The Seybold Report

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

INFORMATION SECURITY GAP ANALYSIS: AN APPLIED STUDY ON THE YEMENI BANKING SECTOR'S TECHNOLOGY AND INNOVATION PRACTICES

ABDUALMAJED A. G. AL-KHULAIDI[1], ADEL A. NASSER[2, 3*], NADA K. AL-ANESI[3], MONEER A. S. HAZAA[4], MIJAHED ALJOBER[3] and NESMAH A. AL-KHULAIDI[5]

[1] Department of Computer Science, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen
[2] Department of Information Systems and Computer Science, Faculty of Sciences, Sa'adah University, Sa'adah, Yemen
[3] Modern Specialized College of Medical and Technical Sciences, Sana'a, Yemen
[4]Faculty of Computer and Information Systems, Thamar University, Thamar, Yemen
[5]Yemen Academy for Graduate Studies, Sana'a, Yemen
*Corresponding author: Adel A. Nasser (e-mail: adel@saada-uni.edu.ye)

Abstract:

This study aims to analyze the level of compliance of Yemeni banks' information security management systems (ISMSs) with technology and innovation controls, identify strengths and weaknesses in their practices, and provide appropriate solutions and treatments to reduce the gap. To this end, drawing on the analysis of previous studies, the problem of the study was determined, its dimensions were explained, and the appropriate assessment framework and maturity model were selected. A questionnaire was used to collect information from 26 carefully selected experts to assess the maturity level of 13 local banks in the Yemeni capital, Sana'a. Through data analysis, it was found that the level of security maturity in the banking sector meets only the key requirements of technology and innovation security, moving away from the ideal maturity level by a gap of 1.1 out of five. In addition, detailed results on maturity levels, weaknesses, and average applied gaps in TI practices were obtained. By interpreting the findings, a classification and ranking of indicators that represent the most likely technological weaknesses for banks and the average level of security gaps that must be reduced by each of them were determined. Finally, the classification and ranking presentations and proposals enable banks to compare their security status with each other, and to build appropriate strategies to bridge the gap and improve their competitive position. Accordingly, the classification and ranking presentations made by this study will enable banks to compare their security situations and take appropriate actions, policies, and technical solutions to bridge the gap and improve their competitive position.

Keywords Banking Sector, Gap Analysis, Information Security Assessment, Maturity Index, Maturity Level, Maturity Model, Technology and Innovation, Yemen

I. INTRODUCTION

The current era is witnessing great development and a qualitative leap in business technology and systems, and the success of enterprises' businesses, including those operating in the banking sector, has become heavily dependent on the volume of information held by these enterprises and on their ability to use modern digital technology in the preservation, addressing, and utilization of information in a manner that contributes to improving and increasing the quality and quantity

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

of their business, marketing, and productivity decisions [1] and on their ability to optimize the use of such technology in addressing the huge volume of electronic transactions imposed by the sector's modern and traditional working environments [2].

However, given the importance of information assets, systems, and technology in financial sector institutions to achieve competitive advantage, business continuity, and other strategic objectives [3], [4], the importance of trade information and data in this sector [5], [6], and the economic, commercial, and service advantages and benefits offered by modern technologies [7], banking institutions have found themselves in a realistic position to innovate.

On the other hand, technology's negative impacts are also increasing. The number of people engaging in threatening online behavior is constantly increasing [7], particularly those related to identity theft, phishing, and exploitation of weaknesses in banking enterprise systems and technology [8]. According to the report (X-Force, 2022) [9], the banking sector is the most vulnerable industry to cyberattacks and has retained its first position in the list of sectors most exposed to these threats throughout 2015–2020.

In any case, there are multiple motives behind targeting banks and the methods of criminals in hacking. Previous studies have indicated that the main motive for cybercriminals, including hackers, identity thieves, and blackmailers, is to seek illegal profit [7], [8]. By exploiting the fact that financial information and operations are very sensitive and critical in sustaining banks' business and in achieving their economic, strategic, and marketing objectives, and their confidentiality, integrity, and availability cannot be impaired under any circumstance, at any cost. To achieve this, criminals use many methods of attack, notably phishing and fraud, and penetrating systems by exploiting weaknesses in organizations' systems and technologies [10], [11].

According to IBM's previously mentioned report (X-Force) [9], weaknesses in enterprise information systems and technologies caused approximately one third of the cyber threats faced by enterprises worldwide in 2021 (0.34%); However, for several reasons, these threats have become a major security concern for the global financial industry around the world. Most notably, information systems, regardless of their sophistication, cannot be fully reliable or guaranteed and remain vulnerable to penetration as a distinctive target for many cybercrime activities, and the continued exposure of banking institutions to cybercrime contributes significantly to many strategic, operational, moral, legal, and economic losses [8], [12]. Most of these losses result from their contribution to the disruption of financial services essential to financial regulations and, to the undermining of the institutions' security and customer confidence in their services, which endangers financial stability and affects stakeholders' choices [7] and their willingness to participate in banking operations [8].

Given the importance of technology in banking, the significant risks that may result from exploiting weaknesses in its use and management, and banks' concerns about the growing threats to this sector's institutions worldwide, adhering to standard technology controls, solutions, and tools, and ensuring their effectiveness, have become mandatory, fundamental, and effective steps recommended by previous standards, studies, and experiences [7], [8], [13-17]. A Study [10]

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

found that the application of sound strategies and innovative and modern technological solutions and the development and implementation of technology use and management policies provided by international standards such as ISO 27001 contribute positively to reducing those risks and their implications, it was found that there is a correlation between the application of IT protection controls provided by this standard and the average value of the critical level of security threats to an enterprise's information and systems, which is approximately five levels lower in systems that apply the controls of this standard (4.00) than in systems that do not adhere to those controls (8.75).

Based on the foregoing, measuring and evaluating technology and innovation practices in Yemeni banks' information security management systems and determining the extent to which banks adhere to their normative implementation requirements is a critical topic, but by analyzing the literature and identifying the research gap, a local theoretical and applied research gap has been found. The only study that dealt with the unilateral identification of the security gap in the banks was the process and procedure aspect oriented. Moreover, that study did not address vulnerabilities as future challenges for each of the institutions assessed, nor did it identify and compare maturity levels or security gaps between those institutions, but rather from the general perspective of the banking sector as a whole. Accordingly, the objective of this study is to analyze the level of compliance of Yemeni banks' information security management systems with technology and innovation controls, identify technological strengths and weaknesses in their practices, and provide appropriate solutions and treatments to reduce the applied gap in such practices; this can be achieved by answering the following questions representing the problem of research:

Q.1: What is the maturity level of the technology and innovation practices implemented by Yemeni banks' information security management systems?

Q.2 Which banks constitute the weakest link in the banking sector's technological and innovation security practices?

Q.3 which indicators constitute the greatest weakness in the banking sector's technological and innovation security practices?

Q.4 what is the applied security gap that each bank must reduce to reach an ideal maturity level at the level of each technology and innovation indicator?

Q.5 which indicators can be considered as future challenges? Are the Yemeni banks' efforts to address them different?

The remainder of this paper is organized as follows: Section II presents previous studies relevant to the research topic and summarizes the theoretical and practical research gaps through which we seek to contribute to its closure, and Section III reviews methods and tools for data collection and analysis. Sections IV and V present and discuss the results of this study. This followed by a summary of the most important conclusions and recommendations in the last section.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

II. Related Works And Literature Review

This section reviews the literature on the topic of this study, which devoted to identifying the main opportunities and challenges associated with the application of modern technology in the banking sector, determining the nature of technological risks, drawing assessment requirements, establishing a suitable methodological framework and method to measure compliance with technology and innovation requirements in information security practices, and formulating the research gaps in the maturity assessment of technology and innovation in Yemeni banks' security practices and the role of the current study in reducing them. The following subsections provide the most important outputs of this phase:

A. The Role of Information Technology and Systems in Improving the Performance of Yemeni Banks

In the current period, decision support, data mining, and artificial intelligence tools and techniques have become a key part of business information systems [18], [19] and are heavily relied upon in management decision-making at all levels in all sectors, including health [20-24], tourism [25], [26], education [27], [28], Social [29] and other critical sectors. However, information plays a critical role in achieving the objectives of these system [18], [28]. It is considered the main driver of business, where the ability of organizations to provide the necessary information for business decisions at the necessary time and at the appropriate quality has become a set of key enabling standards for the success of these organizations and the quality of their competitive business decisions. In the banking sector, the study [30] also indicates that banking business models have mainly focusing on promoting consumer satisfaction, which cannot be achieved without keeping up with modernity, evolution, and innovation in providing appropriate quality services and products that are easy to access, safe, fast, and cheap.

Globally, this topic has been discussed in several previous studies during the era of the fourth industrial revolution. For example, one study [30] addressed the application of blockchain technology in the financial sector. In addition, [31] examines financial sector strategies to keep up with modern technology. Another Chinese study [32] reviewed the effects of volatility in the global financial system under this revolution and its technological financial products, and spoke of the role of the Chinese banking sector as one of the major stakeholders causing this technology at the local level.

Many other studies have addressed the importance and role of modern technology in the development of this sector by improving its output and services. These studies have found that information systems and their technologies have a significant impact on the delivery of banking services to customers [33], enhancing the quality and effectiveness of service performance and operations [34]; and marketing strategies [35], making it more efficient and effective in increasing and improving customer satisfaction with the banking services provided, providing new channels of service, and meeting consumer expectations [36].

Locally, studies [37] and [38] emphasize the importance of their application in Yemeni banks and recommend that they should be used to improve the marketing performance of Yemeni banks and provide high-quality and low-cost services and products by redesigning banking operations.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

Other studies have emphasized their effective role in increasing the speed of communication and fulfilling customers' demands [39]; and in providing extensive data and information on customer consumption patterns quickly, efficiently, and effectively [40]. Another study [41] found that the exemplary application of modern information systems and technologies in Yemeni banks contributes to the provision of information for decision-making on the development of plans and programs; improves the quality of banking service performance; strengthens the management, qualification, and training of human resources by focusing on the efficiency of staff performance and the skills they possess in implementing banking services, remaining its significant contribution to the delivery of services capable of achieving a high degree of customer satisfaction and loyalty.

However, an analysis of literature on the opportunities for the application of information technology in the Yemeni banking sector found that: (1) the banking sector represents the nervous system of the national economy and contributes significantly to its development and growth; (2) this sector is obliged to keep abreast of technological development in all areas linked to its performance as a primary financier of all economic and investment activities in Yemen. Still, (3) the sector's enterprises can only cope with the intense competition imposed by the conditions of globalization at their current capacity by keeping pace with technological development and its tools; and in line with the intellectual and cultural changes generated by the Fourth Industrial Revolution, which are the creation of new, diverse, and changing desires and needs. In addition, (4) the utilization of modern, innovative technology in the banking sector is very important for maximizing profit, reducing costs, improving processing and production processes, and providing market services, thereby enhancing the sector's role in achieving development goals and enhancing its compliance with social responsibility requirements.

B. Information Security Risks in the Banking Sector

Despite the advantages that technology offers to bank sectors around the world and the economic advantages and benefits it offers to the Yemeni banking sector, it has many weaknesses, which expose banks and financial sectors globally to many cyber attacks. According to [9], the finance and insurance sector is the sector most vulnerable to cyber threats among all other industrial sectors and retains its place at the top of this list from 2015 to 2020. In addition, according to this report, it held the top spot in 2021 at the Asian level; at 30%.

With respect to the Middle East and Africa, within which the geographical boundaries of this study lie, with a total tally of almost half of the threats to all sectors (48%), finance and insurance institutions in 2021 were also the most affected [9], while the health care and energy sectors were exposed to a quarter of the threats (25%), occupying second (15%) and third (10%) respectively, reflecting the overall risk to financial institutions globally and regionally.

By analyzing what these studies have presented, cyber threats, in the absence of compliance with protection requirements, can be said to pose a threat to banks globally, entailing many strategic, operational, moral, and legal losses and negatively affecting banks' performance and continuity.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

However, the studies on the impact of cyberattacks are numerous, most notably [7], [8], [11], [12], [42], [43], and [44].

Drawing on these studies, it can be stated that cyber threats, in the absence of compliance with protection requirements, could pose a threat to banks globally, entailing many strategic, operational, moral, and legal losses and negatively affecting banks' performance and continuity. For example, risks arising from the theft and unlawful use of sensitive information, which undermine the achievement of the organization's objectives and the implementation of competitive advantage plans due to the lack of appropriate security strategies for the use of technology, could be considered an example of strategic risks. While risks arising from the exploitation of technical weaknesses to compromise the integrity and availability of banking systems and services, which render them unable to provide services as usual, may be an appropriate example of operational risk, If, for example, an enterprise is sued for failure to comply with stakeholder privacy protection laws or failure to comply with customer service contracts, these risks become legal. If the situation worsens and information is abused to damage the organization's reputation and is disseminated to provide excellent service according to safety, confidentiality, and accuracy standards, the risks become reputational.

Based on the foregoing, Yemen's banking sector, like other international financial sectors, is one of the forces of local development and its economic baptism. Its work is based on modern technology, and the many information assets it possesses are a major factor in the success of its institutions and the continuity of the services and businesses it provides. It will remain vulnerable to cyberattacks and cyber risks to other banks globally unless they adopt appropriate protection policies and strategies and unless they work to provide and use technological and innovative protection tools in accordance with globally applicable standards.

C. Iso 27001-Based Security Controls

It is universally recognized that the stronger the application of information security controls in an enterprise, the higher the level of security that an enterprise enjoys, and the higher this level, the more likely that enterprises will achieve their business objectives.

Technology and innovation controls are key branches of information security controls [13], [15]. They focus on many technical aspects, such as the application of tools, software, and protection algorithms. Identification of mechanisms for the design and development of secure systems, documentation, monitoring, and control of access to information assets. In addition, they contribute to building, developing and documenting policies for the use and management of technical security solutions in the enterprise's information security management system [16], [17].

However, it is not always easy to make decisions regarding identifying, developing, applying, and building technical security tools, solutions and associated policies. Where do specialists in information security management systems face many relevant questions, for example, what technological solutions should be implemented? How can they be devised in line with an ever-changing security landscape? What should be the focus of specific technological policies? To

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

answer these questions, specialists are looking for reliable and universally accredited sources of guidance and standards.

The international information security standard constitutes the most prominent group of such sources [14]. Security standards include a set of officially agreed and recognized rules, practices, and controls that can be used to control the organization's operations and procedures to maintain information security. It can also be seen as the starting point in defining functions for information security departments, defining the basis and requirements for security assessment, promoting communication and common and stakeholder actions, and determining the content that security policies and regulations must entail.

Many international information security standards are available, and many recent studies have analyzed and compared them, such as [45]; and [46]. The ISO Standard 27001-2013, one of the most prominent of these standards, specifies the requirements and obligations necessary for the establishment, application, operation, and maintenance of an information security system in institutions. It also includes the requirements for assessing and addressing information security risks that are commensurate with the organization's needs, the requirements set out in the standard, and aims to be applicable to all institutions, regardless of their type, size, nature, or orientation.

According to [14], and [17], the ISO 27001 standard is characterized by taking into account all kinds of risks to which an enterprise may be exposed, specifying the necessary conditions for the application of security controls that meet each organization's needs, as well as the requirements for assessing and addressing information security risks that are commensurate with the needs of different institutions. Previous studies have also emphasized the importance of applying these criterions' controls to reduce risks, including risks related to weaknesses in information systems and technology.

The study [16] emphasized that the protection of institutional assets is necessary to ensure business continuity and reduce business risk. The study [17] also emphasized that maintaining information security is vital and requires compliance with the technological controls provided by ISO 27001, through which the technology to be used in the enterprise can be known, and the mechanism through which it must be innovated to match the changing security landscape.

In addition, a significant and influential gap has been observed in the level of threats and in the system's effectiveness in reducing security threats to information security systems in organizations that do not comply with ISO 27001 controls compared to those that comply with them. The study [10] concluded that the average security threat level in institutions applying ISO 27001 protection controls and recommendation is decreased by approximately five units (4.00), compared to institutions that do not apply them (8.75). It was also found that the average effectiveness of mitigating cyberattacks in them was also increased by approximately 22 units (40.74), compared to institutions that do not apply them (18.32).

From the foregoing, we can conclude that this standard is one of the most important and efficient international standards that can be used to reduce risk, and there is a critical need to implement technology and innovation protection controls in Yemeni banks to reduce the level of threats and

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

upgrade the efficiency of banking systems. However, this standard contains too many controls and indicators (134), grouped into different areas, not all of which are suitable for measuring the maturity of technology and innovation practices. Therefore, what is the ISO 27001-based framework that is appropriate for measuring information security maturity in the technology and innovation domain? This will be addressed in the next subsection.

D. Maturity Measurement Models Based On Is27001

Previous studies have contributed to the development of different assessment frameworks and models based on the ISO-27001 standard. However, despite the multiplicity of frameworks, the aim is to provide flexible frameworks for evaluation with known evaluation categories, allowing the institution to focus on specific categories that are consistent with their structures, responsibilities, objectives, and orientations. For example, the model proposed by [47] classifies these controls into five categories: data, hardware, software, people, and networks. Through this model, the security level can be measured according to the type of institutional asset, whereas [48] proposed a triple model (administrative, technical, and operational) to measure the level of security compliance. In addition, the study [15] used the previous two models along with another six-dimensional model (strategy, policy, regulation, human and technology, and facilities) to build a multi-architecture assessment framework.

In addition, [17] proposed a framework for evaluating information security maturity. This model covers four security dimensions: processes and procedures; technology and innovation; security governance; and risk management. In Addition, this study developed a maturity model to measure enterprises' maturity levels with technology and innovation controls in accordance with the ISO 27001 standard. This study also proposes a maturity model as a methodological framework for the study and analysis of the level of compliance in the technology and innovation domain practices according to ISO 27001, which is characterized by quantitative and qualitative measures and includes the key requirements for measuring compliance with information security practices in this study.

Local studies on the assessment of information security controls based on the ISO 27001-2013 standard are limited. The studies [13] and [14] aimed to assess the level of compliance with all information security controls in the Yemeni Academy, and a study [15]; proposed and applied a hierarchical model to measure controls according to a set of objectives. In [16], relying on the evaluation framework proposed by [17], the level of compliance of Yemeni local banks to the operations and procedures of security requirements was measured.

However, by analyzing local and international literature on the topic and environment of the study, it was found that (1) there are significant previous scientific contributions, providing appropriate and comprehensive frameworks that can be relied upon to solve the study's problem, and (2) the framework and model proposed by the study [17] provide indicators and a model for measuring maturity in information security practices in four different areas. It has been applied in the Yemeni banking environment to measure maturity in bank practices associated with the field of operations and procedures. It can also be used to measure maturity in technology and innovation security domains. (3) the field of study and its environment have theoretical and

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

applied gaps. Insufficient security studies are available to assess maturity, and identifying the gap in information security practices in general and in Yemeni banking institutions in particular. (4) Limited studies have focused only on measuring the level of compliance with requirements and on identifying the applied gap in banking practices in general, without elaborating on the level of maturity or the extent of the applied gap in each bank's practices.

III. METHODS AND MATERIALS

A. Study Community

The basic community for this study consists of all 17 Yemeni banks located in Yemen's capital, Sana'a. However, in accordance with banking regulations and procedures for scientific research practices in this sector, the approval of banks administration is required. For this purpose, at the basic stage, a member of the research team conducted 17 individual interviews with the directors or deputy directors of the competent departments of all 17 banks to obtain approval and permit for gathering the necessary data and identifying of experts responsible for the evaluation of technology and innovation practices in each organization. Finally, 76.5 percent of the banks approved the researchers' proposals, whereas the remaining banks refused to cooperate with the research team.

The four banks that did not agree to cooperate indicated that their refusal was due to their management preventing external research teams from monitoring or evaluating their practices; because information security in banking institutions is a sensitive topic; and that gathering information about their security situation and knowing the weaknesses in their practices would make them vulnerable to threats. Because the study society is limited and all its members are accessible, researchers have relied on a comprehensive inventory method intended to collect data from all study community members without exception.

Accordingly, all specialists and information security experts have been targeted at all 13 banks, including: B1 - The Yemen Bank For Reconstruction And Development (2 experts); B2- The National Bank Of Yemen (1 expert); B3-Housing Credit Bank (2 experts); B4- International Yemen Bank (5 experts); B5- Yemen Kuwait Bank (2 experts);B6- Cooperative & Agricultural Credit Bank (5 experts); B7- Rafidain Bank (1 expert);B8-Yemen Commercial Bank (5 experts) ;9- Islamic Bank Of Yemen (3 experts);B10-Tadhamon Bank (3 experts); B11- Saba Islamic Bank (2 experts); B12- Shamil Bank Of Yemen & Bahrain (3 experts); and B13- Qatar National Bank (3 experts).

B. Data Collection Tool

In this study, the researchers used a questionnaire to investigate experts and specialists. As previously explained, the questionnaire's questions and maturity measurement levels were built on the tool and maturity model proposed by [17], which was specifically developed to measure technology and innovation security maturity in information security management systems. To facilitate understanding and provide more explicit research questions, the measurement indicators and maturity assessment levels in this model were first translated from English to Arabic. To determine the suitability of the questionaries' statements (indicators) for the objectives

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

they measure and for the category to be targeted to answer, and to ascertain the appropriateness of the measure used in this study, this step was followed by the implementation of the ostensible truthfulness examination of the study tool in its preliminary version. At this stage, the questionnaire was presented to a group of 15 scientific committee members, including academics and security experts in the banking sector. Based on their opinions and observations, necessary adjustments were made, and the final questionnaire version, consisted of two main parts. The first part included respondents' demographic data (sex, scientific qualification, specialization, and years of experience), while the second part included ten indicators to measure the level of maturity. To obtain accurate quantitative results, the indicators in the questionnaire were formulated in the form of multiple-choice questions. The respondents' responses were restricted to five options, the weights of which were determined to represent the five levels of the TI maturity model and include (weak security (L1)), security awareness (L2), basic security (L3), meets the requirements (L4), and robust security (L5)). Table 1 summarizes these components.

In phase III, to determine whether the scale results were consistent, stable, and unchanged in an influential manner if the scale was repeated, Cronbach's alpha coefficient was calculated. The stability rate was high and equal (84%), while the credibility rate was very high and equal (94%). This means that the tool can be disseminated to the study community and used in practice to collect data, as discussed in the following section.

C. Data Collection

The data collection consisted of two phases. In the first phase, 37 questionnaires were distributed to all experts and specialists in the study community via e-mail, of which 83.87% were returned. In the second phase, the integrity and validity of the recovered questionnaires were examined, and valid questionnaires were selected for processing and analysis in subsequent stages. Consequently, five questionnaires were excluded, and the number of processable and analytical questionnaires was 26, representing 83.87% of the total returned questionnaires and 70.27% of the total questionnaires sent. The questionnaires were distributed as follows: B1(1); B2 (1); B3 (1); B4 (3); B5 (2); B6 (3); B7(1); B8 (3); B9 (3); B10 (2); B11 (1); B12 (2); and B13 (3).

D. Data Processing and Analysis.

1) Maturity criteria

This study relies on the maturity model proposed by [17] to determine the maturity level in applying technology and innovation requirements in the management of banking enterprise information security systems. Table 2 presents the five component levels of this model. ML = L1 ,... L5), verbal expression (VE), presents a description of each of these levels and also explains the scope maturity index (MI) and the applied gap (G) mapped to each level.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

Table I: Questionnaire Statements and Their Levels of Implementation

S	Statement	L	Application level		Indicator	L	Application level
1	Supporting the design of information systems for innovation requirements:	1	No support whatsoever	6	Authentication and authorization mechanisms and controls to access the network:	1	There is no mechanism to ensure effective access control.
		2	haven't been matched yet.			2	Resources exist and control policy is applied, but incompletely.
		3	The current requirements have been matched.			3	Network access control and internal resource and equipment policies are applied only.
		4	All requirements are matched and support improvement.			4	There are controls and policies in place to ensure proper identification and validation of network services.
		5	Technology supports change and improvement at an advanced level.			5	Both internal and external network access mechanisms are constantly monitored and reviewed.
2	Technology reflects protection considerations during systems design:	1	There is no indication that security is being taken into account.	7	Average readiness rate of the bank's network per year	1	fewer than 30%
		2	Security is considered as a modification after deployment			2	30-50%
		3	reflects basic security requirements.			3	51-70%
		4	Demonstrate careful security considerations during the design phase			4	71–90%
		5	supports flexibility and innovation in security provisions.			5	91-100%

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

3	Access Control Mechanisms:	1	not available.	8	The policy for implementing encryption techniques and controls	1	There is no policy or interest in information security.
		2	weak.			2	There is an understanding of the role of encryption, but no plans to implement it.
		3	unspecified and imprudent.			3	One form of encryption control is used.
		4	Ideally used.			4	All controls are used according to the text of the encryption policy.
		5	Implemented innovatively and always reviewed			5	Policies and techniques are constantly reviewed and improved.
4	Technical measures or controls to ensure information security .	1	Not existed	9	Activity Registration and Tracking Mechanism	1	Non-existent.
		2	There is only awareness of malware risks			2	A limited number of operational activities are recorded and tracked.
		3	There are basic controls, but they are not upgraded.			3	The activities of all sensitive information systems are recorded and tracked across all departments.
		4	There are constantly applied standard controls.			4	A sophisticated mechanism is used to record and monitor applications, systems, and networks.
		5	There are innovative controls and techniques that are constantly adopted.			5	All activities are recorded and monitored periodically, and previous activities can be retrieved and tracked.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

5	Tools and measures to examine and address technical weaknesses	1	There are no tools to examine weaknesses.	10	The number of security attacks that occurred and hampered the bank's major operations	1	Several times
		2	There are old and ineffective combatants.			2	Two times per month
		3	There are only a few inspection and evaluation tools			3	once every six months.
		4	Assets, vulnerabilities, and processing methods are assessed quantitatively, wholly, and on time.			4	Only about once a year
		5	Vulnerability screening tools and malware are constantly evaluated			5	It never happened.

Table 2: Maturity Criteria for Technology and Innovation Practices.

ML	VE	Description	MI		G	
			From	To	From	To
1	Weak Security (WS)	Technology used is still substandard and vulnerable to threats	0	1.5	3.5	5
2	Security Awareness (SA)	Security investment in information systems is as the need arise and reactive	1.6	2.5	2.5	3.4
3	Basic Security (BS)	Basic security requirements are met. Maintenance and upgrade to match standard is lacking	2.6	3.5	1.5	2.4
4	Meets the requirements (MR)	Full security requirements implementation; standard cryptographic controls are used.	3.6	4.5	0.5	1.4
5	Robust security (RS)	Innovative use of standard and latest technology to ensure security	4.6	5	0	0.4

1) Calculation Of The Average Maturity Assessment And Gap Values

Suppose that the value of evaluating the performance indicator number (S) out of a finished set of technology and innovation indicators (m) expresses the expert opinion number (r^b) of the total number of experts or specialists (n^b) affiliated with the bank (b) out of all the banks studied is equal to $(MI^b_{r^b{}_s})$. Where $s = \{1.2 \ldots . m = 10\}$; $n^b = \{1.1.1.3.2.3.\ 1.3.3.2.1.2.3\}$; $b = \{1.2 \ldots . d = 13\}$. Then, eight steps are performed to calculate the average maturity and applied gap values in technology and innovation practices, which summarized in Table 3.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

Table 3: Steps for Calculating Average Maturity and Applied Gap Values in Ti Practices

Steps	The goal is to determine ……	An equation used
1	The average value of expert assessment values for the bank's performance index (S)	$MI_s^b = \frac{1}{n^b} \sum_{r^b=1}^{n^b} MI_{r^b s}^b$ (1)
2	The value of the average applied gap between the ideal maturity level of the performance index No. (s) and the average value of expert assessment values for this indicator at Bank No. (b).	$G_s^b = EML_S - MI_s^b$ (2)
3	The average value of the evaluation of all technology and innovation indicators in the bank number (b)	$MI^b = \frac{1}{m} \sum_{s=1}^{m} MI_s^b$ (3)
4	The average value of the applied gap between the ideal maturity level (EML) of technology and innovation practices and the average value of assessing all technology and innovation indicators in the bank (b)	$G^b = EML - MI^b$ (4)
5	The average value of the expert assessment of performance index No. (s) in all Yemeni banking sector institutions	$MI_S = \frac{1}{d} \sum_{b=1}^{d} MI_s^b$ (5)
6	The average applied gap between the ideal maturity level (EML_S) of performance indicator No. (s) and the average value of experts' assessment values of this index in the banking sector	$G_S = EML_S - MI_S$ (6)
7	The average value of the evaluation of all technology and innovation indicators in Yemen's banking sector	$MI = \frac{1}{d} \sum_{b=1}^{d} MI^b$ (7)
8	The average value of the applied gap between the ideal maturity level of technology and innovation practices (EML) and the average values of evaluating all technology and innovation indicators in the Yemeni banking sector	$G = EML - MI$ (8)

IV. Assessment Model Application And Results

Through the application of (1), the results of the maturity index assessment averages (MI_s^b) for each (S) of the 10 technology and innovation indicators for each of the 13 banks (b) from the perspective of security experts and specialists were calculated, as summarized in table 4. For example, the value of $(MI_1^5 = 4)$ means that the average maturity index for the first indicator measuring "Supporting the design of information systems for innovation requirements" in Bank No. 5 is equal to 4. Then, through the use of (2), the applied gap value (G_s^b) between the ideal maturity level (L5), which represents the ideal state we aim to achieve to reach a robust security level at each indicator level, and the actual (MI) for each indicator (S) in each bank (b) were calculated, For example, the value of $(G_1^5 = 1)$ means that the applied gap between the fifth maturity level value $(EML_S = EML_1 = 5)$, "Technology supports change and improvement are implemented at an advanced level," which represents the robust security level for the first indicator " Supporting the design of information systems for innovation requirements". The maturity index assessment average for that indicator in the fifth bank $(MI_1^5 = 4)$ is equal to 1.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

Table 4: The Results of the Maturity Index Assessment Averages on Each Bank's Performance Indicator

S	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13
S1	5.0	5.0	4.0	4.0	4.0	3.3	2.0	2.7	3.0	4.5	3.0	4.0	3.7
S2	5.0	2.0	5.0	4.3	2.0	2.7	2.0	3.7	4.0	5.0	2.0	3.0	4.0
S3	4.0	4.0	4.0	5.0	5.0	3.7	3.0	4.0	4.0	4.5	4.0	4.0	3.7
S4	4.0	5.0	3.0	5.0	2.0	2.7	2.0	4.7	4.0	4.5	4.0	4.0	4.0
S5	5.0	4.0	3.0	5.0	4.0	2.7	3.0	4.3	3.0	5.0	5.0	4.0	4.3
S6	4.0	5.0	4.0	5.0	4.0	3.0	2.0	3.3	4.0	5.0	4.0	4.5	4.3
S7	5.0	5.0	3.0	4.7	4.0	4.3	1.0	3.7	5.0	4.5	5.0	4.0	5.0
S8	4.0	5.0	2.0	4.0	2.0	2.7	2.0	3.0	4.0	5.0	5.0	3.5	4.0
S9	4.0	5.0	3.0	4.3	2.0	2.3	2.0	3.0	3.0	5.0	5.0	3.0	4.3
S10	5.0	4.0	5.0	5.0	3.0	4.7	5.0	4.3	5.0	5.0	5.0	3.0	3.3

Subsequently, using (3) and (4), the maturity index assessment averages (MI^b) of the TI security domain for each of the 13 banks (b), the applied gap value (G^b) between the ideal maturity level (L5), which represents the ideal state we aim to achieve in order to reach a robust security level at the overall TI security domain level, and the actual overall (MI) for each bank (b) were calculated. Then, using table 2 on criteria for classifying the security maturity levels, each bank's overall maturity level was determined as shown in table 5.

Table 5: The Results of the Maturity Index Assessment Average, Gap, Maturity Level for Each Bank's Security Management System

	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13
MI^b	4.5	4.4	3.6	4.6	3.2	3.2	2.4	3.7	3.9	4.8	4.2	3.7	4.1
G^b	0.5	0.6	1.4	0.4	1.8	1.8	2.6	1.3	1.1	0.2	0.8	1.3	0.9
ML^b	4	4	4	5	3	3	2	4	4	5	4	4	4
VE	MR	MR	MR	RS	BS	BS	SA	MR	MR	RS	MR	MR	MR

Next, applying (5) and (6), the maturity index assessment averages (MI_S) of each (S) of the TI indicators in the overall banking sector, and applied gap value (G_S) between the ideal maturity level (L5) at the indicator level, and the actual overall (MI) on each (S) were calculated. In the same way, using table 2, the banking sector's overall maturity level for each (S) was determined as shown in table 6.

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

Table 6: The Results of the Maturity Index Assessment Averages, Gaps, and Maturity Levels on Each Indicator

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
MI_S	3.7	3.4	4.1	3.8	4.0	4.0	4.2	3.6	3.5	4.4
G_S	1.3	1.6	0.9	1.2	1.0	1.0	0.8	1.4	1.5	0.6
ML_S	4	3	4	4	4	4	4	4	3	4
VE	MR	BS	MR	MR	MR	MR	MR	MR	BS	MR

Finally, a value of 3.9 out five overall maturity index assessment average (MI) on the whole TI security domain in the Yemeni banking sector, with the value of 1.1 overall applied gap (G) were estimated using equation 7 and equation 8, respectively. Accordingly, the estimated overall maturity level of the Yemeni banking sector on this domain is four.

V. DISCUSSION OF RESULTS

Q.1 what is the maturity level of the technology and innovation practices implemented by the Yemeni banks' information security management systems?

Based on the final outcome of the study, Yemen's banking sector implements technology and innovation security controls, mechanisms, and tools with an average total of 3.9 out of five and an average maturity level of four. This means that the sector's banks in general meet only the key technological and innovative security requirements with an average application gap of approximately one level (1.1). This result can be attributed to the fact that a large proportion of banks (61.5%) apply the TI security requirements at the fourth maturity level, which meets the requirements of technology security and innovation, versus only two banks that make up (15.3%) of the total banks, in which these requirements are implemented at an ideal maturity level (see Table 4). These results indicate that Yemen's banking sector lacks robust technology and innovation security requirements and still needs to strengthen its security practices through the application of appropriate mechanisms that enable enterprises to use innovative security standards and modern technological tools and mechanisms [17].

Q.2 Which banks constitute the weakest link in the banking sector's technology and innovation security practices?

The level of banking institutions' application of technology and innovation requirements varies in general from bank to bank and can be arranged according to the average level of application of field indicators as: (B10 > B4 > B1 > B2 > B11 > B11 > B9 > B12 > B8 > B3 > B6 > B5 > B7). Fig, 1 shows the values of the average maturity index and the average applied gap for each bank.

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

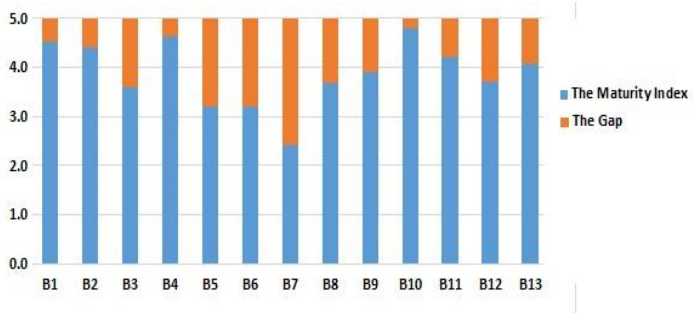

Figure 1: The maturity index assessment average, and gap for each bank's security management system

According to the previous figure, the seventh bank implements technology and innovation requirements with an average overall valuation of 2.4 out of five and a very large gap of 2.6. This means that it is the weakest link in the chain of Yemeni sector banks in terms of meeting these requirements. By reference to Table 5, it is also clear that the maturity level of this bank's practices is only third-level, which means that this bank only complies with the basic security requirements to which it is subject, but lacks maintenance and updating to meet the requirements of information security standards. Also, by reference to table 4, it can be observed that this bank maintains the 10th lowest rating in the results of the evaluation of 80% of TI indicators and the penultimate rating in the results of the evaluation of 10% of them as well.

This indicates that the bank suffers from a significant implementation gap in the application of 90% of the requirements of the indicators; the design of its information systems does not match any of the current or future requirements for innovation, nor support change and improvement as required to reach a robust security level. In addition, the information technology used in its systems does not even reflect the basic requirements of security during the design of information systems, not to mention the large gap between this level and the optimal maturity level that requires the bank's technology to reflect flexibility and innovation in applying security controls when designing bank systems. On the other hand, the access control mechanism is undefined and unrestricted; the basic technical measures needed to ensure information security are not available; and the internal and external network readiness rate is very low, not exceeding 30%. Findings also indicate that the maturity level is limited and does not exceed the security awareness level in the remaining 70% of indicators. For these reasons, the 7th bank is the weakest security link, and it needs to adhere to information security controls at all TI aspects. In addition to the above, by a margin not exceeding one level (0.8), the level of gap resulting from the practices of the fifth and sixth banks for technology and innovation requirements is lower than that of the seventh banks, and therefore, these two banks are second among Yemen's most vulnerable banks in applying the requirements of TI security. The main weaknesses they share are a lack of technical measures or controls; a lack of mechanisms for recording and tracking activities; and a lack of an appropriate policy to use encryption techniques and controls to ensure information security.

Q.3 Which indicators constitute the greatest weakness in the banking sector's technology and innovation security practices?

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

The level of commitment to security requirements for technology and innovation varies depending on the nature of the security controls themselves. Indicators can be arranged according to the average maturity level in their application by banking institutions as follows: (S10 > S7 > S3 > S5 = S6 > S4 > S1 > S8 > S9 > S2). Fig, 2. illustrate the average eligibility level values and the average gap in the banking sector's application of these indicators.

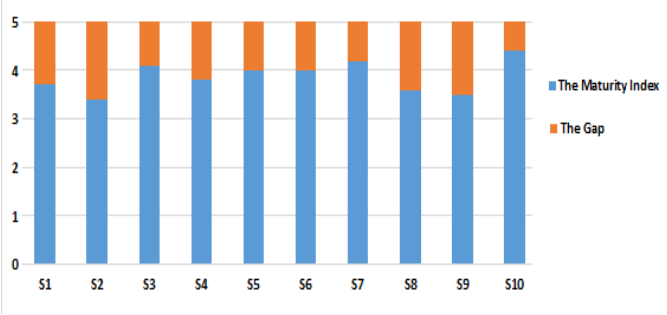

Figure 2:The maturity index assessment average, and gap on each security indicator

According to this figure, with an average overall assessment of no more than 3.5 out of five and with an application gap of at least 1.5, the second and ninth indicators are the most significant weaknesses in the overall level of technology and innovation practices in the banking sector. This means that the banking sector in general applies the requirements of these two indicators at the basic level of security, but it still lacks the maintenance and modernization necessary to meet the maturity requirements of the fourth maturity level, which emphasizes that security issues should be taken into account in the design of banking information systems and that technology can reflect this when used, as well as emphasizing the use of appropriate controls and policies to create and manage users' identities and applications and control their access to resources. This is in addition to the advanced requirements of the fifth maturity level, which emphasize the need for technology to be flexible and capable of accommodating innovations and updates in the area of security controls, as well as the need for periodic monitoring, updating, retrieval, and tracking of all activities and access identities where needed [7]. At the banks level, with a tringle-level common gap, at least 23% and 15% of banks shared the security gaps and weaknesses associated with the second and ninth indicators, respectively, and by the same ranking, with a double-level gap, these weaknesses are shared by at least 53% and 39% of them.

Q.4 What is the applied security gap that each bank has to reduce in order to reach an ideal maturity level at the level of each technology and innovation indicator?

The proportion and level of Yemeni banks' lack of information technology and innovation controls required to ensure a strong level of security maturity vary. Fig. 3 depicts the percentage of indicators that are implemented at a high, and robust level of security maturity through the incorporation of innovations and modern technological security solutions into Yemeni banking business practices(% of $S.ML_S = 5$), It also shows the percentage of indicators that banks still need to look for innovative and modern security solutions that enable them to achieve optimal maturity in their practices (% of $S.ML_S < 5$).

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

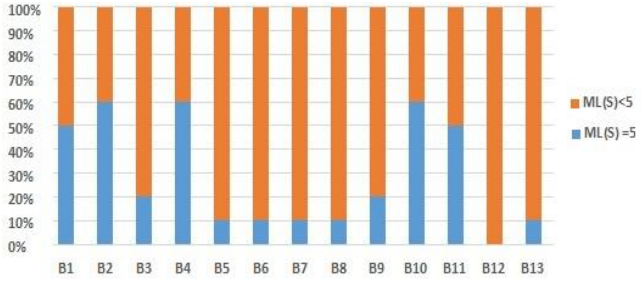

Figure 3:Distribution of indicators according to maturity level in their implementation

By reference to fig. 3, it can be seen that: (1) There are significant discrepancies between the proportions of indicators that Yemeni banks need to strengthen their respective technology and innovation controls to improve security; (2) The range of this discrepancy is fairly large (60%) and falls between (40%) and (100%); (3) A percentage of (7.7%) of the total Yemeni banks (the twelfth bank) need to strengthen TI practices to reach the optimum robust security level, and the main reason for this is that this bank's practices at the level of all indicators were not perfect enough and were distributed at different maturity levels without attaining the required maturity level; (4) Seven banks (54 % of banks) apply optimal level requirements to one (5th, 6th, 7th, 8th, and 13th) or only two (3rd and 9th) of the ten indicators; and (5) five banks (38 % of banks) apply optimal level requirements to five (5th, 6th, 7th, 8th, and 13th) or six (3rd and 9th) of the ten indicators. This means that the group of banks in this category needs an average effort (addressing only 40–50% of indicators) to achieve total compliance with strong security requirements at the level of all indicators, unlike previous groups that require relatively significant efforts to address weaknesses of between 80% and 100% of them.

In detail, these indicators can be classified into four different categories as follows: (1) The first category includes indicators with a significant concentration in the range of 60–100% of banks. In this category, the proportion of banks that achieve the ideal maturity level is not less than 60%. It includes only one indicator (the tenth), which tests "the number of security attacks that occurred and hampered the bank's major operations". With an average rating of 4.4, this indicator is first among the best applied indicators in the banking sector's practices in general. Its requirements are implemented at the level of strong security in 8 banks (62%), while only 5 banks (38%) have a gap in the application of its security controls (see table 4). However, the size of the gap in applying the requirements of this indicator varies among the banks in this category. Two of them (the second and eighth) apply these requirements with a single-level gap, while the other three banks (b12, b13, and b5) apply them with a double-level gap, which means that the five banks that have weaknesses in the application of the requirements related to this indicator need to fill an average application gap of 1.6.

The second category includes indicators with a significant concentration in the range of 40–60% of banks. It also includes one indicator (the seventh), which examines the "average readiness rate of the bank's network per year". This indicator ranked second among the most concentrated indicators, with an average maturity index roughly equal to the tenth indicator's index, which equals 4.2. Unlike the tenth, the proportion of banks adhering to the seventh indicator's

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

requirements at the robust security level is lower (46%) than the proportion of those adhering to them within a gap (54%), (see table 4). However, five banks (the fifth, sixth, eighth, twelfth, and thirteenth) adhere to these requirements with a single-level gap, while the other two banks (the fifth and the seventh) follow them with double-level and four-level gaps, respectively. This means that these partially compliant banks have weaknesses in the application of this indicator's requirements and they should fill a gap, the size of which is approximately equal to that which banks have to fill for the tenth indicator (1.57).

While the third category covers indicators with a significant concentration in the range of 20–40% of banks, compared to the previous two groups, this group includes the largest percentage of indicators (60%), and can be divided into two subgroups; the first subgroup having one indicator is the fifth, while the second contains the second, fourth, sixth, eighth, and ninth indicators. The fifth indicator, which tests "tools and measures to examine and address technical weaknesses," has ranked fourth among the most concentrated indicators, with an average maturity index roughly equal to 4. Like the tenth, the proportion of banks adhering to this indicator's requirements at the robust security level is lower (31%), than the proportion of those adhering to them within a gap (69%). However, in addition to the second indicator, four banks of those who adhere to the second group indicator's requirements with a single-level gap (fifth, eighth, twelfth, and thirteenth) adhere to the fifth indicator's requirements with the same level of gap, while the third, sixth, seventh, and ninth indicators follow them with a double-level gap. The second subgroup's indicators were ranked third, fourth, fourth, fourth, and third, respectively, with an evaluation average ranging from (3.4) to (4th). However, 10 banks do not adhere to their robust security requirements for these indicators. Overall, all banks in this category have weaknesses in the application of these indicators' requirements and they should fill gaps, the size of which are bigger or similar to those which the banks have to fill for the first and second categories' indicators, and these gaps ranged between 1.4 and 2.

The last category covers indicators with a significant concentration of less than 20% of banks. In other words, with this category of indicators, more than 80% of banks are not fully compliant and they should fill the highest security gaps to improve their security status. It covers two indicators, the first and third indicators, these indicators ranked seventh and third, with an average maturity index equal to 3,7 and 4.1, respectively. Unlike other categories, the proportion of banks adhering to these indicator's requirements at the robust security level is lower than the proportion of those adhering to them within a gap by 5.6 times. However, six and ten banks adhere to the requirements of these indicators with a single-level gap, respectively. with the same ranking, four and two banks follow them with a double-level gap. However, these banks have weaknesses in the application of these two indicators' requirements and they also should fill gaps of 1.55 and 1.09 to improve their security status linked to the first and third indicators, respectively. Table 7 summarizes the technology and innovation indicators and the number of banks that need to fill the applied gap for each indicator. It also summarizes the average level of gap that banks in the Yemeni banking sector have to fill to reach an ideal and comprehensive maturity level, as well as the ranking of indicators based on this value. Also, Table 8 summarizes the ranking of Yemeni banks according to the average level of gap that each bank has to reduce to achieve a strong level of security.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

Table 7: The Ranking of Indicators by the Average Level of Gap Needs To Be Reduced By the Banking Sector

S	No of Banks with n - Level gap per indicator				AVG-Gap	Rank
	Single-Level	Double-Level	Triple-Level	Four-Level		
S1	6	4	1	0	1.55	4
S2	4	2	4	0	2.00	9
S3	10	1	0	0	1.09	1
S4	6	2	2	0	1.60	6
S5	5	4	0	0	1.44	3
S6	7	2	1	0	1.40	2
S7	5	1	0	1	1.57	5
S8	4	3	3	0	1.90	8
S9	3	4	3	0	2.00	9
S10	2	3	0	0	1.60	6

Table 8: The Average Level of Gap Needs To Be Reduced By Each Bank

B	No of Banks with n - Level gap per indicator				AVG-Gap	Rank
	Single-Level	Double-Level	Triple-Level	Four-Level		
B1	5	0	0	0	1.00	11
B2	3	0	1	0	1.50	6
B3	3	4	1	0	1.75	4
B4	4	0	0	0	1.00	11
B5	4	1	4	0	2.00	2
B6	2	6	1	0	1.89	3
B7	0	2	6	1	2.89	1
B8	5	4	0	0	1.44	7
B9	5	3	0	0	1.38	9
B10	4	0	0	0	1.00	11
B11	3	1	1	0	1.60	5
B12	6	4	0	0	1.40	8
B13	8	1	0	0	1.11	10

Q.5 Which of the indicators can be considered as future challenges? Are Yemeni banks' efforts to address them different?

According to the foregoing, all these indicators pose future challenges and security weaknesses that Yemeni banking institutions should address and take the necessary measures to address. However, in terms of the average gap that needs to be reduced for the sector's institutions, the amount of effort that Yemeni banks must make is different. Fig, 4 and Fig, 5 summarize these results.

ISSN 1533-9211

DOI 10.5281/zenodo.7307870

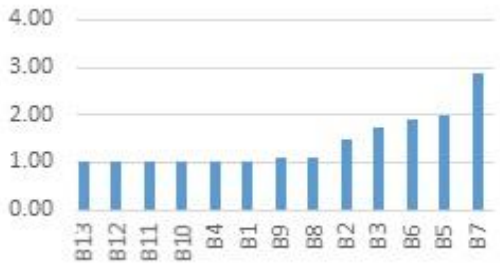

Figure 4:Ranking of banks by their average level of gap

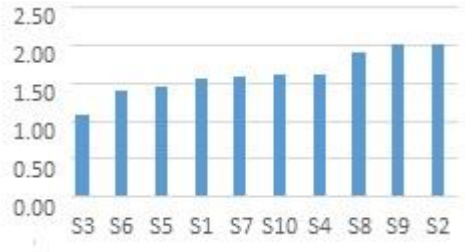

Figure 5:Ranking of indicators by the average level of gap needs to be reduced by the banking sector

Based on the foregoing, the present study has achieved the objective for which it was set. This research significantly contributed to bridging part of the research gap by providing general background that include concepts, theoretical foundations, and practical models needed to measure the level of security compliance in the fields of technology and innovation. It provides a comprehensive and detailed statistical report on the level of maturity and the extent of the applied gap in technology and innovation practices to Yemeni banks' information security management systems, and identifies the weaknesses of each institution in this sector. In addition, it identifies the applied gap averages that each bank must implement to reach an ideal security maturity level. The indicators are classified and arranged according to the banking sector's efforts. Banks were ranked according to the total average security gap each bank had to fill to reach a robust security maturity.

The provided by this study data, statistics, and recommendations, will help decision makers and stakeholders to adopt strategies, solutions, and policies that are commensurate with each bank's situation. As well as, detailed data and statistics on the classification of banks according to their security status and according to the average gap, each has to be reduced compared to the other banks, in particular, will assist banks in taking appropriate future strategies that enhance their ability to ensure their business continuity, earning the trust of their customers, enhance their competitive position, which contributes positively to maximizing the economy and reducing strategic losses. operational, moral, legal, and cyber risk reduction, which in its entirety will have a positive impact on strengthening the social responsibility of those institutions on the one hand,

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

and contribute to the achievement of economic, social, and legal development goals on the other hand.

VI. limitations, applications, and future work

This study only evaluated and assessed the degree of compliance and the applied gap in technological and innovative practices at the level of Yemeni banks in the country's capital, Sana'a, where researchers were given permission to conduct data collection activities. It also limited by building and developing use strategies and policies to address technological weaknesses at the banking level, as well as examining the level of compliance and the applied gap of other security aspects, such as risk management and information security, are among the main trends that researchers recommend.

VII. Conclusion

Yemen's banking sector represents the nervous system of the national economy and significantly contributes to its development and growth. These institutions rely on modern information systems and technologies to achieve strategic objectives. In addition, sectors institution's ability to protect the confidentiality, integrity, and availability of the information assets involved in these systems and to address their gaps and weaknesses through compliance with technology and innovation controls is a key factor in reducing the potential losses and risks of increasing cybercrime proliferation under the modern revolution. Therefore, this study aimed to examine and analyze the level of maturity in the technology and innovation practices of the Yemeni banks' information security management systems, with a view to diagnosing weaknesses, quantifying the applied gap and identifying future security challenges faced by institutions in the sector. Through the analytical-descriptive methodology adopted to achieve this goal, the study has drawn many conclusions, most notably: (1) The Yemeni banking sector only exercises the main requirements of the field of technology and innovation, with an average maturity level equal to (3.9), and a difference of one level from the ideal level. The study also found that (2) the seventh bank constitutes the weakest link among the institutions of this sector in terms of general maturity (2.4) and with a large application gap (2.6), it requires a very large effort and at the level of 90% of the field indicators (S1-S9). (3) 5th and 6th banks also constitute weaknesses in the banking sector, and are more likely to penetrate than other banks because of the large applied gap of at least two levels (1.8). They require a relatively large effort to reach the ideal level and address weaknesses in their practices, especially in those related to indicators (S2, S4, S6, S8, and S9). (4) The S2, and S9 indicators are the main weaknesses practices and are used at an average level of security. This means that the banking sector in general needs to look for appropriate solutions to improve the maturity level in the practice of the indicators to the fourth and fifth levels. Therefore, the study recommends: (1) The banking sector should strengthen its security practices through the use of modern and innovative solutions and commensurate with the normative controls of the strong level of security of the field of technology and innovation, (2) the seventh bank adopt technological and innovative strategies, policies and tools at the level of all technological indicators (3) the fifth and sixth banks adopt technology that reflects protection considerations in addition to adopting technical measures and

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

controls, registration and tracking of activities and the development of policies to implement encryption techniques and controls, as well as policies and mechanisms to validate and authorize access to the network in a manner that meets the requirements of strong security at the level of these practices (4) banking sector in general by adopting appropriate security practices to address the weakness of the second and ninth indicators as the most significant weaknesses by taking precise security considerations during the design phase of the systems, To meet the requirements of flexibility and innovation in security controls, it remained the use of sophisticated mechanisms to record and monitor applications, systems and networks on the one hand, to register and monitor all activities periodically on the other.

References

1. B. De La Hoz-Rosales, J. A. Camacho Ballesta, I. Tamayo-Torres, and K. Buelvas-Ferreira, "Effects of Information and Communication Technology Usage by Individuals, Businesses, and Government on Human Development: An International Analysis," IEEE Access, vol. 7, pp. 129225–129243, 2019.
2. O. S. Al-Mushayt, W. Gharibi, and N. Armi, "An E-Commerce Control Unit for Addressing Online Transactions in Developing Countries: Saudi Arabia—Case Study," IEEE Access, vol. 10, pp. 64283–64291, 2022.
3. S. O. A.- SHBIEl and N. H. A.- OLIMAT, "Impact of Information Technology on Competitive Advantage in Jordanian Commercial Banks. Accounting Information System Effectiveness as a Mediating Variable," International Journal of Academic Research in Accounting, Finance and Management Sciences, vol. 6, no. 3, Aug. 2016.
4. J. Li, J. Wang, S. Wangh, and Y. Zhou, "Mobile Payment With Alipay: An Application of Extended Technology Acceptance Model," IEEE Access, vol. 7, pp. 50380–50387, 2019.
5. S. Mehrban, M. A. Khan, M. W. Nadeem, M. Hussain, M. M. Ahmed, O. Hakeem, S. Saqib, M. L. M. Kiah, F. Abbas, and M. Hassan, "Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges," IEEE Access, vol. 8, pp. 23391–23406, 2020.
6. S. Trivedi, K. Mehta, and R. Sharma, "Systematic Literature Review on Application of Blockchain Technology in E-Finance and Financial Services," Journal of technology management & innovation, vol. 16, no. 3, pp. 89–102, Dec. 2021.
7. M. Uddin and D. Preston, "Systematic Review of Identity Access Management in Information Security," Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 150–156, 2015.
8. B. Jibril, M. A. Kwarteng, R. K. Botchway, J. Bode, and M. Chovancova, "The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory," Cogent Business & Management, vol. 7, no. 1, p. 1832825, Jan. 2020.
9. IBM Security X-Force, "X-Force Threat Intelligence Index 2022," IBM Security, 2022.
10. K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," Egyptian Informatics Journal, Mar. 2022.
11. R. A. Halaseh and J. Alqatawna, "Analyzing CyberCrimes Strategies: The Case of Phishing Attack," 2016 Cybersecurity and Cyberforensics Conference (CCC), Aug. 2016.
12. O. V. Sviatun, O. V. Goncharuk, C. Roman, O. Kuzmenko, and I. V. Kozych, "Combating Cybercrime: Economic and Legal Aspects," WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, vol. 18, pp. 751–762, Apr. 2021.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

13. Nasser, "Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies Sana'a Yemen," Int. J. Sci. Res. in Multidisciplinary Studies, vol. 3, no. 11, pp. 4–10, 2017.
14. A. Nasser, A. A. Al-Khulaidi, and M. N. Aljober, "Measuring the Information Security Maturity of Enterprises under Uncertainty Using Fuzzy AHP," International Journal of Information Technology and Computer Science, vol. 10, no. 4, pp. 10–25, Apr. 2018.
15. A. Nasser, , "Hierarchical Multilevel Information security gap analysis models based on ISO 27001: 2013," Int. J. Sci. Res. in Multidisciplinary Studies, vol. 3, no. 11, pp. 14–23, 2017.
16. A. Nasser, N. K. A. Al Ansi, and N. A. Al Sharabi , "On The Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen," Int. J. Sci. Res. in Computer Science and Engineering, Vol 8, No. 6, pp 8-18, 2020.
17. N. I. Ngwum, " Information Security Maturity Model (ISMM). ," Diss., The University of Manchester., 2013.
18. Насер, А. А., & Гуламов, А. А. (2010). Модель процессов информационно-аналитического обеспечения научных исследований технического вуза. In Современные проблемы образования: материалы науч.-техн. конф. Курск (pp. 93-95).
19. А. Насер, "Информационно-аналитическое сопровождение и информационное моделирование процессов принятия решений в различных подсистемах ВУЗа, "Современные научные исследования и инновации, (8), 4-4. 2011
20. A.S. A. Alghawli, A. A. Nasser, and M. N. Aljober, "A Fuzzy MCDM Approach for Structured Comparison of the Health Literacy Level of Hospitals," International Journal of Advanced Computer Science and Applications, vol. 12, no. 7, 2021.
21. A. Nasser, A. A. Alkhulaidi, M. N. Ali, M. Hankal, and Al-olofe M., "A Weighted Euclidean Distance - Statistical Variance Procedure based Approach for Improving The Healthcare Decision Making System In Yemen," Indian Journal of Science and Technology, vol. 12, no. 3, pp. 1–15, Jan. 2019.
22. Снопков, В. Н., Насер, А. А., & Иванов, А. В. (2012). Нейросетевое моделирование и математические алгоритмы в дифференциальной диагностике диабетической ретинопатии. Известия Юго-Западного государственного университета, (2-1), 50-57.
23. Томакова, Р. А., Серебровский, В. В., Шульга, Л. В., & Насер, А. А. (2012). Спектральные технологии морфологического описания сегментов в задачах классификации сложноструктурируемых изображений. Известия Юго-Западного государственного университета, (1-1), 22а-28
24. Бобырь, М. В., Нассер, А. А., & Абдулджаббар, М. А. (2016). Исследование свойств мягкого алгоритма нечетко-логического вывода. Известия Юго-Западного государственного университета, (1), 31-49.
25. A. Nasser, M. M. Saeed, and M. N. Aljober, "Application of Selected MCDM Methods for Developing a Multi-Functional Framework for Eco-Hotel Planning in Yemen," International Journal of Computer Sciences and Engineering, vol. 9, no. 10, pp. 7–18, Oct. 2021.
26. Mohammed M Said, Adel A Nasser and Abdualmajed A Alkhulaidi, " Prioritization of the Eco-hotels Performance Criteria in Yemen using Fuzzy Delphi Method,". International Journal of Applied Information Systems 12(36):20-29, March 2021.
27. Насер, А. А. (2012). Концепция построения информационной системы вуза на основе структурно-функционального анализа информационных потоков. Вестник АПК Верхневолжья, (1), 81-85.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

28. Насер, А. А. (2011). Информационно-аналитическое сопровождение и информационное моделирование процессов принятия решений в различных подсистемах ВУЗа. Современные научные исследования и инновации, (8), 4-4.
29. S. A. Alghawli, Al-khulaidi Abdualmajed A., A. A. Nasser, N. A. AL-Khulaidi, and F. A. Abass, "Application of the Fuzzy Delphi Method to Identify and Prioritize the Social-Health Family Disintegration Indicators in Yemen," International Journal of Advanced Computer Science and Applications, vol. 13, no. 5, 2022.
30. M. Khalil, K. F. Khawaja, and M. Sarfraz, "The adoption of blockchain technology in the financial sector during the era of fourth industrial revolution: a moderated mediated model," Quality & Quantity, Sep. 2021.
31. E. A. Lauren, "The Fourth Industrial Revolution in Banking Sector: Strategies To Keep Up With Financial Technology," SSRN Electronic Journal, 2021.
32. X. He, D. Xiong, W. M. S. Khalifa, and X. Li, "Chinese banking sector: A major stakeholder in bringing fourth industrial revolution in the country," Technological Forecasting and Social Change, vol. 165, p. 120519, Apr. 2021.
33. J. Kimani, "INFLUENCE OF INFORMATION TECHNOLOGY ON THE BANKING SECTOR," Journal of Technology and Systems, vol. 3, No. 1, pp 48-61, 2021.
34. Khalid and M. Kot, "The Impact of Accounting Information Systems on Performance Management in the Banking Sector," IBIMA Business Review, pp. 1–15, Aug. 2021.
35. L. Zherdetska, Y. Diatlova, V. Diatlova, J. Derkach, A. Goncharenko, and M. Zos-Kior, "Digital banking in the marketing mix and human resource management: improving the approach to the assessment as an innovative component," LAPLAGE EM REVISTA, vol. 7, no. 3A, pp. 111–119, Sep. 2021.
36. S. T., Shashank Bharadwaj, Dr. Sunil Joshi, "A Study of Impact of Cloud Computing and Artificial Intelligence on Banking Services, Profitability and Operational Benefits," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 6, pp. 1617–1627, Apr. 2021.
37. N. H. Al-Fahim, R. Abdulgafor, and E. H. Qaid, "Determinants of Banks' Costumer's Intention to adopt Internet Banking Services in Yemen: Using the Unified Theory of Acceptance and Use of Technology (UTAUT)," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), Jul. 2021.
38. E. Suandi, H. Herri, Y. Yulihasri, and S. Syafrizal, "An empirical investigation of Islamic marketing ethics and convergence marketing as key factors in the improvement of Islamic banks performance," Journal of Islamic Marketing, Apr. 2022.
39. M. Mutahar, A. Aldholay, O. Isaac, A. N. Jalal, and S. Alkibsi, "Predicting Intention to Use Mobile Banking Services among Yemeni Banks' Clients: Is Perceived Value Important?," Lecture Notes in Networks and Systems, pp. 498–520, Aug. 2021.
40. M. A. S. Al-Muhrami, N. A. Alawi, M. Alzubi, and A. A.-A. Al-Refaei, "Affecting the Behavioural Intention to Use Electronic Banking Services Among Users in Yemen: Using an Extension of the Unified Theory of Acceptance and Use of Technology," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Jun. 2021.
41. J. Hadi, W. Huafei, M. Khan, M. Abdulrab, and Z. Yan, "THE IMPACT OF MOBILE BANKING APPLICATION ON CLIENT INTERACTION WITH YEMEN BANKS," International Journal of Business Strategies, vol. 6, no. 1, pp. 58–68, Jun. 2021.
42. Gogolin, Fabian, Ivan Lim, and Francesco Vallascas. "Cyberattacks on Small Banks and the Impact on Local Banking Markets." SSRN Electronic Journal,2021
43. N., Tariq, "Impact of cyberattacks on financial institutions." Journal of Internet Banking and Commerce, vol. 23, no. 2, pp. 2018. 2018.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7307870

44. S. Acharya, and S. Joshi "Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures." PalArch's Journal of Archaeology of Egypt/Egyptology, vol. 17, no. 6, pp. 4656-4670,2020/
45. Mussmann, M. Brunner, and R. Breu, "Mapping the State of Security Standards Mappings," WI2020 Zentrale Tracks, pp. 1309–1324, Mar. 2020.
46. P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Feb. 2020.
47. Shojaie, H. Federrath, and I. Saberi, "Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A," 2014 Ninth International Conference on Availability, Reliability and Security, Sep. 2014.
48. Al-Mayahi, and P. M. Sa'ad, "Iso 27001 gap analysis-case study," In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012