The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

INFORMATION SECURITY GOVERNANCE: AN EXPLORATION STUDY OF YEMENI BANKS' INFORMATION SECURITY MANAGEMENT SYSTEMS

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

[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.
[*]Corresponding author: adel@saada-uni.edu.ye

Abstract

This study aims to analyze the fundamental governance practices of Yemeni banks' information security management systems (ISMS). Therefore, an empirical investigation was performed to define the information security governance (ISG) maturity of banks and make recommendations that allow their administrations to improve security and reduce risks to their businesses. This study uses a mixed qualitative and quantitative approach, convenience sampling, and data collection from 26 experts and specialists in banking information security, in a total of 13 government and commercial banks through a survey. This study adopted Ngwum's maturity framework to develop the study's instrument. It provides empirical insights and identifies the strengths and weaknesses of Yemeni banks' information security management systems' ISG practices. The general level at which bank systems implement ISG requirements was found to be the average basic security maturity level. The results demonstrate that practices at the level of information security management, training, and awareness are the strengths of banks' ISMSs, whereas those of the role and responsibility factors constitute a significant weakness. This study meets the needs identified to assess ISG maturity, includes a detailed discussion on banks' and ISG indicators' strengths and weaknesses, and their implications, and provides the required recommendations. Moreover, these recommendations may help stakeholders in banks formulate more appropriate policies or provide a more effective focus on ISG controversies that are needed to improve the information security situation and reduce the estimated gap in their practices.

Keywords: Bank, Governance, Information security assessment, Maturity, Yemen

1. Introduction

Today's modern industrial revolution has had a significant impact on business performance of and has prompted significant changes in business execution methods and the creation of numerous investment opportunities in many sectors, including the financial sector. In this regard, a study [1] found that the advancement of modern ICTs is closely linked to the sector's development and performance and to its economic profits and benefits. Also, [2] indicates that modern information systems and technologies contribute significantly to the achievement of countries' development goals, allowing the provision of services that meet the needs of the population, promoting equitable and comprehensive access to services, and creating jobs,

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

especially in remote areas, that help better manage and invest resources. For this reason, the issue of coverage of modern digital technology by financial institutions in the Republic of Yemen has become one of the current government's major economic development trends.

However, despite the importance of modern ICT in achieving financial institutions' business objectives and achieving states' sustainable development goals, their poor use and lack of commitment to their protection controls make them vulnerable to ever-increasing cyber risks and threats [3], for many reasons, including that technology, however modern it may be, cannot be fully assured, the number of people engaged in threatening behavior is increasing globally [4], and the assets possessed by financial institutions are of great importance and contain sensitive and highly confidential data, which makes them a significant motive for theft, extortion, hacking, and phishing by cybercriminals [4]. According to many studies, risks to financial institutions contribute significantly to strategic, operational, moral, and legal losses [5]. Study [6] adds that these risks may lead to a loss of trust in an enterprise's systems, affecting its reputation and customer relationship with it.

According to research [3], [7], the successful application of modern information technologies and systems in the financial sector must be accompanied by technological and organizational changes that meet the business's needs and requirements. According to these studies, technological and organizational changes must meet the needs of customers and stakeholders in maintaining confidentiality, integrity, and availability of information, which constitute the three main principles of information security [8-9]. Many recent studies have highlighted the role of the application of information security mechanisms, techniques, and policies in enhancing information security in financial institutions [10-16], helping maintain its confidentiality, integrity, and availability as a key factor in winning customer confidence and enterprises' business continuity [17]. Authors [18] state that compliance enables enterprises to successfully achieve their objectives and reduces the level of threats to enterprise information systems and technologies [18], thereby maximizing the commercial and development benefits and returns of technology in enterprises [17].

From this point of view, the application of good practices to protect the security of financial institutions' information systems is of the utmost importance in order to achieve the objectives of the institutions and enhance their sustainable role. However, the question of "How far do Yemeni banks comply with the security requirements and controls to ensure that they do so?" remains unanswered, with the exception of some partial attempts. One local study has been carried out in this regard to contribute to addressing this problem [12]. It aimed at analyzing the level of compliance and identification of the gap in the practices applied in the field of security operations and procedures in Yemeni banking institutions.

However, although these studies have made significant contributions to identifying weaknesses in information security operations and procedures and in the area of technology and innovation, there is still a local theoretical and applied research gap in addressing this problem in terms of information security governance. This is why we hope to supplement previous efforts with this research by examining and analyzing the level of compliance of Yemeni banks' information security management systems with information security governance controls, identifying

ISSN 1533-9211

DOI 10.5281/zenodo.7304003

technological strengths and weaknesses in their practices, and providing appropriate solutions and remedies to reduce the applied gap in those practices.

The remaining parts of this study review its theoretical and practical contents as follows: Part II contains a brief overview of previous security governance studies, including ISG concepts, relevance, controls, frameworks, and measurement models. Parts III contains both methods and tools for data collection and analysis. This is followed by the results and their discussion, whereas the final part summarizes the study's main conclusions and recommendations.

2. literature review

2.1 Assessment of information security in banking sector

Currently, decision support, data mining, and artificial intelligence tools and techniques have become a key part of business information systems and are heavily relied upon in management decision-making at all levels in all sectors [19-24], Modern technology plays a vital role in achieving countries' development goals, particularly in the area of financial development. The study [1], which aimed to study the impact of technology development and innovation on the financial development of a group of seven emerging economies between 1990 and 2017, found that technological innovation is one of the important variables affecting financial development and that there is a long-term relationship between them. The study [2] discussed recent technological and innovative developments used in the financial sector and their contributions to the achievement of the objectives of this vital sector. This study found that modern technology effectively contributes to the achievement of countries' sustainable development goals and to the promotion of their future sustainable actions. A study [6] found that there are many risks associated with the application of this technology. Such risks could lead to a loss of confidence in accounting information and material misstatement. Besides, they can cause damage to financial institutions' reputations and relationships with their customers. IT surveillance, security, and protection are critical to achieving the objectives of the banks that apply them.

According to previous studies and other similar studies [4], [12], [14], [16], these risks pose a threat to banks globally. The study [17] indicates that the risks to which banks may be exposed can be classified into four types: (1) strategic risks arise from the failure to adopt appropriate strategies for the use and management of technology to ensure the provision of sophisticated services in a manner that does not affect the company's competitive position and strategic plans in the future, (2) operational risks, such as the technical problems encountered by systems during their operation as a result of the lack of business continuity capability at the operational level , most notably, the risks of inefficient systems, the intentional or unintentional misuse of technology, and the failure to provide adequate and adequate protection to the bank's systems, making them intrusive. (3) Reputational risks resulting from the availability of a negative opinion resulting from the failure to provide an excellent service according to standards of safety, confidentiality and accuracy, and (4) legal risks resulting from the lack of clear identification of rights and obligations, or as a result of non-compliance with domestic and international laws, especially under privacy protection laws.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

By analyzing the findings of this literature, Yemen's banking sector, like other international financial sectors, can be said to be one of the forces of domestic development and economic growth and must rely on modern technology for its work. In addition, the information assets he possesses are a major factor in the success of his institutions and the continuity of the services and businesses they provide. It will continue to be vulnerable to cyber-attacks and cyber hazards like other banks around the world if you do not adopt appropriate protection policies and strategies, and if you do not provide and use appropriate protection tools according to global standards.

Researchers state [6] that financial sectors that operate in a traditional way need not only to adopt appropriate technological solutions to improve their services but also to make appropriate changes so that they can enhance the protection of their information assets. Another study [7], which addressed the requirements of this digital transition in financial sector institutions, concluded that the application of this technology must be accompanied by many technological, organizational, and cultural changes and must meet all stakeholders' needs. It also found that information security, ensuring the confidentiality, integrity, and availability of information, is one of the key needs sought by stakeholders. Numerous studies have also addressed the topic of assessing maturity level and identifying the gap using the ISO 27001 standard, such as [8-9],[25]. Previous literature has also found that adherence to normative controls for the protection of information security, through the application of strategies and solutions, and the building and implementation of appropriate use policies for enterprise information technology and systems, is the first and main step for risk reduction.

In any case, controls on information security practices can be classified into four main areas, namely, processes and procedures; technology and innovation; security governance and risk management [25]. The study [12] reviewed the importance and role of process, and procedure controls in enhancing information security in Yemeni banks, as well as the list of key factors and indicators of these areas, based on the general framework proposed by [25], with the participation of a group of local experts, and accordingly conducted an analytical study to determine the level of maturity and identify the gap in the related practices. So, it should also be noted that that study extensively reviewed the general theoretical background they share with this study, including the role of information security in the domestic banking sector, the challenges and risks of information security in the Yemeni banking sector, the importance of information security standards and controls in general in reducing security risks, and ISO 27001 in particular, the classification models of information security controls.

2.2 Information Security Governance

Information security governance, like other branches of information security, is an important topic for enterprises and plays an important role in protecting the data and information of enterprises [26], which form the fundamental building block of different administrative decision-making processes [27-31] and in protecting other information assets that are an important factor for the creation and survival of institutional value and excellence [32]. Many definitions of information security governance have been given in the literature. For example, it is defined by [33] as a set of processes through which information security issues can be

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

addressed at the higher administrative level of an enterprise. Similarly, it has been defined by [26] as the set of activities that define mechanisms for the participation of different departments and at all institutional levels in addressing those issues. It is also defined as the development, provision, and maintenance of the appropriate environment for control, provision of supporting systems and processes in order to achieve the key principles of information security [34].

Although there are many definitions in the literature, there is an overall agreement that: (1) Information security governance necessitates the execution of numerous processes and activities, including planning, policy and strategy development, management, control, coordination, and others. (2) Its processes are geared toward achieving the security institution's goals, which are to protect the confidentiality, integrity, and availability of the institution's various information assets; in other words, they should be aligned with the goals of information security management. (3) The achievement of these objectives requires management and coordination of all relevant information security departments. (4) Top management must understand its role, its responsibilities in planning and coordination, and its responsibility in providing and implementing everything that helps or promotes the achievement of those goals. (5) Other departments are also responsible for adhering to all policies and regulations issued by the top management.

3. Methodology

This study was carried out in three main phases (see Fig.1): the review of literature; the identification of methods and tools for collecting, processing, and analyzing information; the assessment and analysis of maturity levels; and the gap in information security governance practices as follows:

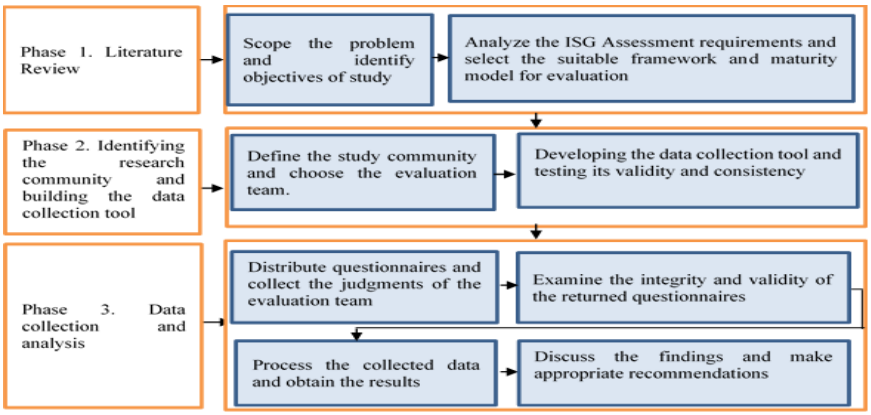

Figure 1: Research methodology

3.1 Phase I: Literature Review.

At this stage, studies relevant to the topic of the study have been studied and analyzed to emphasize the importance of the topic while identifying the main opportunities and challenges associated with the application of information security requirements in general, information security governance in particular, analysis and review of evaluation frameworks, and models.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

Based on this stage the suitable framework for ISG evaluation, and the appropriate maturity model for measuring it were selected.

A. Select the suitable Framework for ISG evaluation

The current study relied on a three-dimensional framework, which has been proposed by [25], which covers the factors of information security management, training and awareness programs, and roles and responsibilities. This choice can be justified as follows: (1) It provides a comprehensive framework for measuring information security not only at the level of governance but also at the level of three other dimensions. As previously stated, (2) it was developed in accordance with the ISO 27001-2013 standard, which is the most widely used security standard in Yemeni banking institutions; and (3) it combines multiple security requirements and controls into a shortlist that reflects all security requirements and controls, including governance requirements. (4) A hybrid model (quantitative and qualitative) was proposed to measure maturity in security practices at the level of all its constituent domains, including the governance domain. Furthermore, (5) in the same research community, this framework has been used to assess maturity and the applied gap in technological and innovation areas as well as in the domain of processes and procedures. Which means that 50% of practices have been studied and analyzed, and appropriate proposals and recommendations have been made to address them. Thus, the use of the same framework will help to complement previous efforts to solve the problem and help researchers avoid repeating the analysis of security factors and indicators that may be classified in another context as governance factors, while in this framework, they can be viewed as an individual domain. On the other hand, its selection will assist banking institutions and researchers in this study, as well as other researchers, in comparing the outputs and results of the current study with the outputs of previous research and will help them in the future to complete the study and analysis of the practices of the fourth unaddressed security domain (risk management domain), in order to achieve integrated outputs obtained through the application of one methodology, based on one framework and one measurement model, covering all aspects and requirements of one international standard to solve problems in one banking environment.

B. ISG practices in accordance with the proposed framework.

According to the foregoing, to evaluate the ISG in the organization, the practices of the ISMS of banks on the main three factors of security governance should be examined, namely, information security management; training and awareness programs; and roles and responsibilities. According to [35], an effective information security program in any organization must be comprehensive in terms of strategy and administrative support. This means that senior management at the institution must be aware of its role and responsibilities while remaining supportive of the strategic plans. Authors in [25] consider that this is not enough to reach an ideal maturity level at an important level and stress that it must be convinced that information security is an enabler of business and support the development and implementation of detailed security strategic plans to ensure information security. The study [30] also emphasizes that the senior management support factor, like other security responsibilities distributed to different units, requires appropriate mechanisms for integration, coordination, and

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

commitment between different units.

From a strategic perspective, [36] believes that governing bodies and senior executives must be fully involved at the governance level in order to ensure the security and integrity of institutional assets and resources, which requires them to guide management and control-related processes. Recent studies in the field of information security, such as [37], emphasize a relationship between it and information security governance and culture, and consider that the senior management of the enterprise should develop clear security policies and exercise a policy of reward and punishment to effectively achieve and disseminate the enterprise's culture of information security.

Also, the study [38] stresses that the development and practice of these policies by senior management encourages employees to comply with the organization's security controls, policies, and regulations and helps them reduce their risk of non-compliance with them. Other studies such as [25],[39] confirm that the institution cannot achieve an ideal maturity level at this sub-level of governance if there are no comprehensive policies covering all areas of business and all legal and security requirements. According to these studies, policies must be updated and reviewed continuously and proactively if the institution wants to achieve an ideal maturity level, and they must be reviewed continuously and proactively. A study [25] found that updating the list of all institutional assets and the list of relevant owners in real time and constantly reviewing them in line with changes in the working environment are key factors in the effectiveness and maturity of information governance security. In addition, institutions' activities in general and financially in particular involve internal and external transactions involving contracts and agreements with other external parties. Numerous studies such as [18], [35] have found that failing to consider information security issues in all aspects, activities, and internal and external plans can have a negative impact on governance performance. In addition, effective governance of information security requires not only compliance with requirements and controls of information security management but also the identification, distribution, and management of the roles and responsibilities assigned to users [26], [32], as well as the provision of appropriate training and qualification programs to comply with them [36]. This is because the roles, responsibilities, and functions assigned to users vary from user to user, and the requirements and needs of qualification also vary and are constantly changing, on the one hand. On the other hand, the distribution of those roles and responsibilities and the development of strategies that enhance the selection and screening of eligible users as well as enhance the level of compliance with the ISG requirements must be carried out by a competent department with the active participation of representatives of the relevant departments.

3.2 Phase 2: Identify the research community and build the data collection tool

A. Define the study community and choose the evaluation team.

In this step, the researchers conducted preliminary interviews with the administrations of all 17 local banks in Yemen's capital, Sana 'a, to obtain their approval for the study on the information security management systems owned by these institutions. Institutions that did not agree to participate in the study for reasons, justifications, and acceptable security and organizational

ISSN 1533-9211

DOI 10.5281/zenodo.7304003

considerations were excluded at the end of this phase. Thus, the actual community of study was identified, representing 76% of this sector's institutions. Furthermore, because the study community is small and each institution's information security specialists are limited (37), researchers used a comprehensive survey method to collect data by surveying all specialists authorized to answer research questions in all institutions under study. Table 1 summarizes the abbreviation scheme of the financial institutions under study, while the distribution of the evaluation team members according to their institutions is illustrated in Fig. 2.

Table 1: Abbreviations used for coding the study community

Bank	Sign.	Bank	Sign.
The Yemen Bank For Reconstruction And Development	RDB	Yemen Commercial Bank	YCB
The National Bank of Yemen	NBY	Islamic Bank of Yemen	IBY
Housing Credit Bank	HCB	Tadhamon Bank	TB
International Yemen Bank	IYB	Saba Islamic Bank	SIB
Yemen Kuwait Bank	YKB	Shamil Bank of Yemen & Bahrain	SB
Cooperative & Agricultural Credit Bank	CAC	Qatar National Bank	QNB
Rafidain Bank	RB		

B. Developing the data collection tool

This step was concerned with the creation of a clear and concise assessment tool (questionnaire) that satisfies the methodological requirements for the development of questionnaires in terms of both validity and consistency. In order to arrive at a clear and valid tool, researchers first translated the proposed maturity measurement framework [25] from English into Arabic. It includes 11 questions (indicators) distributed across three main ISG areas, reflecting the three main assessment factors of ISG. After that, this initial tool was emailed to a list of 15 experts. The main demographic characteristics of them are presented in table 2.

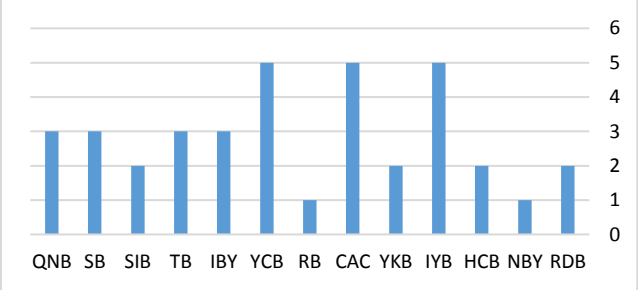

Figure 2: Distribution of evaluation team members

However, experts were asked to provide feedback on the tool's face, content, and construct validity. The purpose of face validity is to ascertain whether the overall appearance of the tool indicates that it measures maturity in information security governance practices. And, the purpose of content validity is to ensure that the quantitative indicators and measures used in this tool are appropriate for measuring ISG maturity in the Yemeni banking sector. While the

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

purpose is to determine whether these factors and indicators encompass all aspects of evaluation, in any case, the results were positive, and the tool was assessed as a valid tool, with some modifications recommended. Accordingly, experts' opinions and observations were taken into account in the process of developing the final version of the questionnaire, which consisted of the demographic data and the assessment sections. Each question has a specific set of options; each of them represents a level of maturity measurement out of five levels. (See table 3), where the evaluators are asked to identify and select the choice that reflects the organization's actual maturity on the indicator measured by each question. The choice number one (1) in the response options represents the weak level of security (WS), gradually rising to five, as shown in table 3. Table 4 summarizes questionnaire questions and evaluation options.

C. Consistency test

Cronbach's alpha coefficient was used to calculate the credibility and stability rates. A very high stability rate (91%), and a very high credibility ratio (95 %) were observed. This means that the tool can be disseminated to the study community and can be used in practice to collect data, as shown in the next sub section.

Table 2: The Demographic Characteristics of Exports

	Class	**Number**	**%**
Type of work	Academic	12	80%
	Non-academic	3	20%
Specialization	Information Security	4	27%
	Computing	6	40%
	Statistics and Scientific Research	5	33%
Place of work	Higher education	12	80%
	Financial sector	3	20%
Experience	5- 10 years	3	20%
	More than 10 years	12	80%

Table 3: The maturity assessment model.

Level	**Verbal expression (VE)**	**Abbreviation**
1	Weak Security	WS
2	Security Awareness	SA
3	Basic Security	BS
4	Meets the requirements	MR
5	Robust security	RS

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

Table 4: ISG statements and their maturity levels of implementation

Id	IS Management	ISG statements and their maturity levels of implementation
1	IS Management	
1.1	Senior management recognizes its role in ensuring IS:	1. It is unconcerned about the value of IS to business. 2. It recognizes but does not support the importance of IS for business. 3. It recognizes its roles and responsibilities and supports IS plans. 4. In senior management's view, IS is a business enabler and detailed plans are being implemented to ensure effective IS. 5. In senior management's view, IS is an essential part of the work
1.2	Your organization has a detailed security policy:	1. There is no policy in place. 2. Only verbal instructions. 3. There is a manual containing non-exhaustive security procedures. 4. There is a detailed policy covering all areas of business and all legal and security requirements. 5. There is a comprehensive policy that is constantly and proactively updated and reviewed.
1.3	The Foundation's information assets are identified and documented:	1. Assets are not inventory, and no owners have been assigned to them. 2. Although the asset list exists, there is no proper inventory of assets with their respective owners in accordance with the changes. 3. The asset list exists, but it is not kept up to date. 4. The list of assets that includes all relevant assets and owners is updated. 5. Inventory records are updated in real time, allowing asset owners to be tracked and proactive information asset protection to be provided.
1.4	Data and information are classified in your organization:	1. Information is not classified. 2. Information is classified informally. 3. Information is classified mainly according to value and sensitivity. 4. The information is classified in detail and an appropriate level of protection is allocated to each category. 5. The classification of information assets is constantly reviewed in line with changes in the working environment, and new assets are classified as they arise.
1.5	Users have abused the authority to access information:	1. Several cases per day. 2. A maximum of one case per week. 3. A single case per month. 4. There is only one case per year. 5. These cases are rare
1.6	IS is a major consideration in all of the institution's plans and dealings with external parties:	1. IS is not taken into account in all transactions. 2. The importance of IS for all business activities and communications is recognized. 3. IS is taken into account during all transactions. 4. IS is incorporated into all aspects of activities and plans, and agreements with external parties' detail IS requirements. 5. IS is an integral part of the enterprise's business, and all transactions are monitored and reported, and the deviations from security requirements agreed with external parties are corrected.
2	Training and awareness programs	
2.1	Your organization has training and awareness programs in the field of IS:	1. There are no awareness-raising or training programs. 2. There are no officially sanctioned programs, but there are some initiatives. 3. There are annual public awareness and training programs. 4. Needs assessment and training courses are provided in accordance with users' work requirements. 5. The Board supports IS awareness programs, and regular training courses are provided according to needs.

ISSN 1533-9211

DOI 10.5281/zenodo.7304003

2.2	Level of awareness and compliance with IS requirements:	1. There is no understanding or compliance among users. 2. There is awareness but no compliance. 3. The level of compliance is poor. 4. Complete compliance. 5. Compliance is proactively carried out.
3	Roles and Responsibilities	
3.1	There is an IS unit, and the directors of the IS unit assign roles and responsibilities:	1. The IS Unit does not exist, and roles and responsibilities are not defined at all. 2. There is no separate unit as IS functions are part of the IT Section's mission. 3. The IS Unit exists, but it is not fully aware of or performing its responsibilities. 4. A well-functioning information security unit and IS managers delegate specific roles and responsibilities in accordance with policy and standards. 5. Roles are constantly monitored, reviewed, and reset in line with users' roles to ensure the highest security performance.
3.2	Security tests are conducted on those eligible for key positions in your organization before granting them the IS roles	1. The need to screen or test users is not taken into account. 2. Users' efficiency and credibility are not formally checked. 3. Users' efficiency is verified without adopting a documented formal approach and manual. 4. There are detailed formal procedures in place to ensure the integrity and efficiency of users and contractors. 5. Users' and contractors' capabilities and activities are constantly reviewed to ensure a high level of information security.
3.3	The Foundation's departments are aware of and co-coordinate IS requirements:	1. There is no awareness in the relevant departments. 2. Departmental key representatives are aware of information security. 3. Representatives from relevant departments are involved in IS coordination. 4. A team of department heads, managers, auditors, and others promotes an IS culture among employees in various departments. 5. A team of representatives from various departments continuously improves and implements security strategies to ensure full compliance with all specific processes, policies, and standards.

3.3 Phase 3: Data collection and analysing.

A. Distribute questionnaires and collect data

At this step, a number of thirty-seven questionnaires were sent by email to the determined assessment team members. However, a total of 31 questionnaires were returned, while a small percentage, not exceeding 17%, of them were not sent back.

B. Examine the integrity and validity of the returned questionnaires

At this step, a number of thirty-one returned questionnaires were tested. At the end of this phase, five questionnaires were rejected due to a lack of acceptance criteria. Table 5 provides statistics on the questionnaires sent, returned, and accepted for future processing and analysis, while Table 6 shows the demographic characteristics of the evaluators whose views have been accepted.

C. Process the collected data and obtain the result

The assessment framework used by this study is limited by the number of three ISG factors. Each factor has a limited number of measurement indicators. So, to determine the security maturity index implemented by a certain financial organization's ISMS at the level of each

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

indicator, the maturity measures reflecting the opinions of all respondents affiliated with that organization on each of those indicators were aggregated. After that, for each factor, the aggregated maturity indexes of indicators were averaged to determine the average maturity index values implemented by each organization's ISMS for each ISG factor, AMI (F). In the same way, the overall ISG maturity index for each organization's ISMS (AMI (O)), as well as the general overall maturity index of the entire banking sector, which represents the average maturity values achieved by all its information security management systems (OMI), are defined. Then, using the maturity model recommended by [25] (see table 3), the maturity levels representing the previously determined indexes were defined. Finally, a value of 3.4 out of five overall maturity indexes (OMI) was estimated, with a value of 1.6 overall applied gap. Accordingly, the estimated overall ISG maturity level implemented by the Yemeni banking sector's ISMS is 3. This level is known as "Basic Security Level (BS)," which means that banks only adhere to the key requirements of ISG. The results of this step are summarized in Tab. 7, and they will be discussed in detail in the following section.

Table 5: Distribution of questionnaires to the study community

Status	RDB	NBY	HCB	IYB	YKB	CAC	RB	YCB	IBY	TB	SIB	SB	QNB
Sent	2	1	2	5	2	5	1	5	3	3	2	3	3
Returned	1	1	1	4	2	5	1	3	3	3	2	2	3
Excluded	0	0	0	1	0	2	0	0	0	1	1	0	0
Accepted	1	1	1	3	2	3	1	3	3	2	1	2	3

Table 6: The demographic characteristics of respondents

	Gender		Qualification		Specialization (Computing)					Job		
	Male	Female	Bachelor	Master	IT	Computer Eng. / Networking	Computer Science	IS	Others	Director/ Dep. director of IT	Head of IS dep.	IS Specialist / Engineer
N	23	3	21	5	5	9	4	4	4	5	6	15
%	88%	12%	81%	19%	19%	35%	15%	15%	15%	19%	23%	58%

Findings and their Discussion

The final results reached through the application of the proposed methodology (see tab. 8) indicate that Yemen's banking industry utilizes ISG security measures, processes, and techniques with an average total of 3.4 out of 5 and a maturity level of three. These results show that Yemen's banking industry, in general, fulfills only the basic security requirements, retains robust ISG needs, and yet still must bridge a typical gap of (0.1) to fulfill the requirements of the fourth ISG maturity level and close an average application gap of roughly two levels (1.6) to completely strengthen its ISG practices to meet the requirements of the robust ISG maturity level. These findings also indicate that a small proportion of financial organizations (7.7 %) apply the ISG requirements at an ideal robust maturity level, versus a large number of organizations that make up (92.3 %) of the total organizations, in which these requirements are implemented at the second, third, and fourth ISG maturity levels.

At the fourth maturity level, half of this percentage (6 banks) practices the aforementioned requirements, indicating that information security management is intimately engaged; security

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

investments seem to be well planned, put in place, and evaluated against achievement; employees' adequate training and competence are checked and upgraded; and risk holders are nominated and continuously redirected to accomplish security goals. At the third and second maturity levels, the other half of this percentage (6 banks) exercises the above requirements at a rate of 2:1, indicating that only 30.76 % of bank executives recognize their responsibility to ensure security and collaborate to engage and make the required attempts to do so; an anniversary security and training programs are taken into account; and holders of information assets understand and uphold their responsibilities regarding their assets. And that only 15.38 percent of these executives recognize the importance of information security to business but at a non-supportive level; their banks' awareness programs are weak and are not supported by effective employee training; and responsibilities and duties are clarified but not strictly.

So, to reach an ideal maturity level, all banks, except the "IYB" bank, should take the necessary administrative measures, appropriate and proactive methods, and proper mechanisms for the distribution of security roles and responsibilities in a manner that contributes positively to a high level of security among institutions, making the issue of information security an essential and integral part of the management of those institutions' business, enabling organizations to ensure a high level of security awareness among staff, reduce the risks of information assets, and enhance their protection..

Talking on the adherence of financial institutions to the ISG controls' requirements it can be seen that the level of banking institutions' application of ISG requirements varies in general from one bank to another. However, these banks can be arranged according to their overall ISG maturity index as: (IYB > QNB> RDB >TB > NBY > SB > YKB > CAC > HCB > YCB > SIB > IBY > RB). Fig. 3 shows the values of the overall maturity indexes (MI) and the overall gap indexes (GI) defined as the absolute value of the difference between these values (MI) and the desired ideal ISG maturity level (EML = 5).

Table 7: Results of study

		RDB	NBY	HCB	IYB	YKB	CAC	RB	YCB	IBY	TB	SIB	SB	QNB	AMI	AML
Measurement indicator	F1.1	4.3	5	3	5	4	3.3	2	1.7	3	5	2	4	5	3.6	MR
	F1.2	5	4	3	5	4	3.3	3	4.3	3	5	2	2	5	3.7	MR
	F1.3	4.3	4.5	5	5	4	4	3	2.3	2	4.7	4	5	5	4.1	MR
	F1.4	4	3	4	5	3	3.7	3	1.7	2	4	3	4	4	3.4	BS
	F1.5	3.3	5	5	5	5	4.3	2	4	2	5	2	5	5	4.0	MR
	F1.6	4.7	4.5	2	5	5	3.7	2	1.7	3	5	2	5	5	3.7	MR
	F2.1	4.3	5	3	4	4	2.3	2	3	2	4	2	5	5	3.5	MR
	F2.2	4.3	3.5	4	4.5	4	4.3	2	2.3	3	4	4	4	4	3.7	MR
	F3.1	4	3	2	4.5	2	2	1	3.7	1	4	2	5	2	2.8	BS
	F3.2	4.3	4	3	5	3	2.7	1	2	2	4.7	1	1	4	2.9	BS
	F3.3	4.7	3	2	4.5	3	3.7	2	1.7	2	3	3	3	5	3.1	BS
Factor	F1	4.3	4.3	3.7	5.0	4.2	3.7	2.5	2.6	2.5	4.8	2.5	4.2	4.8	3.8	MR
	F2	4.3	4.3	3.5	4.3	4.0	3.3	2.0	2.7	2.5	4.0	3.0	4.5	4.5	3.6	MR
	F3	4.3	3.3	2.3	4.7	2.7	2.8	1.3	2.5	1.7	3.9	2.0	3.0	3.7	2.9	BS
AMI(O)		4.3	4.0	3.2	4.6	3.6	3.3	1.9	2.6	2.2	4.2	2.5	3.9	4.3	3.4	BS
AML		MR	MR	BS	RS	MR	BS	SA	BS	SA	MR	BS	MR	MR	BS	

Considering the three factors of ISG, namely information security management, awareness and

ISSN 1533-9211

DOI 10.5281/zenodo.7304003

training, and roles and Responsibilities, this arrangement changes as follows: (IYB > QNB > TB > NBY > RDB > SB = YKB > CAC > HCB > YCB > IBY = SIB = RB); (SB = QNB > RDB > NBY = IYB > YKB = TB > HCB > CAC = SIB > YCB > IBY > RB); (IYB > RDB > TB > QNB > NBY > SB > CAC > YKB > YCB > HCB > SIB > IBY > RB).

Through these results we can observe the following (1) the "RB" bank implements ISG requirements with an average overall valuation of 1.9 out of five, an average standard deviation of (0.49) and a very large gap of 3.1. This means that it is the weakest link in the chain of Yemeni sector banks in terms of meeting the ISG requirements. It is also clear that the maturity level of this bank's practices is only second-level, which means that this bank only complies with the security awareness requirements to which it is subject. But lacks controls to meet the ISG requirements. Also, it was observed that this bank maintains the 11th lowest rating in the results of the evaluation of 33.33 % of ISG factors (F1), and the penultimate rating in the results of the evaluation of 66,66 % of them (F2 and, F3) as well. (2) The bank "RB" retains the lower position not only at the general level but also at the level of all governance factors due to the fact that the bank exercises all the security requirements of these factors at a maturity index not exceeding 2.5, with an average standard deviation of (0.49). This means that the bank's likelihood of being exposed to cyber threats is higher than other banks, and it needs to improve its maturity in all ISG areas. In addition, (3) with average maturity values equal to (2.5, 2.2, 2.6, 3.2), average standard deviation equal to (0.39, 0.41, 0.08, 0.59), and an average applied gap of (2.8, 2.5, 2.4, 1.8), the four banks, namely IBY, SIB, YCB, and HCB, rank second-fifth in the list of weaker Yemeni banks in terms of compliance with ISG requirements.

On the other hand, by analyzing the ISG indicators and domains, it can be seen that, the level of commitment to security requirements for ISG varies depending on the nature of the security controls themselves. Factors can be arranged according to the average maturity indexes with which the banking institutions implement their ISG practices as follows: (F1 > F2 > F3), indicators also can be arranged according to those values as: (F1.3, F1.5, F1.2, F1.6, F2.2, F1.1, F2.1, F1.4, F3.3,F3.2, F3.1) Fig. 4. Illustrate the average maturity level values and the average gap in the banking sector's application of these indicators and factors.

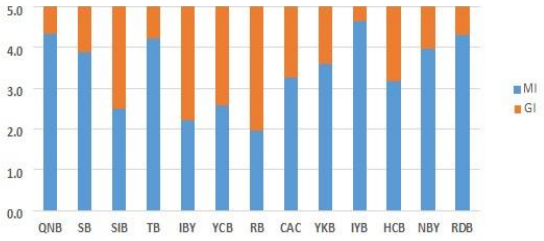

Figure 3: The overall MI and GI values per bank

ISSN 1533-9211

DOI 10.5281/zenodo.7304003

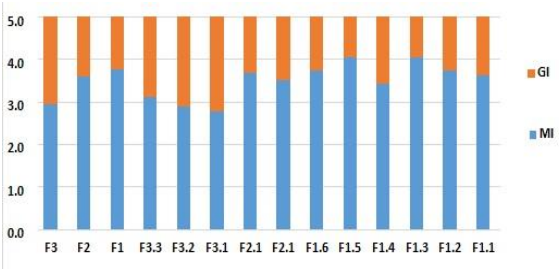

Figure 4: The overall MI and GI values per indicator

According to Fig. 3, the most significant strengths of the banking sector's information security governance practices are information security management and awareness and training, with an average overall maturity index of 3.8 and 3.6 out of five, an application gap of 1.2 and 1.4, and a standard deviation of 0.90 and 0.80, respectively. This entails full involvement of IS management; well-planned, implemented, and measured security investments; and testing and improvement of staff security awareness and competence [25]. The MI values of these factors, however, do not adequately reflect the fact that management assumes information security to be a crucial or integral part of organizational routines, nor do they reflect proactive and awareness-raising methods that guarantee maximum levels of staff security. As a result, the banking sector's practices on these two factors continue to fall short of strong and optimal ISG maturity practices.

The third ISG factor "roles and responsibility," on the other hand, demonstrates a significant weak point in information security management activities in that sector, with an average maturity index of 2.9, an application gap of 2.1, and a standard deviation of 0.97. This simply means that information asset owners understand and adhere to their roles and responsibilities in relation to their assets. However, the banking sector's procedures on this factor also fall short of the ISG requirements of the fourth and fifth maturity levels. Accordingly, the appointment of chief information officers to the IS board, the appointment of information risk owners, and the constant redirection of them to achieve security objectives are all necessary [36].

At the level of ISG indicators, the most prominent findings can be summarized as follows: (1) with an average maturity index of 4.1 , an average gap of 0.9, and a standard deviation of 0.98, the F1.3 indicator, measuring the identification and documentation of a bank's information assets, is ranked first among its category of indicators as well as among all ISG indicators. This is because 78% of banks regularly identify, inventory, and update assets. In addition to this, a large proportion of banks (39%) have strong proactive management practices and update their inventory records in real time, allowing tracking of asset owners and providing proactive protection for their assets. (2) Although the security requirements of this indicator are at the top of the list of most compliant requirements by the banking system as a whole, the requirements of this indicator are implemented at maturity levels not exceeding the basic requirements of security in three banks, namely (RB, YCB, and IBY), as the list of assets is available in these banks, but it is either not updated or is not assigned to its owners according to changes in the enterprise's business. (3) With an average maturity index of four, an application gap of one level, and a standard deviation of 1.2, the F1.5 indicator is ranked second. This is because there are few instances where users have abused the authority to access information in 54% of banks. (4)

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

Although the security requirements of this indicator (F1.5) are adhered to at the robust security maturity level and represent significant strengths for NBY, HCB, IYB, YKB, TB, SB, and QNB, they represent significant vulnerabilities for RB, IBY, and SIB banks. In these banks, users abuse their access authority at a rate of one case per week. Thus, strict administrative controls to strengthen the management of access to information assets and to reduce the potential risk of misuse should be put in place. (5) The F1.2, F1.6, and F2.2 indicators, measuring the banks' ownership of the detailed security policy, the level to which information security is taken into account by bank administrations in planning and in transactions with external parties, and the level of awareness and compliance with IS requirements among users., respectively, are ranked third with an average maturity index of 3.7, an application gap of 1.7, and a standard deviation of (1.06, 1.33, and 0.74), respectively. (6) Although the security requirements of "F1.2" indicator are adhered to at the robust security maturity level and represent significant strengths for 26 % of banks " RDB, IYB, TB, and QNB", and at the fourth level "Meeting requirements" in 23 % of banks (NBY, YKB, and YCB), these requirements represent significant vulnerabilities for HCB, SIB, and SB banks. This is because those banks either rely on oral instructions without a clear and documented security policy (SIB and SB), or there is a guide to limited security procedures that do not cover all relevant issues (HCB). Hence, these banks should adopt, continuously and proactively update and review a detailed policy covering all areas of work, including all legal and security requirements, to enhance security and reduce their governance risks [33]. (7) Although the security requirements of the "F1.6" indicator are adhered to at the robust security maturity level and represent significant strengths for 46 % of banks (" RDB, IYB, YKB, TB, SB, and QNB") and at the fourth level (meeting requirements) in 15 % of banks (NBY and CAC), these requirements represent significant vulnerabilities for HCB, RB, YCB, IBY, and SIB banks. The top management of HCB, RB, YCB, and SIB banks only recognized the importance of IS for business activities and communications, and in addition to this recognition, in the IBY bank, the IS issues are only taken into account in transaction activities. According to the study [18], this group of banks will be exposed to security risks resulting from the failure of external parties to adhere to security controls and requirements, especially those related to encroachment on the confidentiality and privacy of business data, which negatively affects the continuity of the enterprise's business and the trust of its customers in it. Thus, to enhance the level of security and reduce these risks, these banks must adopt appropriate management strategies and policies to ensure that IS aspects are truly incorporated into all their business activities and plans, and that IS requirements are described in detail in their agreements with external parties. In addition, these banks should develop and implement security policies and controls to monitor all transactions, report security abuses, and correct deviations from security requirements agreed with external parties [25]. (8) Although indicator 2.2 is among the top five indicators whose security requirements are complied with by banks, this compliance does not meet the ideal maturity level. These findings indicate that in some banks (RB, and YCB), awareness among users existed but no compliance by them. Also, the poor level of compliance in some other banks (NBY and IBY) was estimated. At a higher level, each of the (RDB, YKB, and SB) banks' users are fully compliant with IS requirements, but compliance is not implemented proactively. (9) With an average maturity index of 3.6, an average gap of 1.4, and a standard deviation of 1.18, the F1.1 indicator, measuring the senior

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

management's recognition of the role required to ensure information security, is ranked fourth among its category of indicators as well as among all ISG indicators. However, this intermediate arrangement can be explained by the fact that the proportion of institutions that comply with the security controls of this indicator at the ideal maturity level is equal to 30%, and at the fourth maturity level "meets the security requirements" is equal to 23%, which collectively equals half the percentage of banks (53%), and equals with a small difference the other percentage of banks (47%). In any event, these findings indicate that some banks' (RB, YCB, and SIB) senior management only recognize the importance of information security for business, but they do not recognize the role and responsibilities they have and do not support information security plans that reflect the level of compliance of the other groups of banks (HCB, CAC, and IBY). At a higher level, each of the (RDB, YKB, and SB) banks recognizes this role, but they only implement detailed plans to ensure the effectiveness of information security as an official recognition of it as a key factor for the institutions' success and do not see information security as an essential part of their business as the senior management of the NBY, TB, and QNB banks do. Therefore, in our view, the senior management of the banks of the first two groups of banks needs more awareness courses on their roles and responsibilities, the importance of information security for business, and the adoption of plans to enhance their role and responsibilities in ensuring the security of the banks to which they belong [39]. (10) The F2.1 indicator, which measures the availability of information security training and awareness programs, ranks second in its category and sixth among overall ISG indicators. It also should be noted that it is ranked last among the list of five indicators representing weaknesses in the ISG security practices of banks (F3.1, F3.2, F3.3, F1.4, F2.1), whose security requirements in the banking sector are complied with on an average basis (basic security level). In other words, training courses, even if available in the banks' security systems, do not meet with adequate management support and are not provided in accordance with the actual needs of almost 77% of the banks under consideration (All banks with exception the QNO, SB, and NBY). This emphasizes that 77% of banks still need more administrative support and resources and adequate policies and controls to assess the actual training needs of the banks under consideration and to prioritize them on a regular basis to increase the effectiveness and maximize the benefit of training programs [37]. (10) The F1.4 indicator, which measures the mechanisms adapted for data and information classification, ranks last in its category, seventh among overall ISG indicators, and fourth among the list of five indicators representing weaknesses in the ISG security practices of banks, with an average maturity index of 3.4, an average gap of 1.6, and a standard deviation of 0.87. With the exception of one bank (IYB), neither the classification of information assets is constantly reviewed in line with changes in the working environment nor are new assets classified as they arise. (11) The F3.1, F3.2, and F3.3 indicators, which measure the requirements of the roles and responsibilities domain, are ranked 10th, 9th, and 8th, respectively, with an average maturity index of (2.8, 2.9, and 3.1), an application gap of (2.2, 2.1, and 1.9), and a standard deviation of (1.3, 1.4, and 1.04). Their requirements are adhered to at a basic security maturity level and represent significant vulnerabilities for banking institutions' security systems.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

4. Conclusion

This study was aimed at studying and analyzing the maturity in the information security governance practices of Yemeni banks' information security management systems for the purpose of identifying strengths and weaknesses in their practices and making proposals that enable their departments to enhance their security. To achieve that, a mixed quantitative and qualitative approach was adopted. This study's main findings were as follows: The Yemeni banking sector only implements the ISG requirements with an average maturity level equal to (3.9) and with a gap of one level from the ideal robust security level; With average maturities ranging from [4.6 to 1.9], Yemeni banks are ranked in the following order: (IYB > QNB> RDB >TB > NBY > SB > YKB > CAC > HCB > YCB > SIB > IBY > RB); With an application gap of not more than one level, the banking group (IYB, QNB, RDB, TB, and NBY) forms the strongest link among the sector's institutions in applying governance practices. This reflects users' high awareness, as well as senior management's awareness of the importance of information security and support for its application in the bank; A percentage of 92.3 % of banks lacks robust ISG requirements and need to take the necessary administrative measures in a manner that contributes positively to a high level of security among institutions and makes the issue of information security an essential and integral part of the management of those institutions' business, take appropriate and proactive methods to ensure a high level of security awareness among staff, reduce the risks of information assets, and enhance their protection; The "RB" bank's likelihood of being exposed to cyber threats is higher than other banks, and it need to bridge an average gap of (3.1) to improve its maturity; With a maturity level equal to four, the highest-rated indicators in the "information security management" sub-dimension are the "F1.5"—information assets in banks are systematically identified and documented—and the "F1.3"—abuses of access authority by bank users are rare; At the same maturity level, the compliance in banks is not implemented proactively and that users' level of awareness and compliance with information security "F2.2" in banks meets only the basic security requirements; Banks' ISMSs comply better with the requirements of the "information security management" and "training and awareness" ISG domains than with the requirements of the domain of "roles and responsibilities".

In addition, there is a range of strengths and weaknesses in of banks' ISMSs with regard to the application of information security governance practices. The main strengths are: the systematic identification and documentation of information assets in banks; the paucity of users' abuse of access authority in banks; information security is a major consideration in all enterprise plans and dealings with external parties; providing a detailed security policy; and a high level of awareness and compliance of users with regard to information security. The main flaws were: the lack of an independent information security unit; failure to conduct appropriate security tests on those eligible for key positions before granting them authority; limited bank administrations' awareness of information security requirements, which was not optimally coordinated; a lack of training and awareness-raising programs for users based on their needs; and inappropriate classification of information, without taking into account the value, sensitivity, and relevance of assets, with no continuous mechanisms available to address this.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

Accordingly, The study recommends the adoption of policies and strategies to enhance banks' information security governance, with a focus on: clearly assigning roles and responsibilities commensurate with employees' qualifications and experience; and thus helping achieve the objectives of information security in the bank in an optimal manner; and establishing an independent information security unit that includes members with the necessary expertise and qualifications from various relevant departments such as risk management, compliance management, and senior management; in particular, those related to testing staff members' security before accepting them in accordance with the bank's information security policies; study and analysis of the foundation's training needs; and providing training and awareness programs tailored to the needs of users to ensure that they maintain an optimal level of awareness and improve their performance; enhancing the level of awareness of awareness of bank departments about information security requirements and developing appropriate mechanisms and plans to ensure the active participation of such departments in all matters related to information security in banks; adopting appropriate controls and policies that allow the management of information assets and users' identities; and work on reviewing and updating the above policies on an ongoing basis.

References

1. J. Gu, K. Gouliamos, O.-R. Lobonț, and M. Nicoleta-Claudia, "Is the fourth industrial revolution transforming the relationship between financial development and its determinants in emerging economies?," Technological Forecasting and Social Change, vol. 165, p. 120563, Apr. 2021.
2. T. G. Hoang, G. N. T. Nguyen, and D. A. Le, "Developments in Financial Technologies for Achieving the Sustainable Development Goals (SDGs)," Disruptive Technologies and Eco-Innovation for Sustainable Development, pp. 1–19, 2022.
3. A. 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.
4. A. 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.
5. 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.
6. Q. A. Al-Fatlawi, D. S. Al Farttoosi, and A. H. Almagtome, "Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study," Webology, vol. 18, no. Special Issue 02, pp. 294–310, Apr. 2021.
7. K. Rostek, "Key technologies in the digital transformation of finance," Digital Finance and the Future of the Global Financial System, pp. 45–64, Jul. 2022.
8. A. Nasser, "Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yeme,n'". Int. J. Sci. Res. in Multidisciplinary Studies Vol, 3(11).2017.
9. A. N. Al-Shameri, "Hierarchical Multilevel Information security gap analysis models based on ISO 27001: 2013," International Journal of Scientific Research in Multidisciplinary Studies, 3(11) , pp 14-23, 2017.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

10. S. Wassan, C. Xi, N. Jhanjhi, and H. Raza, "A Smart Comparative Analysis for Secure Electronic Websites," Intelligent Automation & Soft Computing, vol. 29, no. 3, pp. 187–199, 2021.
11. M. Hamdi, F. Olayah, A. A. Al-Awady, A. F. Shamsan, and M. M. Ghilan, "Attitude Towards Adopting Cloud Computing in the Saudi Banking Sector," Intelligent Automation & Soft Computing, vol. 29, no. 2, pp. 605–617, 2021.
12. A A Nasser, N K A Ansi, N A 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 6,2020.
13. I. Obaid, S. Asad, and A. Qasim, "Modeling and Verification of Payment System in E-Banking," International Journal of Advanced Computer Science and Applications, vol. 8, no. 8, 2017.
14. A. S. and Z. Saleh, "Community Perception of the Security and Acceptance of Mobile Banking Services in Bahrain: An Empirical Study," International Journal of Advanced Computer Science and Applications, vol. 6, no. 9, 2015.
15. C. Paya, "7. Information Security of Financial Data," Harboring Data, pp. 121–144, Dec. 2020.
16. D. Prabakaran and S. Ramachandran, "Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment," Computers, Materials & Continua, vol. 70, no. 1, pp. 1781–1798, 2022.
17. 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.
18. 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.
19. 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).
20. 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.
21. 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
22. 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.
23. Насер, А. А. (2012). Концепция построения информационной системы вуза на основе структурно-функционального анализа информационных потоков. Вестник АПК Верхневолжья, (1), 81-85.
24. 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.
25. N. I. Ngwum, "Information security maturity model (ISMM)," M.S. dissertation, The University of Manchester, 2013
26. M. Sajko, N. Hadjina, Ivan Sedinic, , " Information security governance and how to accomplish it," Proceedings of the 34th International Convention MIPRO (2011), pp 1516-1521, 2011

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7304003

27. 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.
28. A. A. Nasser, A. A. Alkhulaidi, M. N. Ali, M. Hankal, and M. Al-olofe, "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
29. A. 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.
30. 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,
31. A. S. A. Alghawli, Abdualmajed A. Al-khulaidi, 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,pp 680-691 2022.
32. S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," Computers & Security, vol. 99, p. 102030, Dec. 2020.
33. S. Posthumus and R. von Solms, "A framework for the governance of information security," Computers & Security, vol. 23, no. 8, pp. 638–646, Dec. 2004.
34. R. Moulton and R. S. Coles, "Applying information security governance," Computers & Security, vol. 22, no. 7, pp. 580–584, Oct. 2003.
35. T. Kayworth, and D. Whitten, , "Effective information security requires a balance of social and technology factors," MIS Quarterly executive, , vol. 9, no. 3, pp. 2012-52, 2010
36. K. Brotby, "Information Security Governance," Mar. 2009.
37. K. Park and H. Y. Youm, "Improvements of Information Security Level in Electronic Financial Infrastructure (By Analyzing Information Security Management Level)," Journal of The Korea Institute of information Security & Cryptology, vol. 26, no. 6, pp-1605-1618, 2022.
38. P. J., Steinbart, R. L.Raschke, G.,Gal, and W. N. Dilla, "The influence of a good relationship between the internal audit and information security functions on information security outcomes," Accounting, Organizations and Society, v. 71, pp 15-29.,2018
39. C. Lin, J. L. S. Wittmer, and X. (Robert) Luo, "Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance," Information & Management, vol. 59, no. 6, p. 103650, Sep. 2022.