International Journal of Scientific Research in Computer Science and Engineering
Vol.8, Issue.6, pp.08-18, December (2020)
Research Paper
E-ISSN: 2320-7639

On The Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen

Adel A. Nasser[1]*, Nada Kh. A. Al Ansi[2], Naif A. N. Al Sharabi[3]

[1]Dept. of information systems, College of Science, Sa'adah University, Sa'adah, Republic of Yemen
[2]Dept. of management information systems, Al-Hikma University, Sana'a, Republic of Yemen
[3]Dept. of Comp. science, College of Eng. &IT, Amran University, Amran, Republic of Yemen

Corresponding Author: adelru2009@mail.ru, Tel.: +967-772417767

Available online at: www.isroset.org

Received: 13/Nov/2020, Accepted: 08/Dec/2020, Online: 31/Dec/2020

***Abstract*—** This paper aims to discuss the efficacy of the standardization controls of the information security operations in Yemeni banks by investigating the main requirements for their implementation to carry out their security roles effectively. Also, to determine the standardization practices' main weaknesses in the information security management systems (ISMS) of the banking sector and to provide the necessary improvement recommendations based on the ISO 27002-2013 international security standard. The researchers designed a questionnaire distributed to workers responsible for information security statements in 13 banks regulated by Yemen's central bank, in Sana'a. The result shows that these practices' actual maturity level is 3.66 out of 5, which means that best practices are not consistently followed. The gap between the maturity level of real application of information security practices and the robust level was found; it equals 1.34, which means that the ISMSs in this sector do not have most of the security requirements necessary for their practical and robust functioning. Two significant points of strength were defined. Three main lacks and weak points were discovered, and the improvement actions and recommendations have been suggested to improve the standardization practices of information security operations in this sector. Additional implementation matrix mapping schemes and ISO-based implementation guidance for each bank have been recommended.

***Keywords*—** Information security; Assessment; Banking sector; Yemen; Standardization Practices

I. INTRODUCTION

For many countries, the enormous and increasing development of information technology has generated many trades and investment opportunities. It represents one of the main drivers on which these countries are relaying to make significant development leaps and quickly, quality and efficiency achieve its development objectives. Many sectors, including the banking sector, have greatly benefited from this transformation. In the opposite direction of such economic and developmental gains, its application's negative impacts have emerged. In this context, the business sector is facing and affecting thousands of daily scattered around the world, information security threats and attacks. The banking sector and its primary services have not been exempted from these threats and attacks, as confirmed by the IBM Security report [1]. This report indicated that in 2019 the banking sector was the most attacked industry, and information security attacks on this sector accounted for 17 % of all security attacks in the top ten attacked industries. Many studies have been addressed the threat of cybercrime, security attacks, incidents, breaches, and their effect on the banking institutions; some of the most prominent are presented in works [2,3,4,5,6]. These studies and other similar studies have concluded that the exposure of such banking institutions' valuable assets to various attacks and threats may violate the privacy, confidentiality, integrity, and accessibility (availability) of their computer data, information, or systems. This violation could negatively affect the business continuity, competitive advantages that they seek to achieve [7,8].

Like other international financial sectors, the Yemen banking sector will continue to be under heightened and persistent security thread 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. The evaluation process of the banking systems presented one of the critical steps required to achieve this goal. Under our research project, we seek to identify the level - (maturity level (ML)) - to which the Yemen banking sector (YBS) can meet the IS requirements during increasingly distributed security attacks and incidents. The information security assessment categories could be ordered into four main groups under which

different security areas are grouped [9,10]. These categories are Processes and Procedures (IS operations), management and governance aspects of IS, Technology innovations for IS purposes, and capacity risk management. Evaluation, analyzing, and giving the appropriate recommendations and improved controls for a whole banking system in Yemen for all four categories is a long and challenging process. For this reason, this paper addresses to evaluate, rank, and analyze the extent of processes and procedure domain practices (standardization practices related to information security operations- (SPO)) in the YBS.

So, the main problem of the study can be crystallized in the following questions:
Q1- What is the actual ML of the SPO in the YBS?
Q2- What is the gap between the actual ML of the SPO in the YBS and the maximum recommended ML?
Q3- What are the principal strength and weaknesses points of standardization practices in this sector?
Q4- How to rate the institutions in this sector according to their information security maturity level?
Q5- What are the most appropriate solutions and recommendations to improve the security situation in the YBS sector?

Therefore, this paper aimed to ascertain the extent and actual maturity level (ML) of standardization practices related to information security operations (SPO) in the Yemen banking sector (YBS). It also attempts to determine the gap between the real ML of the SPO in the YBS, and the maximum recommended ML. It also aims to discover the vulnerable SPO aspects in the YBS and provide the main necessary recommendations and improvement actions to diminish the gap and facilitate the SPO practices according to the ISO 27002-2013 standard.

The prominence of this work sticks from the reputation of the subject it addresses, i.e., processes and procedures of IS based on ISO/IEC: 27001/2013 international standard. The study is essential as it focuses on the topic of IS in the two primary SPO fields of indicators that this international reference provides, i.e., access management 'AM' and compliance 'COM'. What, too, creates its criticality is the pivotal role of IT and IS infrastructure, data, and assets in providing the banking business and services and the unnamed consequences if it were exposed to IS risks and breaches. It becomes further essential when the study is made under the banking environment, which is externalized as one of the uttermost significant pillars of the Yemeni financial, business, and economic sector. Moreover, this research shall support and serve both the decision-makers, the administrative and functional staff of the IS and IT departments in the YBS, and shall contribute to the progression there IS culture and knowledge on how to control all the SPO aspects so as not to be holdback that restricts the YBS's information protection ability and efficiency. Also, this work is vital as it improves the grasp of handling self-assessment of SPO practices, assuring appropriate management of SPO, which guarantees the permanence of YBS's business. Furthermore, it is expected to provide recommendations, which would help political leaders, strategic decision-makers to translate it into proper work policies and strategic plans. In the remaining four sections of this paper, we complete the proffer of its content as follows. The second part is dedicated to present the literary aspect and previous studies related to the topic of the study. A Methodology of research and steps for its implementation are presented in sec. Three. After that, the applied results were summarized and discussed in the fourth sec., the Fifth section was devoted to the recapitulation of the most prominent conclusions reached.

II. RELATED WORK

A. Information security assessment in banking sector

Many local and regional literatures have addressed the issue of assessing information security practices in banking environments. Among the most prominent local studies in this regard is a study [11], which aimed to know the impact of information security risks on the accounting systems in the Central Bank of Yemen, according to the results of this study, the risks of information safety security affect the integrity, confidentiality and readiness of these systems, in addition, the study concluded that there is no department concerned with risk management in the bank. Regionally, a study [12] aimed at evaluating the performance of security mechanisms in banking institutions, identifying strengths for their development and identifying weaknesses to address them. Among the most prominent findings of this study is that banking institutions do not provide an integrated system dedicated to managing information security issues from all sides. Therefore, they suffer from many weaknesses, most notably the lack of protection policies, as well as the lack of experience among workers with protection mechanisms and technologies. This study presented many recommendations, the most important of which is the necessity to strive to match the work procedures in these banks with the ISO standards and to keep them up to date, to provide the qualified and trained human element to deal with this technology, to provide information security specialists to establish security policies and review their implementation. The study [13] aimed to present and analyse the reality of security measures indicators to prevent penetration of the information systems of the Rafidain Bank. That study concluded that there are many weaknesses, and recommended the necessity of working to reduce security breaches by training the bank's employees on the use of effective and efficient protection programs. It also recommended the activating and applying new indicators to improve the security of information systems in that bank. The study [14] aimed at examining the current status of information security management in Palestinian banks, measuring the degree of application of information security management controls in Palestinian banks, has reached several findings, most notably that banks that adopt international information security management standards apply information security management controls to a higher degree than others. It

recommended that international information security management standards be followed, that an information security regulation and planning approach be formally adopted, that technology development is followed up and pursued to reduce the vulnerability of banks' technologies. The study [15] reviewed the maturity levels of the standard in the financial services sector in Turkey, and concluded that there was still some lack of controls such as the Information Security Department, and recommended that all firms in the financial services sector follow the relevant Security directives.

By analysing these studies, it was clear that, organizations do not provide an integrated system dedicated to managing information security issues in all aspects, there is a variation in information security breaches between banks according to their technical capabilities and human resources experiences, security threats are evolving with the development of time and technology, collaboration at all levels of the organization may bring a safe and secure environment for information security, the more information security maturity in the organization the lower the final cost of security and vice versa.

Through an analysis of local studies, the absence of studies on the application of information security practices in banks in the Yemeni environment is evident. Although the foreign or regional studies that dealt with these practices in foreign banks, they remain studies of a different environment from the practical reality in Yemen, especially. So, we seek through this study to reduce this research gap.

B. The SPO evaluation criteria

Processes and procedures evaluation category is used to identify the extent of standardization of the Organization's operations. International policies and standards provide specific guidelines that must be followed to ensure information security. In keeping with the information security requirements imposed by international standards, two security sub-fields must be included as a measurement indicator for evaluating the organizations' performance on this factor. The access management sub-domain is the first, while the other sub-domain is the compliance. In short, we'll code them by 'AM' and 'COM', respectively.

Many researchers, such as [16, 17], argue that access control's primary goal is to prevent unauthorized access to institutional information assets. This goal can be achieved by assessing the organization's competence to dominate unauthorized access to the informational content within the organization's IT infrastructure. The importance of the access management sub-factor stems from the legal consequences, moral losses incurred, and the commercial damages that affect the continuity of business due to the infringement of institutions' privacy. The other side of the evaluation framework aims to verify the extent to which institutional systems can meet the specific requirements imposed by institutional policies and legal and regulatory standards. The level of compliance must be verified to ensure the extent to which the relevant operational controls and procedures comply with the requirements as mentioned above. According to [10], the main AM criteria are (1) Access control policy;(2) Review of user access rights; (3) Password use; (4) Removal of access rights; (5) Authorization process for information processing facilities; (6) Disciplinary process; (7) Security requirements analysis and specification; (8) Event reporting; (9) Controls against malicious code; (10) Teleworking, Audit logging; (11) Security requirements analysis and specification, and project management. The primary compliance criteria are (1) Identification of applicable legislation; (2) Technical compliance checking; (3) compliance with security policies and standards; (4) Control of technical vulnerabilities; (5) Risk response.

C. The SPO evaluation controls

There are popular international IS standards obtainable. It over systematic management approach to implement the preeminent practice IS controls, measure the acceptable risk level and implement the suitable measures which guard the privacy, reliability, and accessibility of data, The COBIT, ITIL, ISO 27001/2005, and the ISO 27001/2013 are some of them. For each SPO criteria (sec. 2.B), tables 1, 2 illustrate a mapped set of controls and requirements (COBIT, ITIL, ISO) to establish, implement, operate, monitor, review, maintain and improve an SPO information security domain as a part of the overall IS management system.

Table 1. The Main AM Security Controls

C	Cobit 4.1	ITIL v3	ISO 2005	ISO 2013
1	PO2.2,PO6 2	SD 4.6.4, SD 4.6.5.1	11.1.1	9.1.1
2	DS5.4	SO 4.5	11.2.4	9.2.5
3	PO6.2,DSS4		11.3.1	9.3.1
4	PO7.8,DSS4	SD 4.5	8.33	9.2.6
5	PO4.3, PO4.3, PO 4.9, AI1.4	SS 6.1, SO 3.2.4, SO 4.4.5.11, SO 5.4	6.1.4	
6	PO4.8, O7.8, DS5.6	SD 6.4	8.2.3	7.2.3
7	AI1.1	SD3-3, 3-4, 3-5, 3-6	10.1.1	12.1.1
8	PO9.3	SS 9.5, SD 4.1.5., ST 9, SD 4.5	13.1	16.1.2
9	DS5.9		10.4.1	12.2.1
10	PO3.4,AI2.3	SD 4.6.5.1, SO 5.4	11.7.2 10.10.1	6.2.2 12.4.1
11	AI1.2 ;Ai 2.4, P010	SD 2.4.2, 3.6, 4.5.5.2	12.1.1	14.1.1

Table 2. The Main COM Security Controls

C	Cobit 4.1	ITIL v3	ISO 2005	ISO 2013
1	PO4.8	SD 6.4	15.1.1	18.1.1
2	DS5.5	SO 4.5.5.6, SO 5.13	15.2.2	18.2.3
3	PO4.8	SD 6.4	15.2.1	18.2.2
4	AI3.3	**SO 5.4** – 5-11	12.6.1	16.6.1
5	PO9.5; DS4.3	SS 9.5, SD 4.5.5.3, ST 4.6;	13.1.2	16.1

C. The SPO maturity model and assessment framework

To measure an organization's information security performance, the information security maturity model (ISMM) should be used. Many definitions of the term "maturity model" are reported in the existing scientific

literature. Researchers in [18] recalled that any systematic framework used to implement benchmarking and strengthen performance could be deemed a Maturity Model [19]. Another researcher stated that the maturity model could be defined as a methodological framework to estimate and enhance operations in an evolutional paradigm [20]. It also was explained as a range of precisely defined activities that describe the characteristics of effective methods [21].

Many ISMMs exist; some of them are Citigroup's Information Security maturity model (CITI-ISEM); NIST Cybersecurity framework (NIST-CSF), ITIL maturity model, Cobit CMMI, System security engineering CMM, CERT/CSO, CERT/RMM, Saleh's ISMM [20], ISMM for secure e-government services [22], and the Nnatubemugo's ISMM[10]. In this study, we decided to use the Nnatubemugo's ISMM, proposed by [10] for many reasons: The Information security assessment framework (ISAF) of this model is based on the ISO/IEC 27001/27002. This standard is distinguished from other interpretations: this is a good standard for application in different organizations regardless of size and explains the system as a comprehensive and integrated business risk management approach; It provides a customized version of ISAF that covers all relevant security requirements specified in the ISO security standard; The measurement tool is designed based on both qualitative and quantitative measures. This future makes it more helpful to get more accurate results; It determines the performance degree that an organization should be reached to achieve each fixed maturity level at each given security subdomain. Fig 1. Illustrate Nnatubemugo's ISMM.

An appropriate ISAF should be used for assessing the maturity level; author Nnatubemugo provides a mixed qualitative and quantitative measurement framework. This framework covers the questionnaire block and measurement scale. The questionnaire block contains 16 questions, classified into two subgroups (AM and COM). These criteria and indicators will be selected to measure the related ISML in this paper. Fig.2 and Fig 3 illustrate these criteria and indicators -Statements(S)).

SA	ML	Description
AM	1.Vulnerable	No policy/procedures in place for coordinating and protecting information within the organization and while in transit on the networks.
	2. Security Awareness	An access control policy is in place, but implementation across various essential information facilities is still minimal and uncoordinated.
	3.Basic Security	Access control mechanisms for users, networks, applications. are in place with little efforts to track its efficacy and correct shortfalls
	4.Meeting Requirement	Standard ways of managing access to information in various forms are practiced. The mobile computing (BYOD) policy is well defined and followed. Performance is measured
	5: Robust Security	Active control of information access is practiced—regular review of access control policy to match evolving threats. Dynamic management of information assets to ensure security.
COM	1.Vulnerable	Operations are entirely noncompliant for legal, technical, and security regulations and standards
	2. Security Awareness	The compliance regime shows a desire to comply. Constant review/audit of information systems is yet not practicable
	3.Basic Security	Regular reviews by internal audits and actions followed to achieve compliance
	4.Meeting Requirement	Both internal and external auditors ensure full compliance to security policies, standards, and legal requirements
	5: Robust Security	The external audit shows that best practices are consistently followed, resulting in no critical compliance issues.

Fig 1. The Maturity Values and Their Description (Source: [8])

SA	ID	Statement and their maturity levels
AM	1	Is there an access control policy in place for managing user access? L1- No access control policy exists; . L2- Staff with administrative privileges control access at will.; L3- Formal access control policy is documented. L4- Access control policy covers all requirements related to information access control; L5- Constant review and documentation of access control policy to reflect changing business and security requirements.
	2	How regularly are the granted rights/privilege reviewed and updated? L1- Not reviewed at all. ;L2- Annually; L3-6-months interval;L4- Quarterly.;L5- Monthly.
	3	How often are staff prompted for the password change to allow access to the operating system and other applications? L1- Users are not required to do this. L2- Password management/change is at the discretion of the user.;L3- Security mechanisms to prompt the user for password change every six months. L4- Policy and security mechanisms insist that user passwords be changed monthly; L5- Change of password in accordance to access control policy and active identification and blocking of password/user account misuse.
	4	What is the period of inactivity before a user's account deactivated? L1-Never deactivated.;L2-1 year; L3-months.; L4-3months; L5-1month.
	5	Is there a Bring Your Own Device (BYOD) policy in place? Are there proper arrangements for mobile computing/teleworking? L1-Policy and provisions for the use of mobile devices do not exist. ; L2- Individual efforts to ensure security exist without formal BYOD policy. ;L3- Detailed requirements for staff use of personal devices are not fully specified in Policy. ; L4- Detailed policy that specifies how mobile devices should access sensitive information within and outside the organization is in place. ;L5-There is a policy, and it is continuously reviewed to meet renewed security requirements and challenges.
	6	Is there punishment for staff violation of the security policy? L1- Staff security breaches go unnoticed. ;L2- Breaches are noted without penalty.;L3- Staff is punished when there are tangible losses. ;L4- Appropriate mechanisms exist for tracking, identifying, and disciplining staff security misconduct. ;L5- Staff breach of security is punished and documented for future reference.
	7	Are there standard operating procedures across all departments which support information security? L 1-No defined operating procedures in place. ;L2- Understanding of the need for operating procedure exist but not implemented.;L3- Operating procedure exists, but not strictly practiced. ;L4- Operating procedure details the proper use of all information processing facilities;and users' responsibilities. L5- Operating procedure is continuously reviewed for efficacy.
	8	Is there a formal management procedure for information security incidents? L1-Does not exist. ;L2- Report of the incident is uncoordinated and does not follow specific procedures.L3- Procedures exist though not strictly followed, thus ineffective in ensuring a timely response;L4- Well defined procedures for reporting and responding to security incidents exist. ;L5-Standard procedures are strictly followed and continuously improved on to improve security. Proactive measures are in place to prevent past documented incidents
	9	How often are computer systems checked/scanned for malicious applications/activities? L1-Not is done as far as there is no issue. ;L2- Quarterly or only when a problem arises.;L3- Monthly.;L4- Daily. ;L5- Active/real-time monitoring of system activities to identify and resolve Malware.
	10	How often are the firewall and IDS logs monitored and acted? L1-No such operation. ;L2- Annually.;L3- Monthly. ; L4- Weekly. ;L5- Daily.
	11	At what stage in a project life cycle is security considered or introduced? L1-Not considered at all. ; L2- As the need arises.;L3- Implementation.;L4- Design stage.;L5- Inception /conception.

Fig.2. The SPO evaluation criteria and statements – AM field [10]

SA	ID	Statement and their maturity levels
COM	1	How compliant are the operations of the organization to policy, regulatory and legal requirements? L1- Several breaches are recorded often.;L2- Compliance is still reactive and not consistent in all aspects.;L3- Technical compliance is assured with legal and regulatory compliance not adequately enforced.; L4- Full compliance with legal, regulatory, technical, and other security requirements is practiced.;L5- Compliance with legal, regulatory, and security requirements is continually checked and reviewed as necessary.
	2	How regular is the information system audit for compliance conducted? Our penetration testing and vulnerability assessments done? L1-Never is done. ; L2- Individual staff efforts to troubleshoot and correct errors and system vulnerabilities.; L3- System audit is only carried out by internal auditors.; L4- Penetration testing and vulnerability scanning are carried out every six months by external experts. System audit by internal officers is also done regularly.; L5- Penetration testing and vulnerability scanning are periodically done.
	3	How often are cases of staff misuse of access rights/privileges? Are users obliging to their user responsibilities? 1-Several daily cases of a user violation of security policy due to ignorance. ;L2- Users understand their security responsibilities but do not actively abide by it.; L3- Few cases of the breach in a month due to conscious efforts to fulfill security Responsibilities. ;L4- Users understand their security responsibilities and are actively abiding by it.;L5- Access control is useful, and cases of misuse and information compromise are rare ; due to users' proactive compliance with their security responsibilities.
	4	What is the rate of security incidents and breaches in the past year? L1-A year interval or more. ; L2- Incidents are resolved within one month of Occurrence.;L3- Incidents do not exceed one week before resolution.; L4- Incidents are promptly handled within one to five days interval.;L5- It takes no more than a day to resolve incidents.
	5	What is the time between the security incident and its resolution (response rate)? L1-Several breaches. ; L2-20-100 incidents. ;L3-10-20 incidents.;L4-1-5 incidents.;L5- No incident.

Fig.3 The SPO evaluation criteria and statements – COM field [10]

For each question, the measurement scale provides a five-point scale (maturity levels) and the weight of each corresponding maturity level (1-5), which describes the degree of performance, and the qualitative or quantitative evidence for each maturity level. Besides, to determine the overall ML, the maturity level values should be scored. Fig.4 illustrates the boundary scores related to the overall maturity levels and their descriptions.

Score Boundary	ML	Description
0 - 1.5	1.Vulnerable	Complete ignorance of information security criticality
1.51 - 2.5	2. Awareness	Awareness of criticality of information security with little efforts
2.51. - 3.5	3.Basic Security	Basic compliance to information security requirements
3.51. - 4.5	4. Meeting Req.	Full compliance with standard information security requirements
Above 4.5	5: Robust S.	Innovative ways of ensuring information

Fig.4. Assessment Criteria, Source: [10)

III. METHODOLOGY AND MATERIALS

This study relies on two approaches, descriptive and analytical, to analyze the existing SPO in the YBS. It also has applied the case study method, through which relevant data has been collected. The following sequence problem-solving steps structure of techniques is used:

A. *Define the problem, objectives, and questions of research (Section 1).*
B. *Literature review (Section 2);*
C. *Selection the maturity and assessment model (Section 2)*
D. *Design of the searching tools used for data collection;*
E. *Testing the collected data;*
F. *Data analysis; and*
G. *Finding and recommendation's.*

The total number of banks that their central branch located in Sana'a is 16 and the study community comprises all 16 banks except for three of them. The excepted banks have refused to cooperate under the pretext that information security is a sensitive and dangerous subject, and everything about IS should be disclosed no matter how significant the situation. This work was conducted from April to December 2019. The study is limited to achieve the previously defined goal on the YBS in Sana'a. It relies on ISO 27001:2003 international information security standard requirements and applying Nnatubemugo's ISMM and ISAF. The names of the sample banks will be coded with numbers 1 to 13 as follows: 1- The Yemen Bank For Reconstruction And Development; 2- The National Bank Of Yemen; 4-Housing Credit Bank 4- International Yemen Bank; 5- Yemen Kuwait Bank;6- Cooperative & Agricultural Credit Bank;7- Rafidain Bank;8-Yemen Commercial Bank;9- Islamic Bank Of Yemen;10-Tadhamon Bank;11- Saba Islamic Bank; 12- Shamil Bank Of Yemen & Bahrain; and 13- Qatar National Bank.

To collect data, the selected ISMM and ISAF were translated into the Arabic language; after that, the research survey tool was designed and tested. For this purpose, the survey tool was developed in its original form; it was tested; it was presented to a group of arbitrators from 15 academics and bank information security experts. This version was modified based on the arbitrators' views and observations through the addition, modification, and reordering statements [table 3]. Thus, the finalized version was developed and covered two parts. The first one was included the demographic data of the two research workers (gender, scientific qualifications, specialization, job position, years of experience).

In contrast, the second part was included (16) statements, which were grouped into two security areas. After that, questionnaires were distributed to workers responsible for information security in all 13 banks; all responses were accepted and tested. The Cronbach's Alpha has been used to measure the stability of resolution to measure stability and internal consistency. An excellent reliability coefficient (alpha) of 0.87 and an outstanding validity percentage of 93% was reported using the SPSS package.

IV. RESULTS AND DISCUSSION

A. *Results*

The evaluation questionnaire of 13 participating banks using the proposed ISAF is described in this section. For each participant in each investigated bank, the evaluation points on each security statement (indicator) were collected. After which, these values were averaged. After that, the average value of maturity level values on both AM and COM sub-domains and on the SPO main domain is calculated and averaged for each bank, as presented in Table 3. Based on these values, the ranking orders of banks, illustrated in table 4, were achieved.

Table 3. Average Values Of Maturity Level

Security area	Bank Number													AML
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	
AM	4.64	3.82	2.45	4.33	3.27	3.21	2.09	3.61	3.48	4.50	4.00	3.45	4.24	3.62
COM	4.40	3.60	3.00	4.60	2.50	3.27	2.80	3.80	4.20	4.60	4.20	3.30	3.93	3.71
AVG	4.52	4.11	3.43	4.37	3.84	3.81	3.25	4.00	3.94	4.45	4.20	3.93	4.32	4.01

Table 4. Ranking Order of Banks

Security area	Bank Number												
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
AM	1	6	12	3	10	11	13	7	8	2	5	9	4
COM	3	8	11	1	13	10	12	7	4	1	4	9	6
SPO	1	6	12	3	10	11	13	7	8	2	5	9	4

The average values of maturity level values for each security statement (requirement) for a whole banking sector under both AM and COM areas were calculated, as shown in table 5. This table also represents the ranking order (R) of them, the related compliance maturity level (CL), as well as Statistical testing results: relative importance (RI) and standard deviation (SD). The average values (AML) of these averaged values on both AM and COM subdomains and the main standardization security domain SPO. The R, RI, SD, level number (L-id), and CL values are presented in table 7. This table also represents the overall gaps between the actual ML of application of security requirements and the robust level seek by the YBS on both AM and COM subdomains and the main standardization security domain (SPO).

Table 5. The Average Values of ML-Values on Each Statement

SA		Statement number											AML
		1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	
AM	ML	4.2	2.7	3.8	3.7	4.1	4	3.7	2.8	3.5	3.8	3.5	3.62
	R	1	11	4	6	2	3	6	10	8	4	8	
	SD	0.90	0.97	0.97	0.97	0.97	0.97	0.97	1.41	1.41	1.41	1.41	
	RI %	84	84	84	84	84	84	84	56	56	56	56	
	CL	BS	BS	MR	MR	MR	MR	MR	BS	BS	MR	BS	
COM	ML	3.6	3.3	3.4	3.9	4.3							3.71
	R	3	5	4	2	1							
	SD	1.13	1.13	1.13	1.13	1.13							
	RI %	72	72	72	72	72							
	CL	MR	BS	BS	MR	MR							

Table 6. The Overall Results

Security area	AML	L-Id	CL	RI%	SD	Gap	R
Access management	3.62	4	MR	72	0.76	1.38	2
Compliance	3.71	4	MR	74	0.69	1.30	1
SPO	3.66	4	MR	73	0.69	1.34	

B. Discussion of results

Q1- What is the actual ML of the SPO in the YBS?

1) Table 4 represents that the 3d and seventh banks are on level three maturity. They are just fulfilling the SOP basics, while participants number 2,4-6,8-12 and 13 exhibit level four maturity; this implies meeting the SPO security requirements. However, only the first bank measured up to level five maturity. It meets the robust security level requirements, telling the adaption of innovative ways of ensuring its information.

2) Participants number 5,6,9, and 12 are on level three maturity on the access management subdomain, while the 2nd, 4th, 8th,10th, 11th, and 13th banks exhibit the 4th maturity level. This situation implies that the last six participants meet the access management requirements, while the former four banks are only covering the fundamental aspects of this area. However, only two (7 and 3) of these participants were measured down to level two, and one of them (b1) measured up to level Five.

3) Banks with an id number of (3,6,7) and 12 are on level three (3) maturity on the compliance subdomain; participants (1,2,4,8,9,11) and 13 offer level four (4) IS maturity on it. This result means that the last seven banks meet the compliance information security needs, while the former four banks are only accomplishing the fundamentals within this area. However, only one bank (5) of these participants was measured down to level two, and two of them (4 and 10) measured up to level five.

4) The ISMS of the YBD is on level four maturity and meeting the security requirements of access management and compliance subdomains and standardization of the information security operations domain. Its overall MI is 3.62, 3.71, and 3.66, respectively.

Q2- What are the gap between the actual ML of the SPO in the YBS and the maximum recommended ML?

Tables 5 and 6 indicate that: (1) The obtained maturity values distribute on two levels; these are the necessary security and meet requirement levels; a ratio of the total number of banks meeting the requirements of these levels on both access management and compliance subdomains are 4:7 and 2:3, respectively. (2) An overall average ML value is 3.66; this value means (according to [10]) that standard means of controlling access to information in different variants are implemented. (3) The overall gap values of the ISMS of the YBS under the access management and compliance subdomains and the standardization of the information security operations domain are equal to 1.38,1.30 and 1.34, respectively.

Q3- What are the significant points of strengths?

- The proportion of banks in which the information security policies cover all access control requirements is 84.7 %. In approximately half (45.5%) of them, these policies are documented and reviewed to keep pace with changes. The mean average of maturity level values under this security requirement equals 4.2. Therefore, this security practice has topped the practices of access management subdomain.

- The security practice that measured the rate of security breach incidents in the past year has rated first for all compliance subdomain security practices. It also has topped the list of all standardization practices of the information security operations. The mean average of maturity level

values under this security requirement equals 4.3. The main reason for this situation is that more than two-thirds (69 %) of banks under question are not exposed to such incidents during the last year. This result also demonstrates the strength of users' compliance in those banks.

Q4- What are the major weakness and vulnerable points in the YB sector's information systems?

1) The confirmation compliance of information systems to security and regularly penetration testing and vulnerability scanning highlighted the weakness of compliance practices in these banks; the results show that only 15% of these banks were committed to applying these practices, while 38 %of them carried it out every six months.

2) Reviewing and updating the permissions granted for users at far intervals in these banks highlighted the weakness of access control practices; the results show that only 15% of these banks are committed to applying this practice monthly, and 69 %of them used it quarterly.

3) Another weak point in this area is that IS events management's formal procedures were never what they should be. This pint can be interpreted by the too weak proportion of banks that follow strictly standard procedures for this purpose (7.7%), comparing to those where these procedures are never available (23 %), at the ratio of 1:3, or comparing to those where these procedures are available, but uncoordinated. No specific actions can be taken (38.5 %), at a ratio of 1:5.

Table 7 illustrates the matches between these main weaknesses and the banks that are suffering from them. Table 8 shows the mapping between these main weaknesses and the banks that are suffering from them.

Table 7. The Main SPO's Weaknesses of Banks

	Weakness points for each statement	**Bank**
AM (2)	A) Time intervals to review the access rights of users are long: > 6 months B) Time intervals to review the access rights of users are long: intervals > 3 months.	3-7,8,10, and 13 1, 2, and 12
AM (8)	The formal IS management procedure associated with the IS incident is: A) not available, not arranged and not robustly followed; B) not arranged and not robustly followed; C) not robustly followed;	 3,5, and 11 6,7,8, and 12; 2
CO M(1)	A) The permeation screening and vulnerability appraisal for compliance are not conducted B) singular worker efforts are present C) exist but not at the orderly precept.	3; 5,6, and 7 8. and 12

Q5. How to rate the institutions in this sector according to their information security maturity level?

Based on tables 5 and 6: (1) The sequencing order of security practices according to theirs average rate of implementations by the banking sector on both AM and COM security sub domains are (1> 5> 6> 3> 10> 4> 7> 11> 9> 8> 2) and (5> 4>1>3>2) respectively. (2) Rating the YBS institutions, according to their security compliance, is presented in table 5.

C. Recommendations

Q6. What are the most appropriate solutions and recommendations to improve the security situation in this sector?

Solutions that can be recommended for improving the information security situation in a whole system are presented in this section. Based on ISO 27002 security standard, the following recommendations are suggested (tables 8 and 9); the total number of submissions is 16, each recommendation links to one information security requirement that have the same ID number in the questionnaire. Each guidance addresses a set number of banks (B), which have related weaknesses or vulnerabilities in implementing these requirements. Each proposal has the same ID number of additional implementation guidance, which are suggested based on ISO 27002 -2005 and ISO 27002 -2013 (tables 10 and 11). The implementation matrix to match vulnerable points on sub security domains for each bank (B), the linked-to those recommendations, and additional implementation guidance are summarized in table 12.

Table 8. Recommendations to Enhance the AM Security Practices

Q_ID	**Recommendation**
1	Establishment of a security policy for controlling access based on business and security requirements in these banks; this policy must be documented and reviewed continuously
2	Providing and implementing a formal process that helps manage the regular review of rights access to users
3	Build security policies imposed on users to follow its proper security practices for use and selection of passwords.
4	Build security policies imposed on users to follow its proper security practices for use and selection of passwords.
5	Developing an appropriate definition and implementation requirements of the process of authorization for new facilities and preprocessing types of equipment
6	Include the requirements for removing access rights to all information assets and processing systems and storage for all employers, contractors, and third-party users in the event of ending their jobs or change them in cases of adjustment
7	Identify management responsibilities as well as procedures and enforcing techniques associated with the information processing facilities management and operation.

8	Official event reporting requirements and implementation procedures, awareness programs, including business impact and regulations aspects, should be in place.
9	Development and implementation of detection, preventing, and recovery controls to protect institutions from malicious codes and suitable awareness program actions for the user.
10	Develop and implement a teleworking activities policy, operational plans, and procedures. Additional related monitoring, recording, logging activities should be adapted.
11	Information security should be guided in project management, regardless of the type of project. The requirements related to information systems must be defined during the phase of projects' requrirments.

Table 9. Recommendations to Enhance the COM Security Practices

Q-ID	Recommendation
1	Define, document and keep up to date the contractual, legal and organizational requirements.
2	Regularly checking the Information systems of banks for compliance with implementation standards of IS.
3	Managers should ensure that the relevant to their responsibilities procedures are implemented accurately to get compliance.
4	Suitable and in regular time actions must be carried out to overcome the potential technical risks
5	The formal event reporting procedures should be existed. All concerned users should recognize and understand the necessary steps to report them.

Table 10. Implementation Guidance: AM Security Area.

	AM (Q-ID)										
ISO ver	1	2	3	4	5	6	7	8	9	10	11
2005v	11.1.1	11.2.4	11.3.1	8.3.3	6.1.4	8.2.3	10.1.1	13.1	10.4.1	11.7.2,10.10.1	12.1.1
2013 v	9.1.1	9.2.5	9.3.1	9.2.6		7.2.3	12.1.1	16.1.2	12.2.1	6.2.2,12.4.1	14.1.1

Table 11. Implementation Guidance: COM Security Area

	Q-ID				
ISO-vers.	*1*	*2*	*3*	*4*	*5*
2005v	15.1.1	15.2.2	15.2.1	12.6.1	13.1
2013 v	18.1.1	18.2.3	18.2.2	16.6.1	16.1

Table 12. The Finally Implementation Matrix

	Recommendation number according to table 8, IG number according to table 10											**Recommendation number (table 9), IG number (table 11)**				
B	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*1*	*2*	*3*	*4*	*5*
1	■	■														
2	■	■	■	■				■				■		■		
3	■	■	■	■				■	■	■	■		■	■		
4		■		■												
5		■				■	■				■	■	■	■	■	■
6		■					■	■			■	■	■	■		
7	■	■	■	■	■		■	■	■	■	■		■	■		■
8	■	■			■	■		■	■				■			
9	■		■			■			■	■						
10		■									■					
11								■		■				■		
12		■			■		■	■	■	■		■	■		■	
13		■														

V. CONCLUSION

This paper contributes to measuring information security maturity; a case study to evaluate the PSO in the Yemen banking sector has been studied and analysed. The result shows that the actual maturity level of these practices in Yemen's banking sector is 3.66. Moreover, the Information systems of this sector are meeting the related security requirements. The gap between the maturity level of the actual application of information security practices and the robust level equals 1.34.

There is a set of strengths in favor of banks about applying the SPO - information security practices represented in the adoption of a policy to control access in banks, including all access control requirements, the low rate of incidents of security breaches in the past year in banks. There is a set of weaknesses in banks regarding the application of these practices, such as failure to assess weaknesses in the information system, weakness in the implementation of penetration testing procedures, failure to review compliance periodically, failure to review and update users' powers regularly and continuously, in addition to weaknesses in the management of IS Events, and the lack of adequate procedures for that.

The security position (location or order) of each bank is determined. The bank with the best practices is bank the

first bank, while the fourth bank has the weakest SPO practices. Banks should adhere to implement some improvement actions to improve their situation and competitiveness. For this, sixteen improvement actions and recommendations have been suggested to improve this sector's information security operations' standardization practices. Each bank should select the related list of suggestions based on the implementation matrix mapping table, which is also proposed by this study. Additional ISO-based implementation guidance for each bank has been recommended. Hence, the study's objective was carried out successfully; the previously mentioned questions were answered. This paper and its results will help the YBS sector to enhance its information security practices by establishing and implementing these recommendations. Additional works should be done to meet objectives under other security domains and improve security performance and compliance in this sector.

REFERENCES

[1] IBM Security, "IBM X-Force Threat Intelligence Index ", **2020**.

[2] SF. Alomgeer, "*Cyber Crime In Banking Sector of Bangladesh*, ", diss., East West University, **2019.**

[3] S. Kesharwani, M. P. Sarkar, & S. Oberoi, "Growing Threat of Cyber Crime in Indian Banking Sector.", *CYBERNOMICS*, Vol **1**, No **4**, pp **19-22**,**2019**.

[4] N. Tariq, "Impact of cyber-attacks on financial Institutions," *Journal of Internet Banking and Commerce*, Vol. **23**, No **2**. pp. **1-11, 2018**.

[5] A. R. Raghavan, & L. Parthiban, "The effect of cybercrime on a Bank's finances," *International Journal of Current Research & Academic Review*, Vol. **2**, No 2. pp. **173-178, 2014**.

[6] N. Alber, N., & M. Nabil, "The Impact of Information Security on Banks' Performance in Egypt," Available at SSRN 2752070

[7] Sanskriti Choubey , Astitwa Bhargava , "Significance of ISO/IEC 27001 in the Implementation of Governance, Risk and Compliance," *International Journal of Scientific Research in Network Security and Communication*, Vol.**6**, Issue.**2**, pp **30-33, 2018**

[8] Hailye Tekleselase Woldemichael, "Emerging Cyber Security Threats in Organization," *International Journal of Scientific Research in Network Security and Communication*, Vol.**7**, Issue.**6**, pp **7-10, 2019**

[9] M.A.M Stambul, R. Razali, "An assessment model of information security implementation levels.," *In the Proceedings of the 2011 Electrical Engineering and Informatics* (*ICEEI)*, **IEEE**, pp **1-6**,**2011**

[10] Nnatubemugo Innocent Ngwum, " Information Security Maturity Model (ISMM). ," Diss., The University of Manchester., **2013**.

[11] W. M. Zeiad, "The impact of information security risks on the accounting systems in the Central Bank of Yemen." Master Thesis. The Yemeni Academy for Graduate Studies, Sana'a, Yemen, **2019**. [In Arabic]

[12] M. J. Hammodah, " Evaluating information security strategies in banking institutions," Master Thesis. Michigan State University-Dubai Branch, UAE**,2017**. [In Arabic]

[13] Nada Ismaeil , "Protecting the security of information systems, a case study in Al-Rafidain Bank," *Tikrit Journal of Administrative and Economic Sciences.* Vol.7 , Issue 21, pp 72—94, 2011. [In Arabic]

[14] A. L. Muhsen, "Information Security Management In Palestinian Banking," Master Thesis. An-Najah National University. Nablus. **Palestine**," **2014**

[15] İ. A. Gürcan, "Assessing Information Security Management Requirements For Finance Sector Using An ISO27001 Based Approach," Master Thesis. Bahcesehir University. Istanbul. **The Republic Of Turkey**, **2014**

[16] D. Lang & D. Van der Haar, "Recommendations for Biometric Access Control System Deployment in a Vehicle Context in South Africa. ," *In Information Science and Applications*, **Springe**r, **Singapore**., pp**. 305-317, 2020**

[17] N. Agrawal, & S. Tapaswi, "A trustworthy agent-based encrypted access control method for mobile cloud computing environment," *Pervasive and Mobile Computing*, Vol. **52**, pp **13-28.,2019**

[18] Al-Mayahi, Ibrahim, and P. Mansoor Sa'ad. "ISO 27001 gap analysis-case study," *Proceedings of the 2012 International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), **2012**.

[19] A. A Nasser, A. A. Al-Khulaidi, & M. N. Aljober, " Measuring the information security maturity of enterprises under uncertainty using fuzzy AHP," *Int. J. Inf. Technol. Comput. Sci.(IJITCS)*, Vol. **10**, No **4**, pp **10-25**, **2018**

[20] M. F. Saleh,, "Information security maturity model ," *International Journal of Computer Science and Security (IJCSS)*, Vol.**5,** No **3: 21,2011**

[21] Team, CMMI Product. "Capability maturity model® integration (CMMI SM), version 1.1." *CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, V1. 1)* , No **2,2002**

[22] G. Karokola, S. Kowalski, & L. Yngström, Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. *In HAISA*, pp **58-73, 2011**

AUTHORS PROFILE

Mr. Adel A. Nasser pursued a Bachelor of Science (Information technology and computer engineering) from South-West State University in 2007. He also pursued a Master of Science (Devices and Systems of wireless communication networks) in 2009 and a Ph.D. of Technical Sciences in the year 2012. He is currently working as Associate Professor and Head of Information Systems and Computer Sciences Department, Sa'ada University, Yemen. He is a member of the International Association of Engineers (IAENG) and in many academic commissions of Sa'adah and Dar Al-Islam universities, Yemen. He has published more than 40 research papers (In both English and Russian languages) in reputed international journals, including (Thomson Reuters (Web of Science), the Russian Higher Attestation Commission (Росская ВАК), Russian SCI, and International conferences; It's available online (on research gate and E-library Russian scientific research database). He participated in several local workshops to develop several graduate and undergraduate programs. His main research work focuses on information security, information security management, decision support systems, MCDM methods and algorithms, fuzzy-based MCDM tools, and their application in health, education, and business. He has eight years of teaching and research experience.

Ms. Nada Kh. Al-Ansi obtained a BA in Management Information Systems from Dar Al-Salam International University and Yemen in 2014. in 2020, She received a Master's degree in Management Information Systems from the Yemeni Academy for Graduate Studies, Yemen. She is currently working as a lecturer at Al-Hikma University, Yemen.

Mr. Naif A. Al-Sharabi pursued a Bachelor of Science from Technology University – Iraq in 1997. He also pursued a Master of Science in 2005 and a Ph.D. of Sciences in the year 2008 from the Hunan University - China. He is currently working as Associate Professor at Amran University, Yemen. He has published more than 20 research papers in reputed international journals, including (Thomson Reuters (Web of Science)) and International conferences, including IEEE; It's available online. He participated in several local workshops to develop several graduate and undergraduate programs. His main research work focuses on Wireless Network, WiMax, LTE, Cellire Network, and Cellular communication. He has 12 years of teaching and research experience

