ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

"The Impact of the COSO Internal Control Framework on Reducing Cybersecurity Risks: A Field Study of Banks in Sana'a, Yemen:"

[1]Abdulrahman Emran Ali Mohammed Husin., [2]Dr. Sultan Hassan Mohammed AL-halemi

[1]MA Researcher, Accounting Department, Faculty of Administrative and Humanity Sciences, Saba University, Sana'a, Yemen

[2]Associate Professor, Accounting Department, Faculty of Administrative and Computer Sciences(Radaa), Albaydha University, Albaydha, Yemen

https://doi.org/10.51583/IJLTEMAS.2026.150100069DOI:

Received: 22 January 2026; Accepted: 27 January 2026; Published: 08 February 2026

ABSTRACT

This study examines the impact of the COSO Internal Control Framework on mitigating cybersecurity risks in banks operating in the Republic of Yemen. The study adopts a descriptive–analytical approach due to its suitability for the research objectives. Primary data were collected through a questionnaire administered to financial managers, internal audit managers, and employees working in financial management, internal auditing, and information technology departments. A total of 154 valid responses were analysed.

The findings reveal a statistically significant impact of implementing the COSO framework on reducing cybersecurity risks in Yemeni banks. Specifically, a strong control environment, effective risk assessment, and well-designed control activities enhance banks' ability to address cyber threats and minimize system vulnerabilities. The results also emphasize the critical role of information and communication, as well as continuous monitoring, in strengthening responses to cyberattacks and ensuring compliance with relevant standards and regulations.

Keywords: COSO Framework, Internal Control, Cybersecurity, Yemeni Banks.

INTRODUCTION

The challenges facing the banking sector in the field of cybersecurity have increased due to the rapid digital transformation, making banks a strategic target for attacks that threaten data integrity and trust in the financial system (Abu-Musa, 2022). In this context, the urgent need to adopt regulatory frameworks that ensure business continuity becomes evident.

Rapid digital transformation and the expansion of internet-based financial services have significantly increased cybersecurity threats facing the banking sector. However, these risks may sometimes remain unclear, necessitating that boards of directors and specialized committees seek assistance from internal audit departments to ensure the effectiveness of electronic risk management and cybersecurity. The Republic of Yemen faces cyber challenges that require financial institutions to enhance their security response. In response to these risks, the Central Bank of Yemen issued Circular No. (1) of 2024, which established "the minimum basic cybersecurity requirements to reduce risks to information and technical assets" (Central Bank of Yemen, 2024). These instructions emphasized the necessity for boards of directors to have a clear understanding of cyber threats and to utilize oversight to ensure the effective management of these risks. Here, the importance of "internal control" emerges as a vital supervisory tool; traditional efforts alone are no longer sufficient to meet security requirements. To achieve this effectiveness, the Committee of Sponsoring

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

Organizations of the Treadway Commission (COSO) framework is considered the most globally accepted reference due to its comprehensive and flexible approach to risk management and enhancing internal control (COSO, 2013). In light of these requirements, this study aims to highlight the impact of the COSO framework in mitigating cybersecurity risks in banks operating in the Republic of Yemen.

Study Problem

The current study problem lies in evaluating the effectiveness of implementing the COSO internal control framework in banks operating in the Republic of Yemen in mitigating cybersecurity risks. This is done by exploring the relationship between the components of the COSO framework and the cybersecurity measures adopted, and identifying the gaps and challenges that hinder achieving effective cybersecurity in the Yemeni banking environment, thereby contributing to enhancing internal control and protecting accounting information.

Based on the above, the problem can be summarized in the following questions:

1- To what extent does the COSO framework influence the reduction of cybersecurity risks in banks operating in the Republic of Yemen (control environment, risk assessment, control activities, information and communication, monitoring and follow-up)?

The importance of the study

The importance of the study lies in highlighting the vital role of cybersecurity, a topic that has received increasing attention at both the local and international levels recently. This interest comes in light of the technological advancements being witnessed in business operations, which in turn raise the level of cyber risks and information security. The daily challenge lies in the possibility of security breaches that threaten data, which compels the relevant committees to pressure institutions to clarify their strategies for reducing cyber risks. This pressure serves as a strong incentive for internal auditors to engage in the field of cybersecurity. The focus on efficiently implementing cybersecurity management and reducing its risks is an important factor in preventing technological and cyber disasters. This is achieved by closing security gaps, correcting system deficiencies, and strengthening information security policies, which contributes to supporting the financial stability ofinstitutions.
The importance of this study arises from the urgent need to understand how the COSO framework impacts the reduction of cybersecurity risks in Yemeni banks. Statistics indicate a global increase in cybercrime rates, with banks being among the most affected sectors. In light of the current economic and political conditions in Yemen, the need to enhance cybersecurity becomes more urgent, and the COSO framework can play a vital role in this context.

Study Objectives:

The study aims to achieve the primary and main objective, which is to identify the impact of the COSO framework on cybersecurity in banks operating in the Republic of Yemen.

The following sub-objectives can be derived:

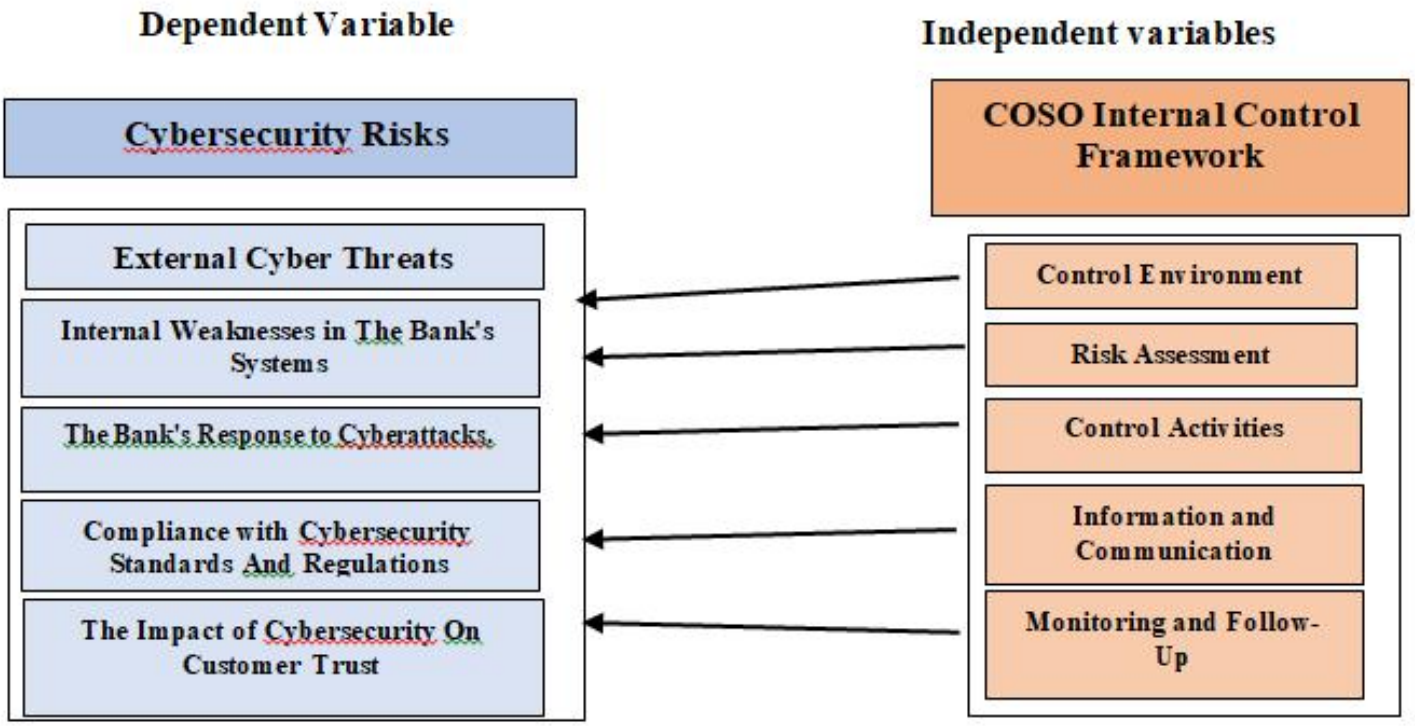
1. Identifying the extent to which the components of the COSO framework (control environment, risk assessment, control activities, information and communication, monitoring and follow-up) reduce cybersecurity risks in banks operating in the Republic of Yemen.

2. Identifying the extent of statistically significant differences among the study sample members regarding the study variables attributed to demographic variables.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

Conceptual Model:

Figure1 The conceptual model of the study



Study Hypotheses:

The Main Hypothesis:

There is no statistically significant impact of the COSO framework on reducing cybersecurity risks in banks operating in the Republic of Yemen.

From the main hypothesis, the following sub-hypotheses are derived:

First sub-hypothesis: There is no impact of the Control Environment on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Second sub-hypothesis: There is no impact of risk assessment on reducing cybersecurity risks in banks operating in the Republic of Yemen.

The third sub-hypothesis: There is no impact of supervisory activities on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Fourth sub-hypothesis: There is no impact of information and communication on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Sub-hypothesis five: There is no impact of monitoring and follow-up on reducing cybersecurity risks in banks operating in the Republic of Yemen.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

LITERATURE REVIEW

The study (Al-Halimi, 2025) primarily aimed to analyze the joint impact of risk-based internal auditing and the internal control system according to the COSO model in mitigating the risks faced by Yemeni banks, with a focus on the crucial role played by the effectiveness of risk management as a mediator, and how cybersecurity practices modify and shape this relationship. The study also relied on the descriptive-analytical approach, where the study population included all banks operating in Yemen, and data were collected from a purposive sample consisting of 134 senior officials and specialists in the relevant fields. The study concluded that the internal control system (COSO) has a direct and strong impact on reducing banking risks, while risk-based internal auditing reduces risks indirectly and completely by enhancing the effectiveness of risk management. The results also showed that cybersecurity practices act as a significant moderator that strengthens this indirect relationship. The study highlighted in its conclusion that the structural and political challenges in Yemen create a fertile environment for risks and limit the effectiveness of traditional regulatory measures.

The study (Ibtihaj, Zahra, 2025) aimed to analyze the role of internal auditing in supporting the recovery of Islamic banks from cyber risks, enhancing business continuity, and improving the banks' ability to handle electronic incidents. The study relied on the descriptive-analytical method, with its community represented by Islamic banks operating in Iraq, and a sample of internal auditors and employees in risk and information technology departments. The results concluded that internal auditing positively contributes to reducing the impact of cyber risks after they occur and improving the efficiency of recovery plans. It also showed a variation in the level of banks' readiness to deal with cyber incidents.

As for the study (Al-Sayed, 2025), it aimed to measure the added value resulting from the internal auditor's assurance on management's claims related to cybersecurity risk management and to enhance the reliability of disclosing these risks. It adopted the descriptive-analytical approach and was applied to a sample of internal auditors and executive management in various organizations. The results showed that the internal auditor's assurance enhances stakeholders' confidence in cybersecurity risk management systems, contributes to improving the level of compliance with control measures, and supports risk governance.

The study (Hanan, 2024) aimed to measure the added value provided by internal audit assurance on management's claims related to cybersecurity risk management and to enhance the reliability of disclosing these risks to stakeholders. The study relied on the descriptive-analytical approach, and its community consisted of organizations that implement internal auditing systems, from which a sample of internal auditors, executive management members, and risk management departments was selected. The results concluded that the internal auditor's assurance positively and statistically significantly contributes to improving the effectiveness of cybersecurity risk management, enhancing the credibility of management claims, and supporting internal control systems and risk governance within organizations.

The study by (Saad, 2022) addressed the impact of internal control on enhancing cybersecurity in the banking sector, with a focus on using the COSO framework. The study found that there is a positive relationship between the application of the components of the COSO framework, such as risk assessment and control activities, and the reduction of cyber vulnerabilities. It concluded with results, the most important of which were noticeable improvements in cybersecurity strategies among banks that rely on the COSO framework, along with recommendations to enhance training for cybersecurity personnel. The study (Jihan, 2022) aimed to clarify the role of internal auditing in reducing cybersecurity risks and their impact on investor decisions by reviewing cybersecurity and identifying the associated risks, as well as explaining the determinants of the quality of internal auditing for cybersecurity. The study also aimed to demonstrate the quality of internal auditing in reducing cybersecurity risks and its effect on investor decisions. The study reached a set of

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

conclusions, the most important of which are that organizations need to expand their skill base and employ qualified personnel to handle technological technologies, and the importance of the internal audit department in providing appropriate information in a rational manner that achieves the highest return in line with investors' needs. It also found a positive relationship between the quality of internal auditing and the reduction of cybersecurity risks.

The study by Amanuel Tadesse & Stephanie M. Walton (2024) aimed to analyze the impact of adopting the COSO internal control framework in reducing cyber intrusions and improving digital risk management. Walton, 2024): aimed to analyze the impact of adopting the COSO internal control framework in reducing cyber intrusions and improving digital risk management. The quantitative analytical approach was adopted using secondary data, applied to listed American companies. The results concluded that companies that implement the components of the COSO framework to a high degree face fewer cyber intrusions and have more efficient internal control systems for early risk detection. The study by Hanwen Chen & Yujie Zhang (2025) to clarify the role of internal control systems based on the COSO framework in improving cybersecurity risk management at the institutional level. I adopted the descriptive-analytical approach and applied it to a sample of public and private institutions. The results showed that the comprehensive application of COSO components contributes to improving the assessment of cyber risks, enhancing supervisory activities, and supporting decision-making related to cybersecurity.

The study by Mark A. Beasley & Dana R. aimed to Hermanson, 2025): To analyze the relationship between cybersecurity governance and the effectiveness of internal control systems, and to clarify the role of senior management in managing digital risks. The descriptive analytical method was adopted and applied to a sample of multi-sector organizations. The results concluded that the presence of effective governance structures enhances the efficiency of internal control systems and contributes to improving the response to cyber risks.

Theoretical Framework

Internal control:

The concept of internal control:

Internal control is defined according to the (COSO) framework as: "A continuous process influenced by the organization's board of directors, executive management, and other employees, designed to provide reasonable assurance regarding the achievement of the organization's objectives related to operations (efficiency and effectiveness of operations), reporting (reliability of financial and non-financial reporting), and compliance (adherence to applicable laws and regulations)." They are not just rigid procedures, but rather a means to achieve an end, not an end in themselves, and they permeate all operational activities of the organization in an integrated manner.

The importance of internal control:

The importance of internal control lies in being the cornerstone of corporate governance, as it works to protect the organization's assets from embezzlement, loss, or misuse. It also contributes to ensuring the accuracy of accounting data and financial records, which raises the level of trust among investors and regulatory bodies. Its utmost importance is highlighted in the context of digital transformation by mitigating the risks arising from electronic data processing, which helps management predict deviations before they occur and address them with high efficiency.

Objectives of internal control:

The internal control aims to achieve three main objectives: First, operational objectives that ensure the effective and economical use of the organization's resources. Secondly, the reporting objectives that ensure the quality and transparency of the financial information provided to stakeholders. Thirdly, the objectives of compliance with laws and internal policies. Additionally, control in the technological environment aims to

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

ensure the safety and confidentiality of information and prevent cyber breaches, thereby enhancing the financial and banking stability of the institution and achieving the sustainability of its operations.

Components of the COSO Internal Control Framework:

The COSO framework consists of five integrated components:

1. The control environment: This is the foundation and includes ethical values, integrity, and the organizational structure. The regulatory environment: It is the foundation and includes ethical values, integrity, and the organizational structure.
2. Risk assessment: Identifying and analyzing the risks that threaten the achievement of objectives (including cyber risks).
3. Supervisory activities: Policies and procedures that ensure the implementation of management directives to mitigate risks. Control activities: Policies and procedures that ensure the implementation of management directives to mitigate risks.
4. Information and communications: Providing and transmitting the necessary information to manage and monitor operations in a timely manner. Information and Communications: Providing and transmitting the necessary information for managing and monitoring operations in a timely manner.
5. Monitoring activities: Continuous and periodic evaluation of the control system's performance to ensure its quality and effectiveness over time. Monitoring activities: Continuous and periodic evaluation of the performance of the control system to ensure its quality and effectiveness over time.

The concept of cybersecurity:

Cybersecurity is defined as "a set of technical, administrative, and educational measures used to prevent unauthorized use and misuse, and to recover electronic information and the communication systems that contain it, with the aim of ensuring their availability and continuity, protecting the privacy and confidentiality of data, and safeguarding information from modification or alteration."

The importance of cybersecurity:

Its importance lies in being the protective shield for banks in the era of digital transformation, as it works to safeguard digital assets and sensitive customer data from theft or manipulation. It also contributes to ensuring the continuity of banking operations without interruption, maintaining the corporate reputation, and enhancing the trust of depositors and investors in the electronic financial system.

Types of cybersecurity:

Cybersecurity in financial institutions has branched out into several areas, the most prominent of which are: network security (path protection), application security (software protection), and information security (data confidentiality protection), in addition to operations security (permissions and access management), and disaster recovery which ensures the retrieval of lost data after any attack.

Cybersecurity risks:

These risks represent threats targeting electronic systems, such as malware, denial-of-service (DoS) attacks that disrupt bank systems, phishing attempts to steal customer data, in addition to the risks of internal threats resulting from weak permissions or human negligence.

Mechanisms for enhancing cybersecurity:

The mechanisms for enhancing cybersecurity lie in the integration of technical requirements with administrative controls; the COSO framework serves as a comprehensive system that ensures the effectiveness of these mechanisms by embedding them within the bank's organizational structure. The

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

adoption of strict security policies and the use of advanced encryption technologies represent "executive control activities," while the activation of early detection systems and continuous training for human resources fall under the "control environment" and "information and communication." This linkage achieves the "defense in depth" strategy, where protection is not limited to technical tools alone, but extends to institutional oversight that ensures the continuity of digital readiness and the bank's ability to confront cyber threats, providing reasonable assurance for the protection of assets and data.

STUDY METHODOLOGY

To achieve the objectives of the study, the descriptive-analytical approach was employed. This approach is defined by Obeidat et al. (2020, p. 70) and Al-Assaf (2012, p. 20) as "a method that relies on collecting information and data about a particular phenomenon or event within a given reality, with the aim of identifying and understanding the studied phenomenon, determining its current status, and identifying its strengths and weaknesses in order to assess the suitability of the current situation or the need to introduce partial or fundamental changes."

A questionnaire specifically designed for this purpose was used as the primary tool for data collection. The collected data were statistically analyzed to obtain appropriate answers and to test the study hypotheses. The descriptive approach was selected due to its suitability for the nature of the study and its objectives, as well as its ability to provide accurate descriptions and analyses of the sample respondents' responses.

To analyze the data and test the proposed hypotheses, the Statistical Package for the Social Sciences (SPSS), version 25, was utilized.

Field study:

Based on the study's problem and objectives, the target population consists of employees working in banks operating in Yemen within their main centers in the capital, Sana'a, which number (22) banks according to the Central Bank of Yemen (Sana'a) statistics for the year 2023. The sample consisted of all employees in the main branches of Yemeni banks operating in Sana'a. As for the unit of analysis, it was carefully selected from bank specialists, totaling 460 employees working in the following positions: financial managers, internal audit managers, financial administration employees, internal audit employees, information technology management, and cybersecurity. Referring to the Krejcie & Morgan table, the researcher found that the appropriate sample size consists of 210 individuals. Therefore, 220 questionnaires were prepared and distributed to the respondents, of which only 167 were retrieved. Upon examining the retrieved questionnaires, it was found that 13 were invalid for analysis. Thus, the number of questionnaires approved for statistical analysis was 154, which is 73% of the distributed questionnaires.

Reliability of the Study:

To ensure the reliability of the study variables and the validity of the sample's responses, Cronbach's Alpha coefficient was employed. This method is based on the internal consistency of respondents' performance across questionnaire items and reflects the strength of correlation and coherence among the questionnaire statements. Although there are no strict standard rules regarding acceptable Alpha values, from a practical perspective, an Alpha value greater than 0.60 ($\alpha > 0.60$) is considered acceptable in research related to the human, social, and financial sciences (Al-Najjar & Al-Zoghbi, 2013).

This test assumes that the responses of the sample should be relatively consistent with one another. The greater the similarity among respondents' answers, the higher the level of reliability. The minimum acceptable level for confirming the reliability of the questionnaire is 0.60 or above. If the reliability coefficient falls below this threshold, the questionnaire should be redistributed to a sample that is more consistent with the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

subject of the study. Moreover, the closer the value of Cronbach's Alpha is to one, the greater the consistency of the sample's opinions, indicating a unified perspective regarding their responses to the questionnaire items.

Table (1) presents the results of the Cronbach's Alpha reliability test.

Table No. (1) Cronbach's alpha reliability coefficient for the study axes and the tool as a whole

Variable	The No of Questions	Sig.	Alpha Coefficient Value
1	7	0.000	.869
2	7	0.000	.846
3	6	0.000	.896
4	6	0.000	.911
5	6	0.000	.910
6	11	0.000	.941
Total	43	**0.000**	**.977**

It is evident from Table (1) that the reliability coefficient (Cronbach's alpha) is high for all axes, ranging between (0.846-0.941). The overall reliability score for all questionnaire items is (0.977). This indicates that the study population is homogeneous in their responses to the questionnaire, and it also suggests that the sample's opinion is consistent. The community's opinion would also remain stable even if the questionnaires were distributed to a larger number of community members. Thus, the validity and reliability of the study questionnaire in analyzing results, answering research questions, and testing hypotheses have been confirmed.

The number of retrieved questionnaires was 154. To verify whether the sample data follow a normal distribution, the Kolmogorov–Smirnov test was applied across all dimensions of the questionnaire. The results of this test are presented in the following table.

Table No. (2) Results of the normality test for the study sample

Variable	The No of Questions	Sig.	Z
1	7	0.000	.176
2	7	0.000	.158
3	6	0.000	.282
4	6	0.000	.237
5	6	0.000	.281
6	11	0.000	.290
Total	43	**0.000**	**.234**

It is clear from Table (2) that the value of the distribution index (Z) ranged between (0.290-0.158) for the study axes, and the overall distribution index for all axes was (0.234). All these values were statistically significant at the significance level (0.05), indicating that the data follow a normal distribution.

Descriptive statistics:

First: Analysis of the descriptive statistics results for the regulatory environment axis, Table No. (3)

Table No. (3) The means, standard deviations, and ranks for the regulatory environment axis.

NO.	Paragraph	MEAN	S.D	Rank

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

1	The existence of written and approved cybersecurity policies by senior management that are applied regularly.	4.52	.734	2
2	Implementing periodic training programs to raise employees' awareness of cybersecurity risks.	4.47	.768	3
3	The presence of a clear and documented separation of tasks in sensitive systems to reduce the likelihood of manipulation or fraud.	4.58	.625	1
4	Written regulations provide clear definitions of data and sensitive system usage permissions.	4.40	.829	4
5	Top management is committed to continuously monitoring cyber risk assessment reports.	4.34	.858	6
6	The presence of an internal audit system to monitor compliance with security policies.	4.33	.687	7
	The senior management monitors the implementation of internal control on the ground and issues periodic reports on it.	4.36	.822	5
	Total	4.52	.734	2

Notice from Table (3) that the arithmetic means for all the items in the axis ranged between (4.33- 4.58), which is higher than the adopted hypothetical mean (3), indicating that all sample members agree with the items included in the axis. It is also noted that item number (3), which states, "the existence of a clear and documented separation of tasks in sensitive systems to reduce the likelihood of manipulation or fraud," It ranked first in the axis with a mean of (4.58) and a standard deviation of (0.625), indicating the sample members' agreement with the content of the paragraph and the consistency and harmony of their responses. The researcher attributes this to the importance of task separation in providing a sound supervisory environment. Paragraph number (6), which states "the existence of an internal audit system to monitor compliance with security policies," ranked last in the axis with a mean of (4.33) and a standard deviation of (0.687), indicating the sample members' agreement with the content of the paragraph as well as the consistency and harmony of their responses. The researcher attributes this to the importance of having an internal audit system to monitor compliance with security policies. In the last position within the axis, with a mean of (4.33) and a standard deviation of (0.687), indicating the sample members' agreement with the paragraph as well as the consistency and coherence of their responses. The researcher attributes this to the importance of having an internal auditing system specifically for monitoring compliance with security policies. The lower ranking of this paragraph compared to others may be due to the nature of the rapidly evolving and accelerating cyber risks and the difficulty of updating security policies at the same pace. As for the ranking of the axes, the "supervisory environment" axis achieved an average score of (4.4276), which is the fifth highest average score among all the axes.

Secondly: Analysis of the descriptive statistics results for the risk assessment axis, Table No. (4).

Table No. (4) The means, standard deviations, and ranks for the risk assessment axis

NO.	Paragraph	Mean	S.D	Rank
1	The existence of a formal written mechanism for continuous risk assessment.	4.42	.790	4
2	The existence of risk analysis reports that	4.43	.722	3

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

	outline potential threats.			
3	Written plans for responding to cyber emergencies are provided, and employees are trained on them.	4.31	.979	6
4	The existence of a risk classification system (low, medium, high) with documented results.	4.41	.829	5
5	Involving different departments in continuously preparing risk assessment reports.	4.27	.833	7
6	The presence of data analysis programs to monitor potential security threats.	4.48	.818	2
7	The existence of risk assessment reports when introducing any new technology.	4.60	.651	1
All Dimensions Combined		4.4156	.58307	*5

Table (3) indicates that the arithmetic means ranged between (4.27–4.60), which is higher than the hypothesized mean adopted in the study (3), and the standard deviations for each item in the "Risk Assessment" axis, indicating the sample members' agreement with the items included in the axis, as well as the consistency and coherence of the sample members' responses, which were concentrated on agreement. It is also noted from Table (3-15) that item number (7), which states "the existence of risk assessment reports when introducing any new technology," It ranked first in the axis with a mean of (4.60) and a standard deviation of (0.651), while paragraph (5) "Involving different departments in continuously preparing risk assessment reports" ranked last in the axis with a mean of (4.27) and a standard deviation of (0.833). In the last position at the level of the axis with an arithmetic mean of (4.27) and a standard deviation of (0.833), which indicates a consensus among the sample members regarding the paragraph. It is worth noting that the axis achieved the sixth highest arithmetic mean among all the axes.

Thirdly: Analysis of the descriptive statistics results for the supervisory activities axis, Table No. (5)

Table No. (5) The arithmetic means, standard deviations, and ranks for the axis of supervisory activities.

NO	Paragraph	Mean	S.D	Rank
1	The presence of a permissions system that precisely determines who can access sensitive data.	4.55	.733	4
2	The presence of continuous internal audits covering sensitive banking operations.	4.61	.608	2
3	The existence of written policies that define the prevention of unauthorized access with a monitoring system.	4.53	.751	5
4	The presence of a technical system that prevents the installation of unauthorized software.	4.59	.746	3
5	Conducting penetration tests or periodic security audits of the system.	4.42	.846	6

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

6	Having a work plan to continuously update security systems.	4.63	.615	1
All Dimensions Combined		4.5530	.58476	*1

We notice from Table (5) that the arithmetic means for this axis ranged between (4.42–4.63), which are higher than the adopted hypothetical mean (3), indicating that all sample members agreed with the items included in the axis. Additionally, the overall mean for the axis reached (4.5530), which indicates the sample members' agreement with the items included in the axis. The standard deviation for the entire axis reached (0.58476), indicating the consistency and agreement of the respondents' answers regarding the items included in the axis, meaning that the answers were centered around agreement. It is also noted from Table (5) that item number (6), which states "the existence of a work plan to continuously update protection systems," It ranked first in the axis with a mean of (4.63) and a standard deviation of (0.615), while paragraph number (5), which states "conducting penetration tests or periodic security reviews of the system," ranked last in the axis. In the last position within the axis, with a mean of (4.42) and a standard deviation of (0.846), indicating a consensus among the sample members regarding the items of the effective management axis based on prior planning, as well as the consistency of the responses and their concentration in agreement. The axis as a whole ranked first with the highest mean.

Fourth: Analysis of the descriptive statistics results for the information and communication axis number (6)

Table No. (6) The means, standard deviations, and ranks for the information and communication axis.

NO	Paragraph	Mean	S.D	Rank
1	The presence of a clear internal reporting mechanism for immediate incident reporting.	4.61	.629	1
2	The presence of ongoing meetings between departments to discuss security challenges.	4.31	.888	5
3	The presence of a monitoring system that measures the level of adherence to security procedures.	4.52	.743	4
4	The existence of an official policy for reporting suspicious activities with 8 guaranteed confidentiality for the informant.	4.53	.734	2
5	The existence of official communication channels between employees and management regarding security incidents.	4.53	.751	3
6	The existence of a written plan to update information systems according to a schedule.	4.31	.966	6
All Dimensions Combined		4.4665	.65910	*4

Table (3) indicates that the arithmetic means for this axis ranged between (4.31-4.61), which are higher than the adopted hypothetical mean (3), indicating that all sample members agreed with the items included in the axis. It is also noted that item number (1), which states "the existence of a clear internal reporting mechanism for immediate incident reporting," It ranked first in the axis with a mean of (4.61) and a standard deviation of (0.629). The researcher attributes this to the importance of the internal reporting mechanism in solving problems arising from cyber risks and avoiding their recurrence. Paragraph number (6), which states "the existence of a written plan to update information systems according to a schedule," also ranked last in the axis. In the last position at the axis level with a mean of (4.31) and a standard deviation of (0.888), which indicates a consensus among the sample members regarding the content of the paragraph. The axis as a whole ranked fourth with the highest mean.

Fifth: Analysis of the descriptive statistics results for the monitoring and follow-up axis, Table No. (7)

Table No. (7) The means, standard deviations, and ranks for the monitoring and follow-up axis.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

NO	Paragraph	Mean	S.D	Rank
1	The existence of periodic review reports for banking operations to monitor risks.	4.57	.645	2
2	The presence of internal and external audits measuring the bank's compliance with cybersecurity standards.	4.59	.622	1
3	The existence of written reports to review security strategies annually.	4.51	.707	3
4	The existence of official reports clarifying the gaps and remedial actions.	4.50	.659	4
5	The existence of benchmark comparison reports with other banks.	4.44	.758	5
6	The presence of practical training and periodic simulations to test emergency plans.	4.36	.981	6
All Dimensions Combined		4.4946	.61316	*3

Table (3) indicates that the arithmetic means for this axis ranged between (4.36-4.59), which is higher than the adopted hypothetical mean (3), indicating that all sample members agreed with the items included in the axis. It is also noted that item number (2), which states "the presence of internal and external reviews measuring the bank's compliance with cybersecurity standards," It ranked first in the axis with a mean of (4.59) and a standard deviation of (0.622), while item number (6), which states "the presence of practical training and periodic simulations to test emergency plans," ranked last in the axis. In the last place at the level of the axis, with a mean of (4.36) and a standard deviation of (0.981), indicating a consensus among the sample members regarding the content of the item. Overall, the general average for the entire axis was (4.4946) with a standard deviation of (0.61316), indicating the sample members' agreement with the content of the axis items, as well as the consistency and concentration of responses in agreement. The entire axis received the third highest mean among the axes.

Sixth: Analysis of the descriptive statistics results for the dependent variable cybersecurity Table No. (8)

Table No. (8) The means, standard deviations, and ranks for the dependent variable cybersecurity.

NO	Paragraph	Mean	S.D	Rank
1	The bank has clear and regularly updated cybersecurity policies and procedures.	4.60	.661	3
2	Strict policies are implemented to protect sensitive data from breaches.	4.55	.658	5
3	Two-factor authentication policies are enforced when logging into sensitive systems.	4.42	.934	10
4	Employees are prohibited from using personal devices to access the bank's systems.	4.62	.688	2
5	All unauthorized access attempts are documented and analyzed.	4.47	.849	9
6	The bank has a strong technological infrastructure that supports cybersecurity requirements.	4.52	.734	7

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

7	The bank uses advanced systems to monitor cyber threats and attacks in real-time.	4.58	.693	4
8	The bank's protection systems and software are continuously and effectively updated.	4.62	.667	1
9	Periodic tests are conducted on the systems' readiness to face cyberattacks based on the latest security threats.	4.49	.777	8
10	Effective encryption tools are available to protect sensitive data in the bank.	4.38	.894	11
11	Regular backup mechanisms are implemented to ensure quick data recovery when needed.	4.55	.723	6
All Dimensions Combined		4.5277	.60222	*2

Table (3) indicates that the arithmetic means for this axis ranged between (4.38-4.62), with the overall mean for the axis as a whole reaching (4.5277), which is higher than the adopted hypothetical mean (3) with a standard deviation of (0.60222). This indicates that all sample members agreed with the items included in the axis, in addition to the homogeneity and consistency of the responses, which were concentrated in agreement. It is also noted that item number (8), which states "The bank's protection systems and software are continuously and effectively updated," ranked first in the axis with an arithmetic mean of (4.62) and a standard deviation of (0.667). It ranked first in the axis with a mean of (4.62) and a standard deviation of (0.667), while item number (10), which states "effective encryption tools are available to protect sensitive data in the bank," ranked last in the axis with a mean of (4.38) and a standard deviation of (0.894). In the last position at the level of the axis with a mean of (4.38) and a standard deviation of (0.894), which means there is an agreement in the opinions of the sample members regarding the paragraph, and the axis as a whole received the second highest mean among the axes.

HYPOTHESES TESTING AND DISCUSSION OF RESULTS

• Result of testing the first sub-hypothesis of the first main hypothesis:

Null Hypothesis Ho.a: There is no effect of the supervisory environment in reducing cybersecurity risks in banks operating in the Republic of Yemen.

This hypothesis aims to measure the impact of the regulatory environment on reducing cybersecurity risks, and simple linear regression analysis was used, as shown in Table (9).

Table No. (9) Result of the simple linear regression analysis for the first sub-hypothesis

		ANOVA		T-test		
(R)	(R2)	(F) value	SIG.F	(B)	(T) value	SIG.T
0.701a	0.498	150.792	0.000	0.706	12.280	0.000

It is evident from Table (10) that there is a statistically significant effect of risk assessment on reducing cybersecurity risks. The value of the correlation coefficient (R) reached 0.701, while the coefficient of determination (R^2) amounted to 0.498. This indicates that 49.8% of the variance in the level of cybersecurity risk reduction is attributable to changes in the level of risk assessment practices, whereas 50.8% of the variance is explained by other factors.

Furthermore, the linear regression coefficient (B) was 0.706, indicating that a one-unit increase in the level of risk assessment leads to an increase of 0.706 in the level of cybersecurity risk reduction. In addition, the significance level (p-value) was 0.000, which is lower than the adopted significance level of 0.05.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

Accordingly, the null hypothesis is rejected and the alternative hypothesis is accepted, confirming that risk assessment has a significant effect on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Result of the third sub-hypothesis test of the first main hypothesis:

Null Hypothesis H.o: There is no effect of regulatory activities in reducing cybersecurity risks in banks operating in the Republic of Yemen.

This hypothesis aims to measure the impact of regulatory activities in reducing cybersecurity risks in banks operating in the Republic of Yemen, and a simple linear regression test was used, as shown in Table (11).

Table No. (11) Results of the simple linear regression analysis for the third sub-hypothesis

		ANOVA		T-test		
(R)	(R2)	(F) value	SIG.F	(B)	(T) value	SIG.T
0.752a	0.566	198.306	0.000	0.752	14.082	0.000

It is evident from Table (11) that there is a statistically significant effect of control activities on reducing cybersecurity risks. The value of the correlation coefficient (R) was 0.752, while the coefficient of determination (R^2) reached 0.566. This indicates that 56.6% of the variance in the level of cybersecurity risk reduction is explained by changes in the level of control activities practices, whereas 43.4% of the variance is attributable to other factors.

Moreover, the linear regression coefficient (B) amounted to 0.752, indicating that a one-unit increase in the level of control activities leads to an increase of 0.752 in the level of cybersecurity risk reduction. In addition, the significance level (p-value) was 0.000, which is lower than the adopted significance level of 0.05. Accordingly, the null hypothesis is rejected, and the alternative hypothesis is accepted, confirming that control activities have a statistically significant effect on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Result of the fourth sub-hypothesis test of the first main hypothesis:

Null hypothesis H.o.d: There is no effect of information and communication in reducing cybersecurity risks in banks operating in the Republic of Yemen.

This hypothesis aims to measure the impact of using information and communication in reducing cybersecurity risks in banks operating in the Republic of Yemen. A simple linear regression test was used, as shown in Table (12).

Table No. (12) Results of the simple linear regression analysis for the fourth sub-hypothesis

		ANOVA		T-test		
(R)	(R2)	(F) value	SIG.F	(B)	(T) value	SIG.T
0.812[a]	0.659	294.375	0.000	17.157	17.157	0.000

It is evident from Table (12) that there is a statistically significant effect of information and communication on reducing cybersecurity risks. The value of the correlation coefficient (R) reached 0.812, while the coefficient of determination (R^2) amounted to 0.659. This indicates that 65.9% of the variance in the level of cybersecurity risk reduction is attributable to changes in the level of information and communication practices, whereas 34.1% of the variance is explained by other factors.

Furthermore, the linear regression coefficient (B) was 0.752, indicating that a one-unit increase in the level of information and communication usage leads to an increase of 0.752 in the level of cybersecurity risk reduction. In addition, the significance level (p-value) was 0.000, which is lower than the adopted significance

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

level of 0.05. Accordingly, the null hypothesis is rejected and the alternative hypothesis is accepted, confirming that information and communication have a statistically significant effect on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Result of the fifth sub-hypothesis test of the first main hypothesis:

Null Hypothesis H.o.e: There is no effect of monitoring and follow-up in reducing cybersecurity risks in banks operating in the Republic of Yemen.

This hypothesis aims to measure the impact of monitoring and follow-up in reducing cybersecurity risks in banks operating in the Republic of Yemen, and a simple linear regression test was used, as shown in Table (13).

Table No. (13) Results of the simple linear regression analysis for the fifth sub-hypothesis

		ANOVA		T-test		
(R)	(R2)	(F) value	SIG.F	(B)	(T) value	SIG.T
0.831[a]	0.690	338.784	0.000	0.831	18.406	0.000

It is evident from Table (13) that there is a statistically significant effect of monitoring and follow-up on reducing cybersecurity risks. The value of the correlation coefficient (R) reached 0.831, while the coefficient of determination (R^2) amounted to 0.690. This indicates that 69.0% of the variance in the level of cybersecurity risk reduction is attributable to changes in the level of monitoring and follow-up practices, whereas 31.0% of the variance is explained by other factors.

Moreover, the linear regression coefficient (B) was 0.831, indicating that a one-unit increase in the level of monitoring and follow-up leads to an increase of 0.831 in the level of cybersecurity risk reduction. In addition, the significance level (p-value) was 0.000, which is lower than the adopted significance level of 0.05. Accordingly, the null hypothesis is rejected and the alternative hypothesis is accepted, confirming that monitoring and follow-up have a statistically significant effect on reducing cybersecurity risks in banks operating in the Republic of Yemen.

Result of the first main hypothesis test using multiple linear regression:

Null hypothesis H.o: There is no statistically significant effect of the COSO internal control framework in reducing cybersecurity risks in banks operating in the Republic of Yemen.

This hypothesis aims to determine the impact of applying the COSO internal control framework in reducing cybersecurity risks in banks operating in the Republic of Yemen.

The multiple linear regression test was used, as shown in Table (14), which considered the COSO framework (control environment, risk assessment, control activities, information and communication, monitoring and follow-up) as independent variables and the reduction of cybersecurity risks as the dependent variable.

Table No. (14) Results of the multiple linear regression analysis between the COSO internal control framework with its five components in mitigating cybersecurity risk

Monitoring And Follow-Up	Information And Communication	Control Activities	Risk Assessment	Control Environment	Coso Internal Control Framework	
0	0.872	0.003	0.04	0	T-TEST	SIG. (T)
3.709	0.162	3.076	2.074	8.472		T-test
0.285	0.013	0.189	0.143	0.643		β

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

0.000b			ANOVA SIG.(F)
138.024			value F-test
Df3	Df2	Df1	df.
153	148	5	
0.823			R2
0.907b			R
COSO Internal Control Framework			dependent variable
Reducing cybersecurity risks			independent variable

We find from Table (14) the results of the multiple linear regression analysis between the axis of the independent variable, the COSO framework with its five components, in reducing cybersecurity risks in banks operating in the Republic of Yemen. The results of the multiple linear regression analysis showed that the value of (F) reached (138.024) with a statistical significance of (0.000), which is less than the significance level (0.05 < a) at a confidence level of (0.95). We also find that the correlation coefficient (R) value reached (0.907), indicating the impact of the COSO internal control framework in reducing cybersecurity risks in banks operating in the Republic of Yemen, and the coefficient of determination (R2) value reached (0.823). This means that 0.823 of the changes in reducing cybersecurity risks are attributed to the implementation of the COSO internal control framework.

The axes were ranked according to the results of the multiple linear regression. In the first place, the "control environment" axis with a coefficient (B) of (0.643) and a statistical significance of (0.000). In the second place, the "monitoring and follow-up" axis with a coefficient (B) of (0.285) and a statistical significance of (0.000). In the third place, the "control activities" axis with a coefficient (B) of (0.285) and a statistical significance of (0.000). In the fourth place, the "risk assessment" axis with a coefficient (B) of (0.143) and a statistical significance of (0.040). As for the "information and communication" axis, it was excluded as it received a coefficient (B) of (0.013) and a statistical significance of (0.872), which is not statistically significant as it is higher than the adopted significance level (0.05).

Results

A- There is a practice of the (COSO) internal control framework to mitigate cybersecurity risks in banks operating in Yemen at a rate of 87.40%.

1- The banks operating in Yemen provide a regulatory environment to mitigate cybersecurity risks at a rate of 88.55%, and the most important methods include the following:

- There is a clear and documented separation of tasks in sensitive systems to reduce the likelihood of manipulation and fraud.
- The existence of written and approved cybersecurity policies by senior management that are applied regularly.
- Implementing periodic programs to raise employee awareness of cybersecurity risks.

2 - Banks operating in Yemen implement risk assessments to mitigate cybersecurity risks at a rate of 88.31%, and the most important methods include the following:

- The existence of risk assessment reports when introducing any new technology.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

• The presence of data analysis programs to monitor potential security threats.

Existence of risk analysis reports that clarify potential threats.

3 - The banks operating in Yemen engage in regulatory activities to mitigate cybersecurity risks at a rate of 91.06%, and the most significant activities include the following:

• There is a work plan to continuously update protection systems.

• Continuous internal audits covering sensitive banking operations.

• The presence of a technical system that prevents the installation of unauthorized software.

4 - Banks operating in Yemen use information and communication to mitigate cybersecurity risks at a rate of 89.33%, and the most important methods were the following:

• The presence of a clear internal reporting mechanism for immediate incident reporting.

• The existence of an official policy for reporting suspicious activities with guaranteed confidentiality for the informant.

• Existence of official communication channels between employees and management regarding security incidents.

5 - Banks operating in Yemen practice monitoring and follow-up to mitigate cybersecurity risks at a rate of 89.89%, and the most important methods include the following:

• The presence of internal and external audits that measure the bank's compliance with cybersecurity standards.

• Existence of periodic review reports for banking operations to monitor risks.

• The existence of written reports for the annual review of security strategies.

B -There is a statistically significant impact of the COSO internal control framework in reducing cybersecurity risks in banks operating in Yemen, at a rate of 90.7%.

1- There is a statistically significant impact of the control environment in reducing cybersecurity risks in banks operating in Yemen at a rate of 86.7%.

2- There is a statistically significant impact of risk assessment in reducing cybersecurity risks in banks operating in Yemen at a rate of 70.1%.

3- There is a statistically significant impact of supervisory activities in reducing cybersecurity risks in banks operating in Yemen at a rate of 75.2%.

4- There is a statistically significant impact of information and communication in reducing cybersecurity risks in banks operating in Yemen at a rate of 81.2%.

5- There is a statistically significant impact of monitoring and follow-up in reducing cybersecurity risks in banks operating in Yemen, at a rate of 83.1%.

C- There are statistically significant differences in the opinions of the study sample regarding the research variables attributed to demographic factors.

1- The study sample was consistent in its opinions regarding the study variables based on the age variable.
2- The study sample was inconsistent in their opinions regarding the risk assessment axis based on the b variable of educational qualification, as they differed on the risk assessment axis. This may be due to their perception of the concept of risk assessment in general, which is influenced by educational qualification.
3- The study sample was inconsistent in its opinions regarding all study axes based on the variable of job title, which is attributed to the impact of the nature of the job on the comprehension and understanding of the study axes.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

4- The study sample was inconsistent in its opinions regarding the axes (regulatory environment, regulatory activities, information and communication, monitoring and follow-up, cybersecurity) based on the variable of years of experience.

Recommendations:

1- The necessity of improving the regulatory environment thru: establishing a strong internal system to monitor security policies, having senior management continuously review cyber risk assessment reports, and working on preparing an appropriate infrastructure.

2- Enhancing risk assessment activities thru: involving various departments in the continuous preparation of risk assessment reports, and the necessity of creating written plans for responding to cyber emergencies, which employees are trained on.

3- Enhancing supervisory activities thru: conducting penetration tests or periodic security audits, and working on disseminating written policies that define the prevention of unauthorized access with a monitoring system.

4- Enhancing the use of information and communication between different departments: by creating written plans to update information systems according to a timeline, and holding continuous meetings between departments to discuss challenges and develop solutions.

5- Enhancing monitoring and follow-up activities: By working on activating practical training and periodic simulations to test emergency plans, and submitting benchmark comparison reports with other banks.

6- The study recommends that banks operating in the Republic of Yemen adhere to the instructions and directives of the Central Bank of Yemen related to cybersecurity, and work on systematically implementing them within their internal policies and procedures, which contributes to enhancing the protection of electronic systems and accounting information systems and reducing cybersecurity risks.

7- The study recommends that the Central Bank of Yemen keep pace with the rapid developments in the field of cybersecurity by periodically updating relevant instructions, regulations, and guidelines in accordance with technological advancements and international best practices, thereby enhancing the effectiveness of supervision and oversight of banks.

REFERENCES

1. Abdullah, M., et al. (2018). Accounting control systems and firm performance. *International Journal of Accounting Research, 6*(2), 1–9.
2. Abu Al-Khair, M. H. (2023). The impact of internal audit quality on reducing cyber risks to support financial stability in electronic banks (Field study). *Scientific Journal of Financial and Administrative Studies and Research*, (1), 15–17.
3. Abu Kamil, M. A. (2011). *Development of internal control tools aimed at protecting electronically prepared data in banks operating in the Gaza Strip* (Master's thesis). Islamic University, Gaza.
4. Abu Mayaleh, S. (2017). Impact of structuring internal control systems on improving the quality of external auditor performance in accordance with COSO model. *Technical Research Journal, 5*(1), 1–15.
5. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics, 11*(1).
6. Al-Baghdadi, M. F. E.-S. (2021). The economics of cybersecurity in the banking sector. *Journal of Legal and Economic Research*, 76, 1446–1513.
7. Al-Dardour, H. (2023). The efficiency of internal control in improving financial performance. *The Arab Journal of Scientific Publishing*, (62).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

8. Al-Fadl, A. A. M. A. (2024). The impact of cybersecurity spending on performance in Egyptian commercial banks. *Journal of Contemporary Business Studies, 10*(17), 1852–1906.
9. Al-Hakeem, M. A. (2010). *The possibility of controlling automated accounting information systems* (Master's thesis). University of Damascus.
10. Al-Halemi, S. H. M. A. (2025). The impact of internal auditing and risk-based controls on reducing banking risks. *International Journal of Scientific Development and Research, 10*(12).
11. Al-Rahhamna, R. (2023). *The impact of internal control and auditing on the financial performance of commercial banks* (Master's thesis). Philadelphia University.
12. Al-Sawalha, R. A. (2021). *The impact of the internal control system structure according to the COSO framework* (Master's thesis). Isra University.
13. Amerham, J. A. (2022). The impact of internal audit quality on reducing cybersecurity risks. *Journal of Financial and Commercial Research, 23*(3), 325–377.
14. Benaroch, M. (2020). Cybersecurity risk in IT outsourcing. In *Information systems outsourcing* (pp. 313–334).
15. Berk, R., Heidari, H., Jabbari, S., Kearns, M., & Roth, A. (2021). Fairness in criminal justice risk assessments. *Sociological Methods & Research, 50*(1), 3–44.
16. Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management. *Procedia Computer Science, 149*, 65–70.
17. Bouche, R., & Owens, R. (2024). *The role of internal control within cybersecurity based on the COSO-ERM model* (Unpublished manuscript). Universidad UNIDOS.
18. Brian, J. (2020). *Internal control and corporate governance*. McGraw-Hill.
19. Buras, M., & Chihawi, A. (2021). *The importance of evaluating the internal control system*. Al-Khaldounia House.
20. Carballal, A., Galego-Carro, J. P., Rodriguez-Fernandez, N., & Fernandez-Lozano, C. (2022). Wi-Fi handshake analysis. *PeerJ Computer Science, 8*, e1185.
21. Castaner, X., & Oliveira, N. (2020). Strategic control and performance. *Strategic Management Journal, 41*(2), 225–246.
22. Crutzen, N., et al. (2017). Management control systems and performance. *Management Accounting Research, 35*, 15–30.
23. de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness. *Government Information Quarterly, 34*(1), 1–7.
24. Elegado, A. N. (2023). Development of 6G network security. *Innovatus Journal, 6*(1), 1–6.
25. Florackis, C., Louca, C., Michaely, R., & Weber, M. (2022). Cybersecurity risk. *NBER Working Paper No. 28196*.
26. Frazer, L. (2020). Internal accounting control systems. *Accounting Review, 95*(3), 89–112.
27. Furnell, S. (2019). Password meters accuracy. *Computer Fraud & Security, 2019*(11), 6–14.
28. Geeng, C., Harris, M., Redmiles, E., & Roesner, F. (2022). Experiences with online security advice. In *USENIX Security Symposium* (pp. 305–322).
29. Ghelani, D. (2022). Cyber security threats and future perspectives. *Authorea Preprints*.
30. Goloshchapova, L., et al. (2017). Internal control and risk management. *Journal of Economic Studies, 44*(6), 900–915.
31. Haas, T. C. (2023). Adapting cybersecurity practice. *Journal of Cybersecurity, 9*(1), tyad004.
32. Hall, J., Sarkani, S., & Mazzuchi, T. (2011). Organizational capabilities in information security. *Information Management & Computer Security, 19*(3), 155–176.
33. Hamada, A. M. (2010). *General control measures on electronic accounting information systems* (Master's thesis). University of Damascus.
34. Hussein, A. (2019). Internal control tools and cybersecurity risk management. *Journal of Financial Research, 8*(1), 101–130.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue I, January 2026

35. Jabr, G. J. (2023). Cybersecurity threats to electronic banks. *Academic Journal of Social Sciences*, (1), 53–70.
36. Khaled, M. (2016). *Internal control in the context of electronic accounting systems*. Dar Al-Fikr Al-Jami'i.
37. Le, N. T., Vu, L. T., & Nguyen, T. V. (2021). Internal control systems as anti-corruption practices. *Baltic Journal of Management, 16*(2), 173–189.
38. Luburić, R. (2017). Three lines of defence. *Journal of Central Banking Theory and Practice, 6*(1), 29–53.
39. Maqsood, S., & Chiasson, S. (2021). Cybersecurity literacy game. *ACM TOPS, 24*(4), 1–37.
40. Mohamed, A., & Ahmed, S. (2022). Internal control and cybersecurity in banks. *Journal of Accounting Research, 14*(2), 90–120.
41. Moussa Aich, & Khemoud, M. (2023). *Cybersecurity* (Master's thesis). Mouloud Mammeri University.
42. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).
43. Rajab Jadallah Khalaf Hamid. (2020). *Evaluation of internal control system procedures* (High diploma research). University of Mosul.
44. Rajawat, A. S., et al. (2021). Securing 5G-IoT connectivity. *Mathematical Problems in Engineering*, 1–10.
45. Richardson, M. D., et al. (2020). Planning for cyber security in schools. *Educational Planning, 27*(2), 23–39.
46. Sinha, A., et al. (2020). Critical infrastructure security. In *Quantum cryptography and the future of cyber security* (pp. 134–162).
47. Taileb, N., & Hamidi, H. (2022). Conceptual approach to cybersecurity. *Scientific Research*, University of Chlef.
48. Tyagi, R. (2020). Cybersecurity challenges in 2020.
49. Ullah, Z., et al. (2020). AI and ML in smart cities. *Computer Communications, 154*, 313–323.
50. Usman, A., et al. (2023). Internal auditors' characteristics in cybersecurity risk assessment.
51. Van Greuning, H., & Bratanovic, S. (2020). *Analyzing banking risk*. World Bank Publications.
52. Wang, V., et al. (2020). Internet banking cybersecurity. *International Journal of Law, Crime and Justice, 62*, 100415.
53. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage Learning.
54. Youssef Abdul Jabbar. (2013). *Effectiveness of internal control procedures* (Master's thesis). Yarmouk University.
55. Zibaei, S., et al. (2022). Password managers and secure passWords. In *SOUPS 2022* (pp. 581–597).