International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I4P220

Volume 71 Issue 4, 225-237, April 2023

Original Article

Information Security Risk Management in Yemeni Banks: An Evaluation of Current Practices

Abdualmajed A. G. Al-Khulaidi[1], Mujib M. Y. Al-Ashwal[2,3], Adel. A. Nasser[2,4,*], Nada K. Al-Anesi[4]

[1]*Department of Computer Science, Sana'a University, Sana'a, Yemen.*
[2]*Department of Information Systems and Computer Science, Sa'adah University, Sa'adah, Yemen.*
[3]*Department of Information Technology, University of Modern Sciences, Sana'a, Yemen.*
[4]*Modern Specialized College for Medical and Technical Sciences, Sana'a, Yemen.*

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

Received: 13 February 2023 Revised: 05 April 2023 Accepted: 12 April 2023 Published: 25 April 2023

Abstract *- This study aims to assess the level of maturity in the risk management practices of Yemeni banks and determine the extent of the gap that these institutions' security systems need to fill in order to reach the ideal level of maturity. To achieve this, a comprehensive survey approach is used, with 26 experts representing specialized experts in all 13 banks in the capital, Sana'a. An appropriate assessment framework and maturity model were selected and adapted to collect, process, analyze, and interpret the data. The main findings were that the Yemeni banking sector's ISMS only meets the requirements of the fourth ISRM maturity level in its practices relating to all information security risk management (ISRM) indicators and dimensions, with average MI values ranging from 3.58 to 4.08 and an overall average index not exceeding 3.84. The backup of the risk management processes is the most prominent strength of the banking sector's ISMS, while insufficient risk assessment and handling are the most significant disadvantages. With a one-level application gap, the TB bank's ISMS is the most compliant bank for risk management requirements, followed by the ISMS of the IYB, RDB, SB, QNB, NBY, SIB, YCB, IBY, and CAC banks; the YKB bank's ISMS is the least compliant bank for requirements. Other local studies have addressed the issue of information security assessment in the banking sector; however, this study takes a different track, discussing ISRM-related challenges and offering suggestions to help banks implement more beneficial policies, improve the security of their assets, and support business continuity.*

Keywords *- Information security, Information security assessment, Gap analysis, Maturity model, Risk management practices, yemeni banks.*

1. Introduction

The fourth industrial revolution has driven major transformations in the global economy and significantly impacted various business sectors, including banking. Digital transformation and the use of modern technology to enhance performance, ensure business continuity, and improve productivity have become essential for all companies, particularly in highly competitive industries. Hassan et al. (2022) found that modern technology adoption in banking greatly contributes to effective customer service delivery via online channels, reduces service costs, and maximizes associated revenue [1]. Gaudio et al. (2021) similarly found that concentrated adoption of information technology and financial technology improves overall economic stability in the financial industry [2]. Stalmachova et al. (2022) identified key reasons for the banking sector's digital transformation to include providing services in remote areas, differentiating from competitors, and reducing operating costs [3].

The transformation process must be continuous and responsive to internal and external environmental changes, as well as aligned with the changes brought about by the industrial revolution [4], [5], and [6]. However, realizing the benefits of digital transformation of banking institutions and its impact on local economic development requires practical implementation by financial institutions and government decision-makers in Yemen.

On the other hand, digital transformation in banking institutions, heavy reliance on modern ICT in their practices, and heavy reliance on different information assets to conduct business pose significant challenges that threaten their success. Many studies have addressed this topic, notably [7], [8], and [9]. According to the authors of [10], the more internal and external data transfers increase, the higher the risk of exposure to information assets and systems in the banking industry, particularly when using modern ICT. Researchers in [11] have added that the risk of increased

vulnerability and amplification of cybersecurity threats against banks is escalating. Therefore, information security must always be adequately ensured to mitigate risks and prevent harm to these institutions.

However, international standards such as ISO 27001 offer security objectives, detailed controls, specific controls, and requirements through which organizations can investigate whether their maturity level of security is sufficient to do so [12],[13]

In addition, the findings of the study [14] confirm that adherence to the ISO 27001 protection controls provided by such standards greatly helps reduce banks' security risks and positively impacts the performance of banks. Reducing the cost of information security procedures, encouraging more good inter-institutional engagement and cooperation, as well as enhancing customer confidence in the services they provide and improving their reputations and brand images [15]. This, in turn, enables them to ensure the success and continuity of their businesses, achieving further economic expansion. Previous studies have also found that assessing the level of adherence to ISO 27001 controls, or what is known as the maturity of information security practices, helps identify weaknesses, guides future research and strategies, and enhances current understanding of how organizations can better equip themselves to reduce the incidence and impact of cyberattacks [12], [16].

In light of increasing security threats, there is a general concern about the readiness of information security management systems in Yemeni banking institutions and the extent to which they adhere to information security controls to mitigate risks. Two aspects must be considered to address this issue. Firstly, an appropriate evaluation framework and maturity model must be used for the evaluation process, and secondly, the security aspect must be analyzed. Based on this standard, many frameworks and maturity models have been developed in the literature. Studies [13] describe some of these. Ngwum [41], for instance, classifies the information security controls provided by the ISO 27001 standard into four areas: processes and procedures, technology and innovation, security governance, and risk management. The study's author suggests a measurement framework and a maturity model with four sub-frameworks and models, providing a systematic approach to evaluating a company's adherence level to these domains.

Practically, at the local level, three studies have been conducted to evaluate the information security maturity of Yemeni banks' ISMS based on the proposed framework and model [18],[19],[20].

These studies analyzed the level of compliance of Yemeni local banks with information security requirements in the first three dimensions of this framework (processes and procedures [18], technology and innovation [19], and security governance [20]) and provided recommendations to improve the IS statutes in those systems. In those studies, the first Ngwum's three sub-frameworks and models were selected and applied as an optimal tool to assess ISML in 13 Yemeni banking institutions.

The reasons behind this decision were that it provided a comprehensive framework for measuring information security in various IS domains covered by the ISO/IEC 27001:2013 standard, which is widely used in Yemeni banking institutions. It also combined multiple security requirements and controlled into a shortlist that reflected all security requirements and controls for those domains. It used a hybrid of quantitative and qualitative measures to reflect appropriate information security maturity levels.

Upon analyzing these studies, it was found that although they addressed much of the general research problem aspects, they did not examine the maturity level of information security risk management practices in the banks' information management systems, which is a major dimension of the assessment framework used. According to [21], enterprise risk management and project success are inextricably linked, and the level of risk management practiced during the project directly impacts its success or failure. Improper risk management contributes to project failure and is a primary factor in the majority of security incidents at institutions. Risk management (RM) is seen as a crucial component in lowering the risks to business continuity because it significantly contributes to protecting institutions' assets and information resources [22]. Information resources and assets should be evaluated and safeguarded according to how sensitive and important they are to the company [12],[13],[22]. Most previous studies and international standards emphasize the need to recognise an enterprise's risk tolerance and adopt relevant policies and strategies for effective risk management and reducing threats to the enterprise's information assets.

Additionally, the overall maturity level, index and gap values differ from one domain to another, as well as from one bank to another. Furthermore, the major weaknesses, vulnerable points, and significant points of strength also differ from one domain to another and one bank to another [18-20]. All those three studies addressed the same study community, and the collected maturity measures reflected the opinions of the same study community members. The research methodology used in all three studies, including assessment frameworks and maturity models, is based on one evaluation framework and one maturity model [41]. This framework divided risk management control areas into two major categories. The first domain includes key indicators for assessing and addressing enterprise information security risks. The other area's main content is incident management and business continuity controls in those organizations.

Based on the literature review, the research gap, research problem, and research objectives can be articulated as follows:

The research gap is the lack of study on the maturity level of information security risk management practices in Yemeni banks' information management systems. Despite the importance of digital transformation and technology adoption in enhancing customer service, productivity, and cost reduction in banking institutions, their heavy reliance on modern ICT exposes them to significant information security challenges. Although several studies have addressed this issue, none have examined the maturity level of information security risk management practices in the Yemeni banking system. This is a critical aspect of information security.

The research problem examines and analyses discrepancies in the maturity level of information security risk management practices in Yemeni banks' information management systems.

The study's specific objectives are to assess compliance with information security risk management controls among Yemeni banks, identify weaknesses in their information security practices, and provide recommendations for improving the information security situation. This study fills a research gap by addressing the risk management dimension previously unaddressed in similar studies. The findings may help stakeholders in banks formulate more appropriate ISRM policies or provide a more effective focus on ISRM controversies to improve the information security situation.

The study is structured as follows: in Section 2, a literature review is conducted to provide context. Section 3 outlines the study's objectives and hypotheses, while Section 4 describes the materials and methods used. Section 5 presents and analyzes the results of a case study, and Section 6 offers a conclusion.

2. Literature Review

Modern information technology and its systems play a major role in achieving countries' development goals and in all educational [25-28,42], health [30-31], industrial [32-33], financial [34] and other sectors [35,43]. Accelerating the development, proliferation, and adoption of digital transformation through process redesign is crucial for enterprises looking to stay competitive in today's fast-paced business landscape [37]. By embracing modern ICT innovations, businesses can effectively address the limitations of traditional systems and reap the benefits of improved efficiency and productivity. In the financial sector, the use and development of modern technology present exciting investment opportunities. The successful implementation of advanced information technology can give companies a valuable edge in both local and regional markets.

Furthermore, incorporating these tools has become imperative for effective business information management and essential for sound managerial decision-making at all levels and across all industry sectors. The significance of embracing modern technology for enterprises, particularly in the banking sector, cannot be overstated. Various studies, including notable ones such as [7], [9-10], have extensively explored technology's pivotal role in ensuring the prosperity of banking businesses. According to [38], digital banking, which is currently considered the new form of banking, involves the use of Internet technology and mobile applications and is exposed to many security risks. The security risks in digital banking are due to the use of online channels for financial transactions, which involve using personal and financial data such as bank account details, credit card details, and login credentials. In addition, cybercriminals are becoming more sophisticated and have developed new methods to breach systems and steal sensitive information, such as phishing scams, viruses, malware, and hacking. These techniques can be used to compromise digital banking systems.

However, research on information security threats and risks in the banking sector shares four primary findings. [7], [9], [18-20],[38]: Cybercriminals heavily target the banking industry because of its potential to yield financial gain. Comprehensive security processes, procedures, tools, applications, and policies are necessary for safeguarding financial stability; following normative controls and standards can provide a framework for reducing risk, and implementing recommended security solutions and policies is the first and most significant step towards mitigating risk.
The ISMS (ISO-27001) standard is one of the most well-known and widely used international standards on information security worldwide. Implementing the ISO 27001 standard can provide a range of benefits to organizations beyond improved effectiveness and economic growth. These benefits can include increased customer confidence in the organization's ability to protect sensitive information, improved data management practices, compliance with legal and regulatory requirements related to data security, better risk management processes, an improved reputation and brand image for the organization,, and the ability for the company to expand economically. A reduced likelihood of security breaches, resulting in cost savings related to avoiding potential data breaches and associated legal or remediation costs [39],[18].

Furthermore, a study conducted by [22] found a significant difference in the level of cyber threats and the effectiveness of information security systems between institutions that adhere to ISO 27001 control mechanisms and those that do not. The study revealed that organizations implementing ISO 27001 protection controls and guidelines have an average cybersecurity threshold of 5 units lower (4.00) than organizations that do not (8.75). Additionally, the

median efficiency in reducing hacking attacks is approximately 22 units higher (40.74) in organizations that implement ISO 27001 security controls compared to those that do not (18.32).

From another perspective, ISO 27001 is a comprehensive standard that can be challenging to understand in its entirety. For this reason, researchers often build summary frameworks based on the ISO 27001 criteria to provide an easier understanding of the standard's requirements. These frameworks typically contain a limited number of indicators and classify them into different categories outside of the standard's own classification. By condensing the criteria into a smaller number of indicators, researchers can simplify the standard and make it more approachable for businesses that are trying to comply [13]. Additionally, classifying the indicators into other dimensions can help organizations better understand how they should prioritize their compliance efforts. For example, a researcher might classify certain indicators as "technical" and others as "administrative" to help companies understand which aspects of their security policies require more focus]. However, the benefits of these summary frameworks include increased understanding and simplified compliance efforts for organizations. Breaking down the ISO 27001 criteria into manageable parts makes it more accessible and easier for organizations to implement.

Nasser's study reviewed a set of evaluation frameworks proposed based on ISO 27001 and classified its controls according to those frameworks [13]. Also, Ngwum has classified the information security controls provided by a standard into four main areas: processes and procedures, technology and innovation, security governance, and risk management [41].

Ngwum has also suggested a measurement framework to evaluate the level of a company's adherence to these security domains. At the local level, three studies have been conducted on evaluating the information security maturity of Yemeni banks' ISMS based on the model proposed by the researchers. The framework proposed by the researchers is distinguished by its qualitative and quantitative metrics and involves the basic criteria for evaluating the levels of compliance within the banking firm's ISMS. The studies analyzed the level of compliance of Yemeni local banks with information security requirements at the level of the first three dimensions of the framework (processes and procedures, technology and innovation, and security governance) and provided recommendations to improve the IS statutes in those systems.

3. Objectives and Hypothesis

After reviewing the works provided in Section 2, several observations can be made. Firstly, while the three local studies addressed many aspects of the general research problem, they did not evaluate the maturity level of information security risk management practices in the banks' information management systems, which is a key dimension of the assessment framework used in these studies. Secondly, differences were observed in the overall maturity level, index, and gap values across different domains and banks. Likewise, significant strengths and weaknesses varied across different domains and banks. Thirdly, all three studies utilized the same study community, and the collected maturity measures reflected the opinions of the same study community members. Fourthly, each of the three studies utilized a research methodology, including assessment frameworks and maturity models, based on one evaluation framework and one maturity model. Therefore, in light of these research gaps, it is necessary to emphasize again that the objective of this study is to examine the level of compliance of Yemeni banks' information security management systems (ISMSs) with information security risk management (ISRM) controls, identify their strengths and weaknesses, and suggest appropriate solutions that could help reduce the gaps in their practices. This would enable stakeholders in banks to develop more effective ISRM policies and focus on key controversies that require attention to improve the information security situation as well as reduce the estimated gaps. To achieve this, based on the aforementioned analysis, we have formulated two hypotheses that will be tested throughout this study:

- The first hypothesis is that the level of adherence to ISRM controls and domains varies among different ISRM domains. The Yemeni banking system needs to bridge different gaps to meet the robust maturity level requirements.
- The second hypothesis: the level of adherence to ISRM controls and domains varies among different banking systems. Each system needs to bridge different gaps to meet the robust maturity level requirements.

4. Materials and Methods

In this study, a hybrid methodology was utilized, which combined two distinct methodologies: an analytical-descriptive methodology and a comprehensive survey methodology. The primary goal of the analytical-descriptive methodology was to assess current information security management systems and evaluate their adherence to ISO 27001-2013 standards, focusing on risk management. This was accomplished through the implementation of a specific assessment framework and maturity assessment model [41] using precise procedures. To obtain the input of IS specialists in all of Sana'a's banking institutions, a tool was developed that corresponded to their demands. The following sequence of steps was utilized to address the issue using this methodology: S.1: Define study problem; S.2: Conduct literature review; S.3: Develop data collection tool; S.4: Collect and analyze data; and S.5: summarize observations, engage in discussions, and make pertinent recommendations.

Table 1. Risk management capability assessment framework [41]

Domain	ID	Indicator	ML	Expected evidence for each corresponding ML
Risk assessment and treatment	F1.1	Is there adequate physical security in place to protect information assets?	L1	Information assets are easily accessible to all
			L2	Physical protection for information assets is loose.
			L3	The physical protection of information assets is provided, but there is a lack of proper risk assessment to determine if the level of protection is sufficient
			L4	A thorough risk assessment is conducted, and appropriate physical protection measures are implemented to ensure the safety of information assets, considering all potential threats to humans and the environment.
			L5	To enhance our security measures, physical protection controls are constantly updated in line with modern technological advancements in order to implement the most effective security practices.
	F1.2	Has the organization performed a thorough risk assessment and implemented appropriate risk management measures for all information assets?	L1	No form of risk assessment
			L2	Risks are often neglected until they materialize, and little proactive action is taken to address them.
			L3	Although the risk assessment has been completed, the treatment plans have not been completely executed.
			L4	The organization conducts detailed risk assessments, establishes its risk appetite, and implements treatment plans as necessary.
			L5	The organization engages in continuous review of its risk registers and risk appetite. It regularly assesses the treatments for identified risks to ensure they are up to date with the changing nature of risk.
Incident and business continuity management	F2.1	Is there a comprehensive business continuity and disaster recovery plan in place for the company's information systems, and how frequently is it reviewed and tested?	L1	Currently, there are no business continuity plans in place.
			L2	In the event of an incident, the organization only takes emergency actions.
			L3	The organization's business continuity plans solely focus on data and databases.
			L4	The organization has comprehensive incident and business continuity plans in place, with monthly checks to ensure they are always ready for activation.
			L5	The organization continually reviews and tests its business continuity plans to ensure they are always prepared to support business operations.
	F2.2	How often are data backed up? Are there an active data backup policy and strategy in place?	L1	There are no policies or plans in place to back up information assets.
			L2	The importance of data backup is not being given due attention.
			L3	Data backup is only done on a monthly basis without taking active measures to ensure fast recovery in case of a problem.
			L4	Adequate policies and strategies are in place for data backup and restoration, and they are regularly tested to ensure effectiveness.
			L5	Policies are reviewed regularly, and strategies are rehearsed continuously to ensure readiness at all times.
	F2.3	How often are virus scans performed, and are updates implemented as needed?	L1	Annually
			L2	Quarterly
			L3	Monthly
			L4	Weekly
			L5	Daily

Table 2. Study community: banks and their abbreviations

Bank	ABB.	Bank	ABB.
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		

5. Define the Problem the Study

In this sub-phase, the problem of the study was defined as presented in Sec.1.

6. Review of Literature

During this initial phase of the study, a specific selection of works was thoroughly examined and analyzed in order to highlight the significance of the study topic, identify prior research contributions, determine any gaps in the research, formulate the research problem statement, construct appropriate hypotheses, and identify theoretical frameworks for evaluation. Practical tools and models were also recognized for collecting and analyzing data.

In addition to the information provided in the earlier part of the study, the results from this phase indicate the utilization of the risk management capability assessment framework proposed by the researcher [41] as the main evaluation framework. As shown in Table 1, this framework is segmented into two domains regarding information security risk management. The first domain addresses two crucial indicators for assessing and mitigating banks' information security risks, while the second domain comprises three indicators for gauging practices in incident management and business continuity within selected organizations (see table. 2). According to this framework, the degree of compliance for each evaluation indicator can be evaluated at five different maturity levels: level 1 (vulnerable), level 2 (information security awareness), level 3 (basic security), level 4 (fulfillment of requirements), and level 5 (strong security). Each level has a corresponding set weight, commencing at 1 and culminating at 5. The preceding table also reveals the projected evidence for each corresponding maturity level, which summarizes the bank's level of commitment to security requirements for each indicator.

7. Designing the Data Collection Tool

This step focused on creating a clear and reliable assessment tool (questionnaire) that adheres to methodological standards regarding validity and consistency for questionnaire construction. The suggested maturity measurement framework was translated into Arabic, and five questions (indicators) were dispersed among the two primary ISRM dimensions, which correspond to the two core RM evaluation fields. A group of 15 academic and non-academic experts, including computing specialists, information security experts, and statisticians, provided feedback on the tool's face, content, and construct validity. The results were positive, and the tool was assessed as a valid tool with recommended modifications. The final version of the questionnaire was created using experts' observations and consisted of demographic data and assessment sections with five levels of maturity measurement for each question. This version would be sent to bank evaluators to determine the maturity level that reflects their banks' ISMs at the level of each of the five indicators.

8. Data Collection and Analysis

In this step, a questionnaire tool was used to collect and analyze data related to security practices in 26 banks. The sample was distributed based on the size of the banks and their policies regarding research studies. Regarding the demographic characteristics of this sample, 88% of the individuals were male. In terms of education, 81% held a university degree, while 19% held a higher degree.

Table 3. Results of study

Factor		RDB	NBY	HCB	IYB	YKB	CAC	RB	YCB	IBY	TB	SIB	SB	QNB	Avg. MI	OML
F1	F1.1	4.00	3.00	3.00	4.70	2.00	3.30	3.00	4.30	4.30	5.00	5.00	5.00	4.70	3.95	MR
	F1.2	5.00	4.00	4.00	4.30	1.00	2.70	3.00	3.00	4.00	5.00	3.00	3.50	4.00	3.58	MR
F2	F2.1	4.00	4.00	5.00	4.00	2.00	3.00	2.00	4.00	4.00	5.00	3.00	3.50	4.30	3.68	MR
	F2.2	4.00	5.00	4.00	4.70	3.00	4.30	3.00	3.70	4.00	4.50	4.00	4.50	4.30	4.08	MR
	F2.3	5.00	5.00	1.00	4.70	5.00	5.00	1.00	5.00	2.00	5.00	5.00	5.00	4.00	4.05	MR
F	F1	4.50	3.50	3.50	4.50	1.50	3.00	3.00	3.65	4.15	5.00	4.00	4.25	4.35	3.76	MR
	F2	4.33	4.67	3.33	4.47	3.33	4.10	2.00	4.23	3.33	4.83	4.00	4.33	4.20	3.94	MR
Avg. MI		4.42	4.08	3.42	4.48	2.42	3.55	2.50	3.94	3.74	4.92	4.00	4.29	4.28	3.84	MR
OML		MR	MR	BS	MR	SA	MR	SA	MR	MR	RS	MR	MR	MR	MR	

Table 4. A maturity model to analyze the current state of ISRM practices in banks [41].

OML	AVG MI		Domain		
	From	*To*	*Risk assessment and treatment*	*Incident and business continuity management*	*ISRM*
L1: Vulnerable	0	1.5	The organization lacks an information risk policy and fails to assess and treat risks properly.	Incident reporting and response procedures are absent, and no business continuity plan is in place.	The information security risk management (ISRM) approach is substandard and vulnerable to threats.
L2: Security Awareness	1.6	2.5	While risk policies and risk owners exist, there is a lack of effective risk management in place.	There is a lack of coordination in reporting security events and no implementation of business continuity plans.	Investments in information systems security are reactive and only made in response to immediate needs rather than being proactive.
L3: Basic Security	2.6	3.5	The company's risk appetite, policy, and owners' expectations are clearly defined and adhered to. The risk register identifies and addresses important business risks.	The organization has established protocols for reporting security incidents. They have implemented business impact analyses and plans.	Basic ISRM requirements are met.
L4: Meeting Requirements	3.6	4.5	The company's risk appetite, policy, and owners' expectations are clearly defined and adhered to. The risk register identifies and addresses important business risks.	A reliable system for reporting and addressing security events should be in place, while comprehensive business continuity plans should encompass all aspects of the business.	Full ISRM security requirements are implemented.
L5: Robust Security	4.6	5	Regularly reviewing risks, threats, and vulnerabilities helps ensure they remain within the organization's risk tolerance level.	Security event procedures and business continuity plans undergo constant testing, maintenance, and review to adhere to standards.	Novel methods are employed to meet industry standards.

All participants had a minimum of 8 years of experience in the security field and occupied various positions, with 58% working as security professionals, 23% as heads of the information security department, and the remainder as directors or deputy directors of the technology department. All questionnaires were tested for validity, and returned questionnaires were accepted for processing and analysis. The process involved calculating average maturity index values at various levels, including each indicator, subdomain, and the security domain as a whole. The results are presented in Table 3. Then, the overall maturity level values (OML) were analysed using the maturity model presented in [41] and listed in Table 4. The security situation can be categorized into five overall maturity levels (OML) based on the average maturity index values. Each maturity level (ML) has associated indicators and a corresponding average maturity range for the ISRM sub-domains of risk assessment and treatment, incident and business continuity management, and the ISRM security domain. Table 5 presents these levels, their indications, and the average MI for each. The final step of the methodology involves summarizing and discussing the results and making appropriate recommendations, which will be discussed in detail in the next two sections.

9. Results and Discussion

9.1. Hypothesis 1

Hypothesis 1: "The level of adherence to ISRM controls and domains varies among different ISRM domains, and the Yemeni banking system needs to bridge different gaps to meet the robust maturity level requirements". Based on the evaluation of the risk management and handling dimension's indicators described in Table 3, it can be concluded that the physical protection measurement indicator (f1.1) has the highest application rate among all indicators at the risk management and handling dimension level. This indicator measures the extent of physical protection of information assets in banks and has an average mi of 3.95, a standard deviation of 1.07, and a relative significance of 72%. The second-highest rated indicator in this dimension is F1.2, which assesses the availability of appropriate risk assessment and handling mechanisms covering all information assets in banks and has an average arithmetic of 3.58, a standard deviation of 1.08, and a relative significance of 72%. These results mean that banking systems based on these two indicators comply with information security requirements only at the fourth level of maturity. The evaluation results of the business continuity management dimension's indicators

show that indicator (F2.2), which assesses if there is a policy and strategy for data backup in banks, has the highest application with an average mi of 4.08, a standard deviation of 0.96, and a relative significance of 82% in the second ISRM dimension. The second indicator (F2.3), which assesses banks' obligation to perform regular virus and system screenings, has an average mi of 4.05, a standard deviation of 0.59, and a relative significance of 81%, putting it in second place. The third indicator, which assesses the availability of a business continuity and disaster recovery plan for bank information systems, is in third place with an average mi of 3.68%, a standard deviation of 0.98, and relative importance of 74%. These results indicate that banking systems meet the information security requirements based on these three indicators only at the fourth maturity level.

When considering the dimensions of ISRM, it is important to note that the business continuity management dimension (f2) has a higher ranking. On average, it received a 3.94 MI rating, with a standard deviation of 0.76 and a relative importance of 79%. This means that most banks only apply controls in this dimension at the fourth maturity level, as only 23% of banks commit to the fifth level through their compliance programs. In fact, 54% of banks are applying this dimension's requirements at maturity level 4, which includes effective mechanisms for reporting security incidents and covering business continuity plans. These findings suggest that 78% of banks still need to close a 1.06-point security gap to reach a high level of security in this area. To do so, they should implement more follow-up and monitoring procedures and mechanisms, develop suitable business continuity management plans, and continuously test, maintain, and review them.

On the other hand, the first dimension (f1) obtained the lowest order, with an average MI of 3.76 and a relative relevance of 75%. Only one bank, or 0.076% of banks, complies with this domain indicator's standards at a strong maturity level. While 23% use these requirements at a maturity level no higher than level III, it is estimated that 54% of banks comply with risk management controls at a maturity level no higher than level IV. This means that 93% of banks still need to adapt active activities to review risks, threats, and vulnerabilities and fill a gap of 1.24 to reach the ideal maturity level that ensures that risks are kept within the bank's rations. Banks can achieve this goal by actively reviewing risks, threats, and vulnerabilities and implementing more comprehensive risk management and reduction plans [11],[14].

Based on the preceding information, the findings support the initial hypothesis and indicate that the banking system adheres to the required risk management indicators and dimensions, meeting the information security requirements at the fourth-level maturity. The average MI values range from 3.58 to 4.08. Additionally, it can be inferred that the banking sector's strong risk management practices for data backup regulations account for their security management system. However, deficiencies in security procedures became evident as it relates to risk assessment and appropriate treatment. Thus, standardized procedures are not being followed. This leads to the conclusion that the industry's information security management systems have not reached the fifth optimum level of maturity but rather have an operational gap to fill of 0.92 to 1.42. To achieve that, there should be effective testing, maintenance, and continuous review of processes and mechanisms for security events and business continuity plans according to international standards, along with appropriate procedures for current risk, threat, and weakness assessments [39],[40].

The findings from the evaluation of the risk management and handling dimension's indicators show that while there are some areas of strength, such as the high application rate of the physical protection measurement indicator and the policy and strategy for data backup in banks, there are also significant areas of weakness. The third indicator in the business continuity management dimension's indicators, which assesses the availability of a business continuity and disaster recovery plan for bank information systems, shows that only at the fourth level of maturity do banking systems meet the information security requirements based on these three indicators.

The evaluations suggest that 78% of banks still need to close a 1.06-point security gap to reach a high level of security in business continuity management. Banks can implement more follow-up and monitoring procedures and mechanisms to achieve this goal and develop suitable business continuity management plans. It is also important for them to continuously test, maintain, and review their plans. Furthermore, the findings suggest that only one bank, or 0.076% of banks, complies with the first dimension (f1) standards at a strong maturity level. This means that 93% of banks still need to adapt active activities to review risks, threats, and vulnerabilities and fill a gap of 1.24 to reach the ideal maturity level that ensures that risks are kept within the bank's rations. Banks can achieve this goal by actively reviewing risks, threats, and vulnerabilities and implementing more comprehensive risk management and reduction plans [11],[14],[21],[24].

In conclusion, there are some strengths in the banking system's adherence to required risk management indicators and dimensions, but there are also significant areas for improvement. Banks should implement more effective testing, maintenance, and continuous review processes and mechanisms for security events and business continuity plans according to international standards and appropriate procedures for current risk, threat, and weakness assessments.

9.2. Hypothesis 2

Hypothesis 2: the level of adherence to ISRM controls and domains varies among different banking systems, and each system needs to bridge different gaps to meet the robust maturity level requirements.

At the bank level, the banking groups (TB, SIB, SB) and (QNB, IYB) ranked first and second on their compliance with the first indicator (F1.1) requirements, with an average maturity level (ML) of (5), and (4.7), respectively. These banks' information security management systems (ISMS) strive to maintain the most up-to-date physical protection controls. Other banks varied in their level of commitment to the requirements of this indicator, with the amount of applied gap varying depending on the system's maturity level. Banks that ranked third (IBY and IBY) and fourth (RDB), with an average ML of no more than 4.3, still need to improve their systems by filling a gap of at least 0.7 to reach the ideal level of maturity. The remaining banks, which topped the list of most vulnerable banks to physical protection risks, require significantly improved security levels. To prevent all threats to information assets using best practices, these banks should enhance their physical protection mechanisms, assess risks, and provide proportionate physical protection while constantly updating their physical protection controls in their systems. (27).

Furthermore, the TB and RDB banks have met the requirements of the second indicator, F1.2, with a perfect average MI of 5. These banks continually review their systems' risk records and processing methods. The IBY and HCB, IBY, QNB, and NBY banking groups ranked second and third with an average MI of no more than 4.3. Although they have adequate and thorough risk assessment mechanisms and manage their risks to meet the fourth level of ISRM maturity, there is still a gap of at least 0.7 levels that need to be closed to attain an ideal level of maturity. These banks must continually review their risk records and methods to address the gap. The remaining banks that ranked highest in susceptibility to external risk should enhance their security status by closing a minimum 1.5-level maturity gap by implementing more efficient risk assessment procedures, creating detailed and comprehensive risk management plans, and regularly reviewing their risk management records and procedures. [40].

Furthermore, the TB and HCB banks have effectively implemented the first (F2.1) indicator requirements, per the audit of the business continuity management dimension's indicators, achieving an excellent average MI score of 5. These banks continually evaluate and analyze their business continuity plans to ensure complete business support preparedness. QNB and IYB, IBY, YCB, RDB, and NBY banking groups ranked second and third consecutively, with an average MI score of less than 4.3. Although they possess comprehensive incident and business continuity plans, they still need to bridge a minimum 0.7-level maturity gap to attain the desired level of maturity. It is vital for them to undergo regular reviews and testing of their business continuity plans to guarantee business support. The remaining banks that topped the list of those most susceptible to business continuity risks must strengthen their security, fill a minimum 1.5 level maturity gap by adopting modern and effective risk assessment procedures, and develop comprehensive business continuity plans, which should be regularly tested to ensure their security.

NBY and IYB banks have top compliance rankings for the F2.2 indicator, with average MI values of 5 and 3.7, respectively. Both banks' data backup plans and policies undergo continual assessment and testing. Meanwhile, banking group systems (TB and SB, CAC and QNB, RDB, HCB, IBY, and SIB) ranked third, fourth and fifth, respectively, receiving an average MI score no higher than 4. Despite having effective data backup and recovery policies, these banks need to improve by at least 0.5 levels to reach the ideal level of maturity. They must keep reviewing their plans to ensure readiness for business support.

Other banks that received rankings for their susceptibility to business continuity risks must strengthen their security to reduce maturity gaps by creating more modern backup and recovery policies and plans. SB RDB, SIB, CAC, YKB, TB, NBY, and YCB banks were rated highest according to standards set by the F2.3 indicator, garnering an average MI score of 5. IYB came in second with an average MI value of 4.77. However, frequent examinations of viruses and systems are necessary to maintain information security.
The QNB bank was ranked third with an average MI score no higher than 4. Although they execute virus and system checks on a weekly basis, they require a daily examination to ensure information security. The remaining banks that ranked the highest in vulnerability to risks must improve their security by developing more up-to-date and efficient periodic screening policies, strategies, and tools. They must reduce at least a three-level maturity gap and continuously update them for ongoing efficacy [16,41].

When discussing the ISRM (Information Security and Risk Management) domain, it is important to recognize that TB Bank's ISMS (Information Security Management System) is the most compliant among banks in regard to risk management requirements. This is because they apply 80% of these requirements at an ideal maturity level of 5. This indicates that the bank uses proactive methods to maintain information security and regularly reviews policies and procedures to ensure their effectiveness. In contrast, only 20% of requirements are implemented at a lower-than-optimal level. As such, the bank's ISMS is likely the least exposed to security risks.

On the other hand, YKB Bank's ISMS has an average MI (Maturity Index) of 2.4 and a maturity level that does not exceed 2, which makes it the least compliant bank for risk management requirements. This suggests that, although decision-makers recognize the importance of managing information security risks, they do not implement sufficient measures on the ground. Additionally, the bank only applies 60% of risk management requirements at maturity levels one or two, which indicates weak policies and plans to address risks. Therefore, the bank must improve its ISRM practices to avoid being vulnerable to security threats. Furthermore, it was noted that several banks lacked an audit of their business continuity plans to ensure they were fully prepared for disasters and crises. The banks that showed weak risk review, handling, and updating were HCB, YKB, RB, and IBY banks' ISMS.

Overall, these findings confirm that each bank's system complies with the ISRM domain's requirements to varying extents with different average MI values and levels. However, as previously recommended, each system has specific gaps that need to be bridged to meet the ISRM domain's robust maturity level requirements.

The results suggest that the level of adherence to information security and risk management (ISRM) controls and domains varies among different banking systems. The study identified gaps in compliance levels for different indicators and found that some banks were more vulnerable to physical protection risks while others were more susceptible to external risk and business continuity risks. The study also highlighted the importance of regular reviews and testing of business continuity plans and the need for more up-to-date and efficient periodic screening policies, strategies, and tools to maintain information security. The study found that TB bank's ISRM was the most compliant among banks, while YKB bank's ISRM was the least compliant, indicating the need for improvement in their risk management practices. Overall, the study recommends that each bank's system needs to bridge gaps to meet the robust maturity level requirements of the ISRM domain.

10. Study Contributions

The Scientific Contributions of this study are:

- The paper examines and analyzes discrepancies in the maturity level of information security risk management practices in Yemeni banks' information management systems.

- The paper assesses compliance with information security risk management controls among Yemeni banks and identifies weaknesses in their information security practices.

- The paper fills a research gap by addressing the risk management dimension previously unaddressed in similar studies.

- The study uses a hybrid quantitative and qualitative approach to comprehensively analyse the information security risk management practices in Yemeni banks.

- The findings provide insights into the compliance of different banking systems with the information security risk management controls and domains.

11. Study Applications, Limitations, and Future Works

The study's findings and recommendations can help stakeholders in banks formulate more appropriate ISRM policies or provide a more effective focus on ISRM controversies to improve the information security situation.
The study is limited to the Yemeni banking sector, and the findings may not be generalizable to other countries or industries. Future research can explore the effectiveness of the recommendations provided in this study and evaluate the impact of implementing them on the information security risk management practices in Yemeni banks.

12. Conclusion

In order to identify the strengths and weaknesses in the Information Security Risk Management (ISRM) practices of Yemeni banks and provide recommendations for improvement, we conducted a study using a hybrid quantitative and qualitative approach. Based on our findings, we have reached the following conclusions: Firstly, we found that the Yemeni banking sector's ISRM systems only meet the fourth ISRM maturity level requirements in their practices relating to all information security risk management indicators and dimensions, with average mi values ranging from 3.58 to 4.08 and an overall average index not exceeding 3.84. Secondly, while the backup of the risk management processes is the most prominent strength of the banking sector's security management system, insufficient risk assessment and handling are the most significant disadvantages. Thirdly, we found that TB Bank's ISMS is the most compliant bank for risk management requirements, followed by the ISMS of RDB, SB, SB QNB, NBY, SIB, YCB, IBY, and CAC banks, with a one-level application gap. In contrast, YKB Bank's ISMS is the least compliant bank for risk management requirements.

Based on these findings, we recommend the following:

- The Yemeni banking sector's ISMS does not adhere to standard practices enabling it to reach the fifth ideal level of maturity. Therefore, security officials in these systems should actively work to close an operational gap of 0.92 to 1.42 at the level of different indicators. This will enable them to provide appropriate procedures for actively reviewing risks, threats, and weaknesses and work to continuously test, maintain, and review procedures and mechanisms for security events and

business continuity plans in line with modern international standards.

- The risk appetite treatments for identified risks should be evaluated on a regular basis in order to keep up with the changing nature of risk through ongoing risk record evaluation.
- The TB Bank's ISMS may be the least vulnerable to related security threats.
- Weak risk review, management, and updating were observed at the ISMS of RB, CAC, YKB, NBY, and HCB banks, as well as a lack of auditing of the business continuity plan to assure complete readiness for emergencies and disasters at the ISMS of HCB, YKB, RB, and IBY banks.
- The YKB Bank's ISMS may be the most vulnerable to security threats, and it needs to bridge an average maturity gap of 2.6 to improve its security status.

We recommend that decision-makers in these banks periodically assess weaknesses in their banks' information systems, examine the level of penetrations to which they may be exposed drastically, and review the compliance of their banks' information management systems with information security policies and standards. We also advise them to ensure business continuity by implementing documented and comprehensive plans, reviewing them on a regular basis, and ensuring that they are always prepared and adequate to deal with disasters and crises. Finally, we recommend that these banks establish a risk management and management plan that is constantly updated to respond to risk effectively.

References

[1] Hisham Hassan, and Panteha Farmanesh, "Customer Adoption of Self-Service Technologies in Jordan: Factors Influencing the Use of Internet Banking, Mobile Banking, and Telebanking," *Management Science Letters*, vol. 12, no. 3, pp. 193-206, 2022. [Google Scholar] [Publisher Link]

[2] Belinda L. Del Gaudio et al., "How do Mobile, Internet and ICT Diffusion Affect the Banking Industry? An Empirical Analysis," *European Management Journal*, vol. 39, no. 3, pp. 327–332, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Katarina Stalmachova, Roman Chinoracky, and Mariana Strenitzerova, "Changes in Business Models Caused by Digital Transformation and the Covid-19 Pandemic and Possibilities of Their Measurement—Case Study," *Sustainability*, vol. 14, no. 1, pp. 127, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Snopkov, V. N., A. A. Nasser, and Alexander Viktorovich Ivanov. "Neural network modeling and mathematical algorithms in the differential diagnosis of diabetic retinopathy," *Bulletin of the Southwestern State University*, 2-1, pp. 50-57, 2012. [Google Scholar]

[5] Swapan Ghosh et al., "Digital Transformation of Industrial Businesses: A Dynamic Capability Approach," *Technovation*, vol. 113, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] A. A. Nasser, "Information-Analytical Support and Information Modeling of Decision-Making Processes in Various Subsystems of the University," *Contemporary Research and Innovation*, vol. 8, pp. 4-4, 2011. [Google Scholar]

[7] Xuanli Xie, and Shihui Wang, "Digital Transformation of Commercial Banks in China: Measurement, Progress and Impact," *China Economic Quarterly International*, vol. 3, no. 1, pp. 35-45, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Alexeis Garcia-Perez et al., "Resilience in Healthcare Systems: Cyber Security and Digital Transformation," *Technovation*, vol. 121 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Nehal Chatterjee, and Ratul Goswami, "Information Technology and Security Analysis," *International Journal of Computer Trends and Technology*, vol. 68, no. 10, pp. 66-68, 2020. [CrossRef] [Publisher Link]

[10] Dervis Kirikkaleli, and Emine Ünar Kayar, "The Effect of Economic, Financial and Political Stabilities on the Banking Sector: Cases of Six Balkan Countries," *Sustainability*, vol. 15, no. 4, pp. 3000, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Luca Allodi, and Fabio Massacci, "Security Events and Vulnerability Data for Cybersecurity Risk Estimation," *Risk Analysis*, vol. 37, no. 8, pp. 1606–1627, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. A. Nasser, "Information Security Gap Analysis Based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies Sana'a Yemen," *International Journal of Scientific Research Multidisciplinary Studies*, vol. 3, no. 11, pp. 4-13, 2017. [Google Scholar] [Publisher Link]

[13] A. A. Nasser Al-Shameri, "Hierarchical Multilevel Information security gap analysis models based on ISO 27001: 2013," *International Journal of Scientific Research in Multidisciplinary Studies*, vol. 3, no. 11, pp. 14-23, 2017. [Google Scholar] [Publisher Link]

[14] Nilo Legowo, and Yoyo Juhartoyo, "Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001," *Journal of System and Management Sciences*, vol. 12, no. 3, pp. 181-199, 2022. [Google Scholar] [Publisher Link]

[15] Harrison Stewart, "Why ISO27001 Certified Organizations Still Experience Data Leakage?," *Journal of Digital Information Management*, vol. 20, no. 3, no. 91, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Adel A. Nasser, Abdualmajed A. Al-Khulaidi, and Mijahed 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, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[17] V.Usha Bala, and B.D.C.N.Prasad, "Steering the Enterprise's Information System Security Risks in Relation with Uncertainty (Information System,Risks)," *SSRG International Journal of Computer Science and Engineering* , vol. 5, no. 2, pp. 5-8, 2018. [CrossRef] [Publisher Link]

[18] Adel A. Nasser, Nada Kh. A. Al Ansi, and Naif A. N. Al Sharabi, "On the Standardization Practices of the Information Security Operations in Banking Sector: Evidence from Yemen," *International Journal of Scientific Research in Computer Science and Engineering*, vol. 8, no. 6, pp. 8–18, 2020. [Google Scholar] [Publisher Link]

[19] Abdualmajed A. G. Al-Khulaidi et al., "Information Security Gap Analysis: An Applied Study on The Yemeni Banking Sector's Technology and Innovation Practices," *Seybold Report journal*, vol. 17, no. 10, pp. 2493–2519, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdualmajed A. G. Al-Khulaidi et al., "Information Security Governance: An Exploration Study of Yemeni Banks' Information Security Management Systems," *Seybold Report journal*, vol. 17, no. 10, pp. 133-153, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Yudi Fernando et al., "Cyber Supply Chain Risk Management and Performance in Industry 4.0 era: Information System Security Practices in Malaysia," *Journal of Industrial and Production Engineering*, vol. 40, no. 2, pp. 102–116, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Khairur Razikin, and Benfano Soewito, "Cybersecurity Decision Support Model to Designing Information Technology Security System Based on Risk Analysis and Cybersecurity Framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383-404, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] I.Lakshmi, "A Study on the Internet of Things and Cyber Security with Intruders and Attacks," *International Journal of P2P Network Trends and Technology*, vol. 9, no. 3, pp. 4-13, 2019. [Publisher Link]

[24] Richard Busulwa, *Navigating Digital Transformation in Management, The Digital Business and Digital Transformation Imperatives*, Routledge Taylor & Francis group, 2022. [Publisher Link]

[25] Adel Abdulsalam Nasser, "Information-Analytical Support and Information Modeling of Decision-Making Processes in Various Subsystems of the University," *Modern Scientific Research And Innovation*, no. 8, pp. 4-4, 2011. [Google Scholar]

[26] S. S. Olimov, and D. I. Mamurova, "Information Technology in Education," *Pioneer: Journal of Advanced Research and Scientific Progress*, vol. 1, no. 1, pp. 17-22, 2022. [Publisher Link]

[27] Adel Abdulsalam Nasser, "The Concept of Building an Information System of the University Based on the Structural and Functional Analysis of Information Flows," *Bulletin of APK Upper Volga* 1, pp. 81-85, 2021. [Google Scholar]

[28] Gulamov, A. A., S. N. Mikhailov, and A. A. Nasser, "Model of the processes of information and analytical support of scientific research of the university," *Information-measuring and control systems*, vol. 9, no. 4, pp. 28-31, 2011. [Google Scholar]

[29] Subir Kochar et al., "Enhancing Information Security Risk Management for Organizations," *International Journal of Computer and Organization Trends*, vol. 5, no. 2, pp. 55-59, 2015. [CrossRef] [Publisher Link]

[30] Donghua Chen, and Runtong Zhang, "Exploring Research Trends of Emerging Technologies in Health Metaverse: A Bibliometric Analysis," *SSRN Electronic*, 2022. [Google Scholar] [Publisher Link]

[31] Abed Saif Ahmed Alghawli, Adel A. Nasser, and Mijahed 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, pp. 81-97, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Bobyr M.V., Nasser A.A., and Abduljabbar M., "Research of the Properties of Soft Fuzzy-Logical Inclusion Algorithm," *Proceedings of the Southwestern State University*, vol. 1, pp. 31-49, 2016. [Google Scholar]

[33] G. Saravanan et al., "Implementation of IoT in Production and Manufacturing: An Industry 4.0 approach," *Materials Today: Proceedings*, vol. 5, pp. 2427–2430, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Ibrahim Daud et al., "The Effect of Digital Marketing, Digital Finance and Digital Payment on Finance Performance of Indonesian SMEs," *International Journal of Data and Network Science*, vol. 6, no. 1, pp. 37–44, 2022. [Google Scholar] [Publisher Link]

[35] Roel van Klink et al., "Emerging Technologies Revolutionise Insect Ecology and Monitoring," *Trends in Ecology & Evolution*, vol. 37, no. 10, pp. 872–885, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[36] Miton Abel Konnon et al., "An Extended Layered Information Security Architecture (ELISA) for e-Government in Developing Countries," *International Journal of Engineering Trends and Technology*, vol. 71, no. 1, pp. 109-123, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Tory Cenaj, "Accelerating Digital Health Trends and Transformation through Scientific Communications," *Blockchain in Healthcare Today*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Chat Chuchuen, "The Perception of Mobile Banking Adoption: The Study of Behavioral, Security, and Trust in Thailand," *International Journal of Social Science and Humanity*, vol. 6, no. 7, pp. 547–550, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[39] Chirag Goel, "Information Security Least Privilege Requirement Analysis for SQL Database Backups," *International Journal of Computer Trends and Technology*, vol. 68, no. 1, pp. 35-37, 2020. [CrossRef] [Publisher Link]

[40] John R.S. Fraser, Rob Quail, and Betty J. Simkins, "Questions asked About Enterprise Risk Management by Risk Practitioners," *Business Horizons*, vol. 65, no. 3, pp. 251–260, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[41] Nnatubemugo Innocent Ngwum, "*Information Security Maturity Model (ISMM)*," M.S. thesis, the University of Manchester, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[42] Gulamov, A. A., and A. Nasser, "Information model of university library resources management," *Actual problems of infotelecommunications*, 2010. [Google Scholar]

[43] Adel A. Nasser, M.M. Saeed, and Mijahed 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, 2021. [CrossRef] [Google Scholar] [Publisher Link]