnaire and greatly can depend on the results and generalize it to the research community. Consistency coefficients indicate that the instrument generally has a high coefficient of consistency, indicating the instrument's ability to achieve its intended purpose. The final model depicted in Fig (2).

4.2 Descriptive Results

Table 2: presents the summary of basic statistics for the participants in this survey.

	Gender	**Frequency**	**Percentage %**
Gender	Male	115	89.1%
	Female	14	10.9%
Education	Diploma	9	7.0%
	Bachelor	98	76.0%
	Master	22	17.1%
	PhD	0	0%
Major	Information systems	26	20.2%
	Information Technology	39	30.2%

	Networks and connections	13	10.1%
	Computer science	40	31.0%
	Others	11	8.5%
Position	Manager	13	10.1%
	Supervisor	25	19.4%
	Employee	91	70.5%
Experience	Less than 5 years	26	20.2%
	From 5 to Less than 10 years	33	25.6%
	From 10 to Less than 15 years	42	32.6%
	15 years and more	28	21.7%

4.3. Conceptual Model Testing

The test process focused on model structure and its measurements using AMOS program where the test conducted during two phases:

1 Structure Equation Model:

Confirmatory factor analysis (CFA) is applied on the conceptual model for analyzing overall measurements of the model that includes all latent constructs with their corresponding indicators. In this phase different sub factors are evaluated on the basis of convergent validity [108], where sub factors with loading greater than 50% considered as effective sub factors in the new proposed model while those sub factors with loading factors less than 50%are eliminated from the new proposed model as shown in Fig. 2 which represents the new proposed model.

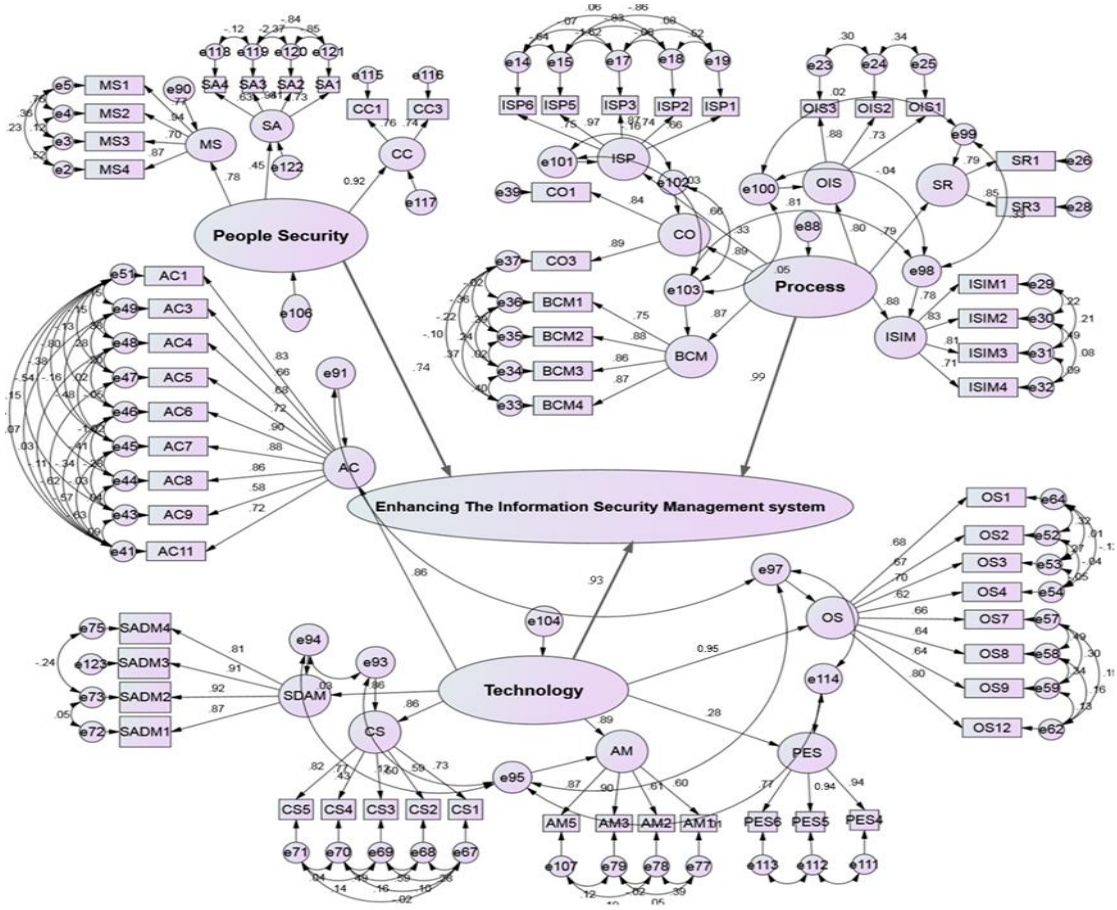

Fig. 2. Overall CFA Model for Research Model

2 Structure Equation Model for Framework Fitness

Structural equation modeling (SEM) is applied for evaluating the proposed model, this technique is a suitable data analysis tool. In this phase, the evaluation process focused on computing the fitness of proposed model base on some statistical measures [haird]:

- Chi-square test measures the adequacy of a hypothesized model in terms of its ability to reflect variance and covariance of the data. Such test is sensitive to sample size, and therefore, the value of x^2 to its degree of freedom (x^2 /df) should be less than 3 which indicates an acceptable fitness between the original model and the sample data. The proposed model in this experiment achieved 2.210 as indicated in table 3 which is less than 3. This value reflects the adequacy of the proposed model and its best fit.
- Comparative fit index (CFI) examines the discrepancy between the data and the hypothesized model. The CFI value ranges from 0 to 1 with larger values indicating better fit. The proposed model in this experiment obtained 0.927 which is quite reasonable to indicate the best fit of the proposed model.
- Root Mean Square Residual (RMR), is used to judge the validity of the proposed model to explain the relationships between the study dimensions, and the acceptable value ranges from 0 to .08, and it indicates the value of the residual variance. The proposed model in this experiment obtained the value 0.014 which indicates the proposed model best fit.
- Root Mean Square Error of Approximation (RMSEA) is the standard deviation of residuals which measures the quality of prediction. The RMSEA value ranges from 0.2 to 0.5, while the proposed model obtained 0.067 which falls within the valid range and indicates model best fit.

Table 3 reveals that all measures of goodness of fit fall within the recommended values and the model has a good fit with the data.

Table 3 The measures of model fitness

Fit Measure	Recommended Value	Fitness Measure	Reflection
x^2/ df	<3	2.210	Good Fit
CFI	≥ 0.90	.927	Good Fit
RMR	< 0.080	.014	Good Fit
RMSEA	< 0.080	.067	Good Fit

4.5 Hypotheses test:

Table 4 Results of Hypothesized Direct Effects of the Variables in Structural Model

path			Estimate	S.E.	C.R.	P	Supported
People	<---	EISMS	0.740	.156	4.758	0.000	Support
Process	<---	EISMS	1.351	.284	4.758	0.000	Support
Technology	<---	EISMS	1.134	.208	5.455	0.000	Support

The experiment results of the path analysis as shown in Table 4 reflects those three hypotheses are Significant. The independent variables: People, Process and Technology account for a significant variance in the dependent attitude latent variable. In addition, the indicators: People, Process and Technology account for a significant variance in the dependent construct of ISMS. The results indicated that the variance of ISMS improvement is 0.28. The model presented in Figure 2 has the potential to predict improvement of ISMS based on process, people and technology security to enhance ISMS in banks sector of Yemen.

5. CONCLUSION

In today's technological and social environment, security issue represents a very important part of banks sector in Yemen. Unfortunately, exposing assets of Yemen banks sector to various attacks may violate the privacy, confidentiality, integrity and availability of their data, information or computer systems resulting in financial loss. The main objective of this study is to evaluate the current ISMS of Yemen banks based on ISO standards and to introduced a model that integrates three various security factors: people, process and technology which improve ISMS as shown in Fig.2. The results obtained by this study indicate a significant and positive relationship among most of the investigated factors. The findings of this model reflect that the process factor has the most direct positive effect on improving ISMS with rate (0.990), while the technology factor has the second direct positive effect on improving ISMS with rate (0.930). Finally, the people variable has obtained the least positive effect on improving the ISMS with rate (0.740). The model was validated and compared with other similar models available in the literature, and the results were within valid domain. Adapting and applying this model by Yemen banks sector would improve and enhance its ISMS. Also, the findings and contribution of this study could be useful for Yemen banks policymakers in imposing the model adaption and application for raising up banks' security.

References

[1]. Kim, S., B. Kim, and M. Seo, Impacts of Sustainable Information Technology Capabilities on Information Security Assimilation: The Moderating Effects of Policy—Technology Balance. Sustainability, 2020. 12(15): p. 6139.

[2]. Samimi, A., Risk Management in Information Technology. Progress in Chemical and Biochemical Research, 2020: p. 130-134.

[3]. Anton, N. and A. Nedelcu. Security risk analysis and management. in MATEC Web of Conferences. 2018. EDP Sciences.

[4]. Ključnikov, A.,L.Mura, and D. Sklenár, Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 2019. 6(4): p. 2081.

[5]. Itradat, A., et al., Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. Jordan Journal of Mechanical & Industrial Engineering, 2014. 8(2).

[6]. K. Samota1, J.P., Recent IT Trends: A Review Paper. International Journal of Scientific Research in Multidisciplinary Studies, 2017. Volume-3,Issue-5.

[7]. Kiilu, K. and D.M. Nzuki, Factors affecting adoption of information security management systems: a theoretical review. International Journal of Science and Research (IJSR), 2016. 5(12): p. 162-166.

[8]. Elamin, B., The Impact Of Information Security Management For E- Banks Performance In Kingdom Of Sudi Arabia. 2016.

[9]. Boese IV, R.F., PCI DSS Compliance Challenges for Small Businesses. 2020, Utica College.

[10].Ula, M. and W. Fuadi. A method for evaluating information security governance (ISG) components in banking environment. in Journal of Physics: Conference Series. 2017. IOP Publishing.

[11].Kaušpadienė, L., Simona Ramanauskaitė, and Antanas Čenys., Information security management framework suitability estimation for small and medium enterprise. Infinite Study 2019.

[12].Kaušpadienė, L., S. Ramanauskaitė, and A. Čenys, Information security management framework suitability estimation for small and medium enterprise. 2019: Infinite Study.

[13].Achmadi, D., Y. Suryanto, and K. Ramli. 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). 2018. IEEE.

[14].Mohamad Noorman Masrek, Q.N.H., Ishak Ramli, Prasetyo, The Role Of Top Management In Information Security. International Conference on Education, Social Sciences and Humanities 2019. 24-26 June

[15].Dey, M. Information security management-a practical approach. in AFRICON 2007. 2007. IEEE.

[16].Surwade, Y.P. and H.J. Patil, Information Security. E-Journal of Library and Information Science, 2019: p. 458-466.

[17].Amini, M., H. VakiliMofrad, and M.K. Saberi, Designing and Psychometric Evaluation of Questionnaire of Human Factors Affecting Information Security in Libraries. Library Philosophy and Practice, 2020: p. 1-19.

[18].Volonino, L., S.R. Robinson, and C.P. Volonino, Principles and practice of information security: protecting computers from hackers and lawyers. 2004: Pearson/Prentice Hall.

[19].Wu, Y. and F. Meng, Categorizing security for security management and information resource management. Journal of Strategic Security, 2018. 11(4): p. 72-84.

[20].KHOURI, S., Analýza bezpečnosti informačných systémov organizácií Analysis of information systems' security in companies.

[21].Li, Y., Z. Li, and L. Chen, Dynamic state estimation of generators under cyber attacks. IEEE Access, 2019. 7: p. 125253-125267.

[22].Andress, J., The basics of information security: understanding the fundamentals of InfoSec in theory and practice. 2014: Syngress.

[23].Raggad, B.G., Information security management: Concepts and practice. 2010: CRC Press.

[24].Abebe, G. and L. Lessa, Human Factors Influence in Information Systems Security: Towards a Conceptual Framework.

[25].Pavlov, G. and J. Karakaneva, Information security management system in organization. Trakia Journal of Sciences, 2011. 9(4): p. 20-25.

[26].Jouini, M., L.B.A. Rabai, and A.B. Aissa, Classification of security threats in information systems. Procedia Computer Science, 2014. 32: p. 489-496.

[27].Gerić, S. and Ž. Hutinski, Information system security threats classifications. Journal of Information and organizational sciences, 2007. 31(1): p. 51-61.

[28].Ruf, L., C. Thorn, and T. Christen, Threat Modeling in Security Architecture-The Nature of Threats. ISSS Working Group on Security Architectures. 2006.

[29].Radu, L.-D., Green ICT: Some challenges and potential solutions. Acta Oeconomica Universitatis Selye, 2018. 7(2): p. 141-150.

[30].Davidavičienė, V., et al., The importance of security aspects in consumer preferences in electronic environment. Journal of Security & Sustainability Issues, 2019. 8(3).

[31].Kazemi, M., H. Khajouei, and H. Nasrabadi, Evaluation of information security management system success factors: Case study of Municipal organization. African Journal of Business Management, 2012. 6(14): p. 4982-4989.

[32].Chernysh, I., V. Makhovka, and L. Lobach, Management of information security Of the enterprise in the conditions of dynamic business environment. ЕКОНОМІКА І РЕГІОН Науковий вісник, 2020(1 (76)): p. 106-112.

[33].Haqaf, H. and M. Koyuncu, Understanding key skills for information security managers. International Journal of Information Management, 2018. 43: p. 165-172.

[34].Standardization, I.O.f., ISO/IEC 27001: 2013: , Information Technology--Security Techniques--Information Security Management Systems--Requirements. International Organization for Standardization., 2013.

[35].Al-Dhahri, S., M. Al-Sarti, and A. Abdul, Information security management system. International Journal of Computer Applications, 2017. 158(7): p. 29-33.

[36].Jr, N., Information Security Policy Development: A Literature Review. International Journal of Innovative Research in Information Security, 2016. 3 (4): 01-06.

[37].Siponen, M.T. and H. Oinas-Kukkonen, A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2007. 38(1): p. 60-80.

[38].Awad Elfergani , A.S., Assessment of Security Issues in Banking Sector of Libya. international Journal of Computer Applications 2020. Volume 176 – No. 13, April 2020.

[39].Ahmad, A., et al., How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 2020. 71(8): p. 939-953.

[40].Tjirare, D.J. and F.B. Shava. A gap analysis of the ISO/IEC 27000 standard implementation in Namibia. in 2017 IST-Africa Week Conference (IST-Africa). 2017. IEEE.

[41].Javaid, M.I. and M.M.W. Iqbal. A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). in 2017 International Conference on Communication Technologies (ComTech). 2017. IEEE.

[42].Zaydi, M. and B. Nassereddine, A Conceptual Hybrid Approach for Information Security Governance. Computer Science, 2021. 16(1): p. 47-66.

[43].De Haes, S., et al., Enterprise Governance of IT, Alignment, and Value, in Enterprise Governance of Information Technology. 2020, Springer. p. 1-13.

[44].Apriliana, A.F., R. Sarno, and Y.A. Effendi. Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5. in 2018 International Conference on Information and Communications Technology (ICOIACT). 2018. IEEE.

[45].Bernard, P., COBIT® 5-A management guide. 2012: Van Haren.

[46].Hago, E.B.E., M.E.A. De Vigal Capuno, and S.H.M. Ali, IT Service Management System for Central Bank Of Sudan. International Journal of Managing Information Technology (IJMIT) Vol, 2019. 11.

[47].Yulianto, S., C. Lim, and B. Soewito. Information security maturity model: A best practice driven approach to PCI DSS compliance. in 2016 IEEE Region 10 Symposium (TENSYMP). 2016. IEEE.

[48].Ukidve, A., D. Smantha, and M. Tadvalka, Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 framework. International Journal of Engineering Research and Applications, 2017. 7(01): p. 42-48.

[49].Ismail, Z., et al., Framework to manage information security for Malaysian Academic Environment. Journal of Information Assurance & Cybersecurity, 2010. 2010: p. 1-16.

[50].Munir, U. and I. Manarvi, Information security risk assessment for banking sector-A Case

study of Pakistani banks. Global Journal of Computer Science and Technology, 2010.

[51].Ula, M., Z. Ismail, and Z.M. Sidek, A Framework for the governance of information security in banking system. Journal of Information Assurance & Cyber Security, 2011. 2011: p. 1-12.

[52].Susanto12, H., M.N. Almunawar, and Y.C. Tuan, Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS, 2011. 11(5): p. 23-29.

[53].Tebkew, K., Information Security Management Framework For Banking Industry In Ethiopia. 2013, Thesis work, Addis Ababa University, Addis Ababa.

[54].Mohseni, M., Has your organization compliance with ISMS? A case study in an Iranian Bank. arXiv preprint arXiv:1303.0468, 2013.

[55].Gürcan, İ., 'Assessing information security management requirements for finance sector using an ISO27001 based approach (Master Thesis), Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul. Bahçeşehir University Graduate School of Sciences, İstanbul, Turkey, 2014.

[56].Muhsen, A.L., Information Security Management in Palestinian Banking. 2014.

[57].Aginsa, A., I.Y.M. Edward, and W. Shalannanda. Enhanced information security management system framework design using ISO 27001 and zachman framework-A study case of XYZ company. in 2016 2nd International Conference on Wireless and Telematics (ICWT). 2016. IEEE.

[58].Wu, S.M., et al., Web-based analytic hierarchy process (AHP) assessment model for information security policy of commercial banks. 2015.