International Journal of Applied Economics, Finance and Accounting
ISSN 2577-767X
Vol. 22, No. 2, pp. 116-132
2025
DOI: 10.33094/ijaefa.v22i2.2305

The Impact of Cybersecurity Assurance on the Quality of Internal Audit at The Financial Technology Companies in Jordan: The Moderating Role of COBIT 2019

Hisham Mohammed Ahmad[1*]
Al-Shayeb[2]

[1,2]*Department of Accounting, Faculty of Graduate Studies, The World Islamic Sciences and Education University, Amman, Jordan.*
Email: hishamshayeb40@gmail.com

Keywords:
COBIT 2019
Cybersecurity assurances
FinTech companies
Internal audit quality
Jordan.

JEL Classification: *JEL Code: M42 – Auditing*

Received: *21 March 2025*
Revised: *16 June 2025*
Accepted: *19 June 2025*
Published: *20 June 2025*
(Corresponding Author)*

Abstract

Investigate the impact of cybersecurity assertions across its five dimensions (data security, system security, network security, operational security, and physical security) on the quality of internal auditing in FinTech companies operating and examined the role of the COBIT2019 framework as a moderating variable in this relationship. The research relied on a descriptive analytical approach. The study targeted employees of the internal audit, cybersecurity, and IT governance departments in FinTech companies. A total of 180 questionnaires were distributed, and 143 valid responses were obtained for analysis. Cybersecurity assurances have a positive impact on internal audit quality. System security is considered the most influential factor in internal audit quality. The COBIT2019 framework also strengthens this impact by aligning governance and audit processes. The COBIT 2019 framework provides a systematic mechanism for aligning cybersecurity requirements with internal audit standards, and contributes to enhancing integration between information security units and audit teams, leading to improved integration of risk management and decision-making. Fintech companies build a governance framework that ensures their effectiveness by adopting the COBIT 2019 standards as a foundation for digital governance and measuring the compliance of IT governance practices with the International Standards for Internal Auditing.

Funding: This study received no specific financial support.
Institutional Review Board Statement: The Ethical Committee of the World Islamic Sciences and Education University, Jordan has granted approval for this study on 21 November 2024.
Transparency: The authors declare that the manuscript is honest, truthful and transparent, that no important aspects of the study have been omitted and that all deviations from the planned study have been made clear. This study followed all rules of writing ethics.
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: Both authors contributed equally to the conception and design of the study. Both authors have read and agreed to the published version of the manuscript.

1. Introduction

The worldwide financial industry has changed dramatically due to the fast growth of financial technology (FinTech) applications, leading to new solutions like digital banking systems, blockchain technologies, and automated financial advisory platforms. This digital transformation has been accompanied by the emergence of unprecedented levels of cybersecurity threats, primarily manifested in financial data breaches, exploitation of security vulnerabilities in banking systems, and sophisticated phishing attacks (Kure, Islam, & Razzaque, 2018).

In the face of these challenges, cybersecurity assurances have emerged as a fundamental pillar in enhancing the operational and organizational resilience of financial institutions. Studies indicate that these assurances are not limited to protecting digital assets only but also extend to ensuring compliance with various regulatory frameworks such as the Basel III Accord (Evans, Maglaras, He, & Janicke, 2016). It also plays an effective role in enhancing the reliability of auditing operations, as it contributes to enhancing the accuracy of financial data, ensuring the integration of systems, and improving the effectiveness of internal controls (Al-Toni, 2023).

Leading financial institutions are implementing integrated governance frameworks in this regard; the COBIT 2019 framework is the most widely used because it combines strategic business dimensions with cyber risk management requirements through internal controls, risk assessment mechanisms, and key performance indicators (KPIs) (Romney & Steinbart, 2020).

However, further research is needed into how cybersecurity assurances impact internal audit quality and the role of COBIT2019 in this relationship within FinTech companies, which are characterized by complexity and rapid technological advancement.

1.1. Problem Statement and Research Gap

Prior studies have highlighted the importance of cybersecurity in managing financial risk. However, there is a lack of focused research that investigates the direct impact of cybersecurity assurance on internal audit quality in FinTech firms. Furthermore, existing literature does not adequately explore the moderating influence of COBIT2019 in this relationship.

1.2. Research Objectives

This study aims to address the identified research gap by:

1. Examining the impact of cybersecurity assurance and its five dimensions (data security, system security, network security, operational security, and physical security) on the quality of internal audit in FinTech companies.
2. Assessing the moderating role of the COBIT2019 framework in strengthening the relationship between cybersecurity assurance and internal audit quality.
3. Providing practical insights into how FinTech institutions can strengthen their cybersecurity governance through the strategic integrating of COBIT2019. This includes enhancing cybersecurity controls, improving the efficiency of internal audit, and ensuring compliance with dynamic regulatory requirements.

These objectives seek to advance the understanding of the complementary relationship between cybersecurity assurance and internal audit quality. The study presents a practical framework that supports FinTech companies in enhancing transparency, improve operational effectiveness, and maintain regulatory compliance in the context of rabid digital transformation.

Figure 1 illustrates the conceptual framework of the study, highlighting the relationship between cybersecurity assurance and internal audit quality, and underscoring the moderating role of the COBIT2019 framework in this relationship.

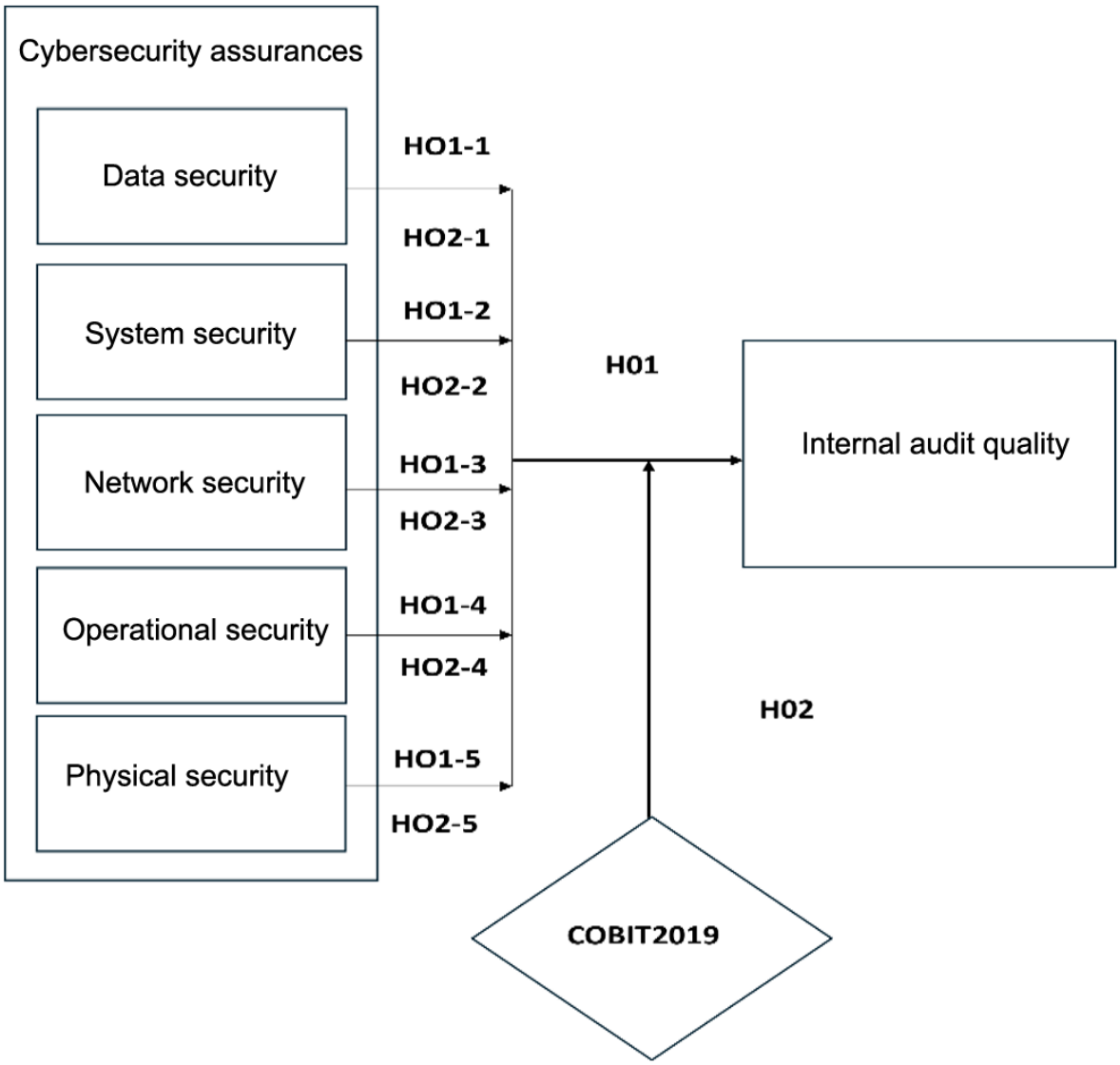

Figure 1. Research framework.

2. Literature Review

2.1. Cybersecurity Assurance

Cybersecurity refers to the combination of technical and organizational measures designed to protect digital infrastructure, including computer systems, communication networks, and data storage, from unauthorized access, cyberattacks, and operational disruptions. According to the Central Bank of Jordan (2024) effective cybersecurity ensures the confidentiality, integrity, and availability of information through strict security policies and proactive risk management. Its role has become increasingly vital in preserving data privacy, protecting digital communication, identifying vulnerabilities, and ensuring the safe exchange of information online (Kure et al., 2018).

Beyond its technical function, cybersecurity has broader implications across economic, legal, social, and political domains. Economically, it helps prevent financial losses by protecting the foundational digital infrastructure that modern economies depend on. Legally, it necessitates the development of regulatory frameworks that define accountability for cybercrimes and safeguard digital rights. Socially, cybersecurity contributes to building trust in the digital environment, while politically, it plays a role in defending national sovereignty against cyber threats (Fawzi, 2019; Youssef, 2022).

Cybersecurity assurance encompasses several overlapping dimensions that support digital resilience. Data security focuses on maintaining the accuracy and proper use of sensitive information (Hu, Wang, Chih, & Yang, 2018). System security involves defending IT systems and software against both internal and external threats (Beretas, 2024). Network security addresses the protection of digital communications from interception or disruption (Győrffy, Leitold, & Arrott, 2017). Operational security relates to controlling access to systems and managing exposure to internal vulnerabilities (Al-Toni, 2023). Physical security ensures that

the physical components of digital systems, such as servers and hardware, are protected from cyber-related risks (Pourmadadkar, Lezzi, & Corallo, 2024).

Managing cybersecurity risks requires a comprehensive approach that includes identifying threats, assessing potential impacts, responding to incidents, and fostering a culture of cybersecurity awareness across all organizational levels (American Institute of Certified Public Accountants (AICPA), 2017). In Jordan, the National Cybersecurity Center is responsible for developing national policies and strategies that aim to strengthen institutional readiness, build resilient digital infrastructure, and promote collaboration at both national and international levels. As outlined by the Ministry of Digital Economy and Entrepreneurship (2018) the national framework obligates institutions to develop capabilities that optimize the use of digital resources while minimizing risks.

2.2. Internal Audit Quality

Internal audit is a key organizational function that ensures accountability, transparency, and effective governance. The IIA The Institute of Internal Auditors (2024) defines it as an independent and objective activity that helps organizations evaluate and improve the effectiveness of their risk management, control, and governance processes. In practice, internal audit contributes to fraud detection, compliance enhancement, operational improvement, and strategic decision-making (Al-Naimat, 2022; Majidah & Falikhatun, 2024).

The role of internal audit extends beyond traditional oversight, it includes both assurance services, which verify the accuracy and effectiveness of controls, and consulting services, which provide management with recommendations on improving governance and mitigating risk (IIA The Institute of Internal Auditors, 2024). In FinTech environments, internal auditors are expected to navigate complex systems and emerging technologies with a clear focus on regulatory compliance and business continuity.

Quality of audits is usually judged by things like impartiality, professional know-how, independence, the amount of work done, and how clear the audit results are (Ndubuisi & Ezechukwu, 2017). Auditors' freedom and honesty are very important for making audit results more reliable and building trust with stakeholders. The amount of schooling and work experience inspectors have, as well as their educational level, directly affects how well they do their jobs. Clarity of audit procedures, the efficiency of planning systems, and the extent of senior management support also play a pivotal role in ensuring the effectiveness of audit operations. Adherence to international auditing standards (such as those issued by the IIA) and the optimal use of available resources are two critical elements for achieving excellence in audit outcomes, as they ensure consistency and reliability of practices (Addaraini & Erlina, 2020; Kotb, Elbardan, & Halabi, 2020). Thus, the interaction between these factors ultimately determines the effectiveness and quality of internal auditing and its ability to add real value to the organisation.

2.3. COBIT 2019 Framework

The COBIT (Control Objectives for Information and Related Technologies) framework dates back to the 1990s and has undergone a series of continuous developments to keep pace with technological changes and organizational requirements. The latest and most advanced version, COBIT2019 (2019), provides integrated tools for aligning IT with corporate strategy, increasing operational efficiency, and addressing governance challenges in rapidly changing digital environments (Haouam, 2020). COBIT2019 (2019) features a comprehensive structure that includes 37 high-level oversight objectives, distributed across five main areas: meeting stakeholder expectations, enhancing the scope of governance beyond IT, adopting a unified framework, applying a comprehensive governance methodology, and clearly distinguishing between governance and management (COBIT2019, 2019).

COBIT2019 (2019) introduced significant improvements compared to previous editions, increasing the number of governance principles from five to six to better reflect stakeholder expectations and support performance oversight processes. Figure 2 illustrates these developments by comparing key objectives across different COBIT editions, highlighting the added value the latest edition provides in enhancing the effectiveness of digital governance.

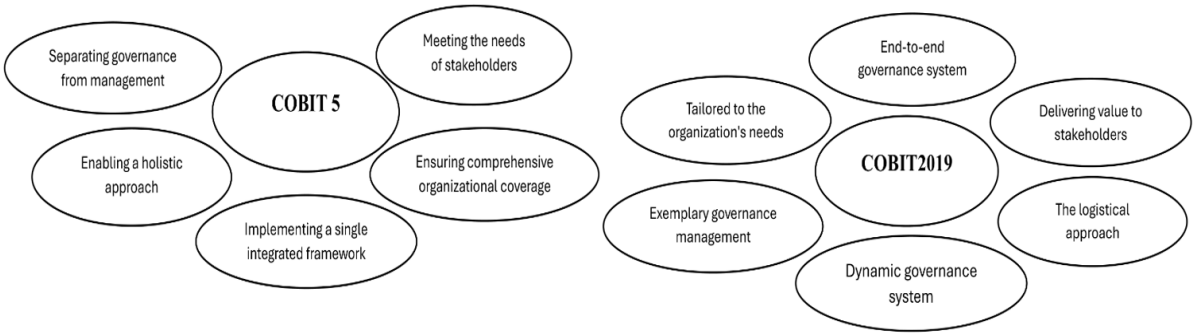

Figure 2. Key principles of COBIT5 and COBIT 2019.

COBIT2019 (2019) framework is built upon three core pillars: IT processes that cover planning, acquisition, delivery, and evaluation; information standards that ensure data relevance, accuracy, and confidentiality; and IT resources, including hardware, software, facilities, and human expertise. The integration of these elements provides a structured environment for consistent IT governance and operational oversight.

By adopting the COBIT2019 (2019) framework, organizations can strengthen internal controls, improve risk management, and ensure compliance with national and international regulations. The framework also promotes stronger alignment between IT operations and business strategy, enhances competitiveness, and increases the overall strategic value derived from technology resources. Its structured approach makes it particularly relevant for sectors such as fintech, where flexibility, accountability, and regulatory compliance are critical to operational success.

2.4. Theoretical Framework of Study Variables

This study is based on the premise that cybersecurity assurances are a fundamental pillar for enhancing the efficiency of regulatory processes in sensitive technological environments, such as financial technology companies. This perspective is based on two main principles: risk management theory and IT governance literature. The study presents an integrated model of cybersecurity assurances based on five interconnected pillars: data security, systems security, network security, operational security, and physical security. The strength of this model lies in the integration of these elements to achieve three strategic objectives: protecting digital assets, maintaining information accuracy, and preventing security breaches. This positively impacts the audit environment by strengthening oversight mechanisms, enabling auditors to perform their duties in complex digital systems, and ensuring regulatory compliance efficiently.

This aligns with the concept of internal audit quality in the context of the study, which is defined as the effectiveness, independence, and reliability of internal audit processes in detecting risks, preventing fraud, and ensuring compliance with regulations. Studies confirm that the strength of cybersecurity assurances directly impacts the ability of audit teams to accurately perform their tasks, especially in environments with high technical complexity.

The COBIT2019 (2019) is introduced into the model as a moderating variable, based on its role in providing structured governance mechanisms and aligning IT operations with strategic objectives. By integrating COBIT principles, organizations can enhance coordination between cybersecurity and audit functions, establish clearer accountability, and ensure more consistent application of controls. The framework assumes that COBIT2019 (2019) strengthens the relationship between cybersecurity assurance and internal audit quality by integrating governance at both the technical and procedural levels of control.

Accordingly, the study proposes a conceptual model in which cybersecurity assurance influences internal audit quality, and this relationship is moderated by the implementation of COBIT2019 (2019). This model guides the research hypotheses and empirical tests in the subsequent sections.

3. Research Methodology

3.1. Research Design and Approach

This study followed an applied research approach using both descriptive and quantitative methods. A deductive approach was used to explore the relationship between cybersecurity assurance and internal audit quality, as well as the moderating role of the COBIT2019 (2019) framework.

3.2. Data Collection Methods

The research was based on two types of sources to collect the necessary data, which were as follows:

1. Primary Data: A structured survey questionnaire was distributed electronically to professionals in FinTech companies, including internal auditors, compliance officers, and IT security specialists. The questionnaire was designed to measure perceptions of cybersecurity assurance, internal audit quality, and COBIT2019 (2019) implementation.

2. Secondary Data: The research incorporates data from academic journals, industry reports, regulatory guidelines, and cybersecurity governance frameworks such as COBIT2019 (2019) and ISO 27001 to provide additional insights into best practices in FinTech firms.

3.3. Study Population and Sample

The study targeted fintech companies in Jordan. A purposive sampling was used to select professionals in cybersecurity, internal audit, or IT governance. A total of 180 questionnaires were distributed, with a valid response rate of 143 (79.4%).

3.4. Measurement Instrument

The questionnaire was divided into three main sections:

- Independent variable: Cybersecurity assurance, measured across five dimensions (data, system, network, operational, and physical).

- Dependent variable: Internal audit quality, measured through the effectiveness of risk detection, compliance, and fraud prevention.
- Moderating variable: COBIT2019 (2019) assessed for its integration with cybersecurity within governance and audit functions.

A five-point Likert scale was employed to gauge respondents' perceptions. Table 1 summarizes the structure of the research instrument.

Table 1. Components of the research instrument.

Variable	Dimension	Paragraph limits	No. of paragraphs
Demographic data	Age	1-5	5
	Educational level	1-4	4
	Years of experience	1-5	5
	Academic specialization	1-6	6
	Job title	1-7	7
	Professional certificates	1-6	6
Independent variable	Data security	1-8	8
	System security	1-8	8
	Network security	1-8	8
	Operational security	1-8	8
	Physical security	1-8	8
Cybersecurity assurances			
Dependent variable	Internal audit quality	1-10	10
Moderating variable	COBIT 2019 framework	1-10	10

3.5. Data Analysis Techniques

The collected data were analysed using a combination of descriptive and inferential statistical methods to assess the relationships between the study variables. Descriptive statistics were first used to summarize participant characteristics and identify general patterns related to cybersecurity practices in fintech companies. To test the study hypotheses, regression analysis was used to examine the direct impact of cybersecurity assurance on internal audit quality. Furthermore, structural equation modelling (SEM) was used to evaluate the moderating effect of the COBIT2019 (2019) framework on the relationship between cybersecurity assurance and audit performance. All statistical analyses were conducted using SPSS, ensuring a robust and systematic approach to data interpretation and extracting valuable insights.

3.6. Reliability and Validity Measures

Cronbach's alpha coefficient was used to assess the internal consistency of the measurement scales. Factor analysis was conducted to ensure construct validity. A Pilot test was conducted prior to full-scale data collection to ensure clarity and reliability.

3.7. Ethical Considerations

This study was conducted in alignment with academic ethical standards to ensure the protection of participants' rights and the confidentiality of their data. All respondents were informed of the research objectives, procedures, and their voluntary participation. Informed consent was obtained prior to data collection, and all survey responses were anonymized to protect personal privacy. The research process followed institutional ethical principles and ensured transparency and responsibility throughout the study.

3.8. Limitations of the Study

Despite its systematic approach, the study acknowledges several limitations:

- Geographical scope: The study focused exclusively on FinTech companies in Jordan, which may limit the generalizability of the findings to other regions or sectors.
- Self-reported data: The use of survey-based responses introduces the potential for respondent bias and subjectivity.
- Dynamic cybersecurity landscape: The continuously evolving nature of cybersecurity threats may outpace static governance models, requiring regular updates beyond the study's timeframe.

This methodological framework supports a comprehensive assessment of the relationship between cybersecurity assurance and internal audit quality, while accounting the moderating role of COBIT2019 (2019). By incorporating COBIT2019 (2019) principles, the study adopts a structured and context-specific approach to analyzing cybersecurity governance in FinTech environments.

4. Results and Analysis

Understanding the nature of the relationship and impact between cybersecurity assertions, internal audit quality, and COBIT2019 requires first describing the reality of these variables in the study environment, represented by financial technology companies, using descriptive statistical methods, and then testing the direct relationship between cybersecurity assertions and internal audit quality. Finally, structural equation modelling (SEM) was used to test the moderating role of the COBIT2019 IT governance framework on this effect.

4.1. Descriptive Statistics

Table 2 shows the demographic distribution of the respondents, including variables such as age, educational level, work experience, job title, professional certification and field of specialization

Table 2. Summary of respondent demographics.

Variable	Category	Frequency	Percentage (%)
Age	Less than 25 years	21	14.7%
	25 - 34 years	43	30.1%
	35 - 44 years	61	42.7%
	45 - 54 years	14	9.8%
	55 years and above	4	2.7%
Educational level	Bachelor's degree	95	66.4%
	Higher diploma	0	0.0%
	Master's degree	43	30.1%
	PhD	5	3.5%
Work experience	Less than 5 years	28	19.6%
	5 - 9 years	12	8.4%
	10 - 14 years	35	24.5%
	15 - 19 years	44	30.8%
	20 years and above	24	16.8%
Job title	Internal auditor	33	23.1%
	Internal control department manager	31	21.7%
	IT department manager	11	7.7
	Information security / Cybersecurity department manager	27	18.9%
	Audit committee manager	14	9.8%
	Programmer	4	2.8%
	IT officer	23	16.1%
Professional certification	No certification	63	44.1%
	CPA	6	4.2%
	JCPA	8	5.6%
	CISA	34	23.8%
	Other (e.g., CIA, CMA)	32	22.8%
Field of specialization	Accounting	61	42.7%
	Business administration	8	5.6%
	Finance and banking	12	8.4%
	Computer information systems (CIS)	17	11.9%
	Accounting and managerial information systems	36	25.2%
	Programming	9	6.2%

The results show that 42.7% of the participants were between 35 and 44 years old, and more than 60% of them had a bachelor's degree. The results also show that the participants had high practical experience, as it was found that 30.8% had experience between 15 and 19 years, especially in the fields of internal auditing, information security, and cybersecurity. However, 44.1% of participants confirmed that they did not hold specialized professional certifications, and more than 40% of them were accounting specialists. These results reflect a participant base with extensive knowledge and experience.

4.2. Hypothesis Testing and Regression Analysis

This section summarizes the results of hypothesis testing to assess the impact of cybersecurity assurance and the moderating role of the COBIT2019 (2019) framework on internal audit quality.

H_{01}: There is no statistically significant effect (at $P \leq 0.05$) of cybersecurity assurance—across its dimensions of data, system, network, operational, and physical security—on the quality of internal auditing in FinTech companies in Jordan.

Table 3 presents the findings from the multiple linear regression analysis, highlighting the direct impact of cybersecurity assurances on the quality of internal auditing within financial technology companies in Jordan.

Table 3. Regression results for H01 – Effect of cybersecurity assurance on internal audit quality.

Dependent variable	Model summary				Analysis of variance (ANOVA)		
	(R) Correlation coefficient	(R^2) Coefficient of determination	(Adj.R^2) Adjusted coefficient of determination	Standard error of the model	(DF)	Calculated F-value	(Sig F*) Significance level
Internal audit quality	0.720	0.519	0.501	0.328	5	29.559	0.000

Note: *The effect is statistically significant at the significance level ($P \leq 0.05$).

The regression model revealed a correlation coefficient R of 0.720 and an R^2 value of 51.9%, indicating that more than half of the variance in internal audit quality can be explained by cybersecurity assurance. The F value was 29.559 and the p value was 0.000, confirming statistical significance. Therefore, the null hypothesis (H01) is rejected, and the results support that cybersecurity assurance significantly improves internal audit quality in FinTech companies.

Table 4 presents the regression coefficients for the various dimensions of cybersecurity assurances and their influence on the quality of internal auditing within financial technology companies in Jordan.

Table 4. Regression coefficients for H01.

Regression coefficients					
Variable	**(B) Coefficients**	**Standard error**	**Beta value**	**Calculated F-value**	**(Sig T*) Significance level**
Regression constant	1.235	0.254		4.866	0.000
Data security	0.064	0.136	0.066	0.468	0.640
System security	0.412	0134	0.427	3.063	0.003
Network security	0.172	0.127	0.181	1.354	0.178
Operational security	0.111	0.160	0.117	0.697	0.487
Physical security	-0.041	0.097	-0.043	-0.426	0.671

Note: *The effect is statistically significant at the significance level ($P \leq 0.05$).

The coefficients in Table 5 show that among the five dimensions of cybersecurity assurance, only system security has a statistically significant impact on internal audit quality ($p = 0.003$). It also has the highest standardized beta ($\beta = 0.427$), indicating a strong predictive power. The remaining dimensions—data, network, operational, and physical security—do not show statistically significant effects individually, although their collective contribution was confirmed in the overall model. This suggests that while cybersecurity assurance as a whole is impactful, the strength of the effect varies by dimension, with system security being the most influential.

H_{02}: There is no statistically significant moderating effect (at $P \leq 0.05$) of the COBIT2019 framework on the relationship between cybersecurity assurance and internal audit quality in FinTech companies in Jordan.

Table 5. Statistical analysis of hypothesis 2.

Dependent variable	Independent variables	Model 1			Model 2		
		(B) Coefficients	Calculated T value	(Sig T*) Significance level	(B) Coefficients	Calculated T value	(Sig T*) Significance level
Internal audit quality	Data security	0.064	0.468	0.640	0.027	0.226	0.821
	System security	0.412	3.063	0.003	0.268	2.244	0.026
	Network security	0.172	1.354	0.178	0.188	1.687	0.094
	Operational security	0.111	0.697	0.487	-0.016	-0.115	0.909
	Physical security	-0.041	-0.426	0.671	-0.098	-1.151	0.252
	COBIT 2019 framework				0.462	6.608	0.000
	R^2 (Coefficient of determination)	0.519			0.636		
	ΔR^2	0.519			0.117		
	ΔF	29.559			39.583		
	Sig ΔF	0.000			0.000		

Note: * The effect is statistically significant at the significance level ($P \leq 0.05$).

The results of the regression analysis examining the moderating effect of COBIT2019 revealed a coefficient R^2 of 63.6%, indicating that the inclusion of COBIT2019 in the model significantly increases the explanatory power, compared to the baseline model in H01 (which had an R^2 of 51.9%). The p-value for the interaction term was 0.000, confirming statistical significance at the 0.05 level.

These findings lead to the rejection of the null hypothesis (H02), confirming that the COBIT2019 significantly moderates the relationship between cybersecurity assurance and internal audit quality. The presence of this framework enhances the positive impact of cybersecurity practices on internal audit outcomes in FinTech companies. Specifically, COBIT2019 supports the alignment of IT governance with audit objectives, increases accountability, and ensures the systematic application of cybersecurity controls within the audit function.

4.3. Sub-Hypothesis Analysis

Each dimension of cybersecurity assurance was individually tested to determine its specific influence on internal audit quality. Tables 6 through 10 present the statistical analysis for each sub-hypothesis, corresponding respectively to.

Results of the Analysis of the First Sub-Hypothesis from the Second Main Hypothesis

Table 6. Statistical analysis of sub-hypothesis 1.

Results of the analysis of the first sub-hypothesis from the second main hypothesis							
Dependent variable	**Independent variables**	**Model 1**			**Model 2**		
		(B) Coefficients	**Calculated T value**	**(Sig T*) Significance level**	**(B) Coefficients**	**Calculated T value**	**(Sig T*) Significance level**
Internal audit quality	Data security	0.631	10.252	0.000	0.287	4.241	0.000
	COBIT 2019 framework				0	7.862	0.000
	R^2 (Coefficient of determination)	0.427			0.603		
	ΔR^2	0.427			0.175		
	ΔF	105.108			106.129		
	Sig ΔF	0.000			0.000		

Note: * The effect is statistically significant at the significance level ($P \leq 0.05$).

Results of the Analysis of the Second Sub-Hypothesis from the Second Main Hypothesis

Table 7. Statistical analysis of sub-hypothesis 2.

Results of the analysis of the second sub-hypothesis from the second main hypothesis							
Dependent variable	**Independent variables**	**Model 1**			**Model 2**		
		(B) Coefficients	**Calculated T value**	**(Sig T*) Significance level**	**(B) Coefficients**	**Calculated T value**	**(Sig T*) Significance level**
Internal audit quality	System security	0.679	11.800	0.000	0.357	5.225	0.000
	COBIT 2019 framework				0.467	6.905	0.000
	R^2 (Coefficient of determination)	0.497			0.625		
	ΔR^2	0.497			0.128		
	ΔF	139.248			116.510		
	Sig ΔF	0.000			0.000		

Note: * The effect is statistically significant at the significance level ($P \leq 0.05$).

Results of the Analysis of the Third Sub-Hypothesis from the Second Main Hypothesis

Table 8. Statistical analysis of sub-hypothesis 3.

Results of the analysis of the third sub-hypothesis from the second main hypothesis							
Dependent variable	**Independent variables**	**Model 1**			**Model 2**		
		(B) Coefficients	**Calculated T value**	**(Sig T*) Significance level**	**(B) Coefficients**	**Calculated T value**	**(Sig T*) Significance level**
Internal audit quality	Network security	0.633	10.550	0.000	0.312	4.891	0.000
	COBIT 2019 framework				0.513	8.016	0.000
	R^2 (Coefficient of determination)	0.441			0.617		
	Δ R^2	0.441			0.176		
	Δ F	111.309			112.744		
	Sig Δ F	0.000			0.000		

Note: * The effect is statistically significant at the significance level (P ≤ 0.05).

Results of the Analysis of the Fourth Sub-Hypothesis from the Second Main Hypothesis

Table 9. Statistical analysis of sub-hypothesis 4.

Results of the analysis of the fourth sub-hypothesis from the second main hypothesis							
Dependent variable	**Independent variables**	**Model 1**			**Model 2**		
		(B) Coefficients	**Calculated T value**	**(Sig T*) Significance level**	**(B) Coefficients**	**Calculated T value**	**(Sig T*) Significance level**
Internal audit quality	Operational security	0.647	10.907	0.000	0.304	4.392	0.000
	COBIT 2019 framework				0.502	7.255	0.000
	R^2 (Coefficient of determination)	0.458			0.606		
	Δ R^2	0.458			0.148		
	Δ F	118.954			107.578		
	Sig Δ F	0.000			0.000		

Note: * The effect is statistically significant at the significance level (P ≤ 0.05).

Results of the Analysis of the Fifth Sub-Hypothesis from the Second Main Hypothesis

Table 10. Statistical analysis of sub-hypothesis 5.

Results of the analysis of the fifth sub-hypothesis from the second main hypothesis							
Dependent variable	**Independent variables**	**Model 1**			**Model 2**		
		(B) Coefficients	**Calculated T value**	**(Sig T*) Significance level**	**(B) Coefficients**	**Calculated T value**	**(Sig T*) Significance level**
Internal audit quality	Physical security	0.543	8.096	0.000	0.175	2.620	0.010
	COBIT 2019 framework				0.605	9.140	0.000
	R^2 (Coefficient of determination)	0.317			0.572		
	Δ R^2	0.317			0.255		
	Δ F	65.542			93.725		
	Sig Δ F	0.000			0.000		

Note: * The effect is statistically significant at the significance level ($P \leq 0.05$).

The regression results from Tables 6 to 10 indicate that each dimension of cybersecurity assurance — data, systems, network, and process security, and physical security—has a statistically significant positive impact on internal audit quality. This finding highlight that each individual component plays an important role in strengthening audit performance. When combined, these dimensions contribute to a more reliable, secure, and efficient internal audit environment in FinTech companies, enhancing risk management and compliance.

4.4. Summary of Hypothesis Testing Results

Table 11 summarizes the results of all tested hypotheses, indicating whether each null hypothesis was accepted or rejected based on the statistical results.

Table 11. Summary of hypothesis testing results.

Hypothesis no	Hypothesis text	Hypothesis result
H01	There is no statistically significant effect at the significance level (P≤0.05) of cybersecurity assurances across its dimensions (data security, system security, network security, operational security, physical security) on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of cybersecurity assurances across its dimensions (Data security, system security, network security, operational security, physical security) on the quality of internal auditing in FinTech companies in Jordan.
H01-1	There is no statistically significant effect at the significance level (P≤0.05) of data security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of data security on the quality of internal auditing in FinTech companies in Jordan.
H01-2	There is no statistically significant effect at the significance level (P≤0.05) of system security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of system security on the quality of internal auditing in FinTech companies in Jordan.
H01-3	There is no statistically significant effect at the significance level (P≤0.05) of network security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of network security on the quality of internal auditing in FinTech companies in Jordan.
H01-4	There is no statistically significant effect at the significance level (P≤0.05) of operational security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of operational security on the quality of internal auditing in FinTech companies in Jordan.
H01-5	There is no statistically significant effect at the significance level (P≤0.05) of physical security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of physical security on the quality of internal auditing in FinTech companies in Jordan.
H02	There is no statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of cybersecurity assurances across its dimensions (data security, system security, network security, operational security, physical security) on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of cybersecurity assurances across its dimensions (Data security, system security, network security, operational security, physical security) on the quality of internal auditing in FinTech companies in Jordan.
H02-1	There is no statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of data security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of data security on the quality of internal auditing in FinTech companies in Jordan.
H02-2	There is no statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of system security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of system security on the quality of internal auditing in FinTech companies in Jordan.

H02-3	There is no statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of network security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of network security on the quality of internal auditing in FinTech companies in Jordan.
H02-4	There is no statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of operational security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of operational security on the quality of internal auditing in FinTech companies in Jordan.
H02-5	There is no statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of physical security on the quality of internal auditing in FinTech companies in Jordan.	There is a statistically significant effect at the significance level (P≤0.05) of the COBIT2019 framework in improving the effect of physical security on the quality of internal auditing in FinTech companies in Jordan.

5. Discussion

This study aims to investigate the impact of cybersecurity assertions and their five dimensions (data security, system security, network security, operational security, and physical security) on internal audit quality in FinTech companies and to evaluate the moderating role of the COBIT2019 (2019) framework in enhancing the relationship between cybersecurity assertions and internal audit quality. The results revealed that cybersecurity assurances have a statistically significant positive impact on internal audit quality. Fintech companies' adoption of comprehensive security measures contributes to improved internal audit performance, reduced exposure to risks, and ensured regulatory compliance.

Although all aspects of cybersecurity assurance are important in enhancing the quality of internal auditing, system security is considered the most influential. Secure systems constitute a fundamental foundation for auditing operations by providing immediate protection for data processing mechanisms and operational processes. Secure systems are a fundamental pillar of auditing operations, providing immediate protection for data processing mechanisms and operational processes. Therefore, any breach or failure in them disrupts the ability to collect evidence, analyze data, and issue accurate reports. Evans et al. (2016) study confirmed that security systems contribute to improving the efficiency of auditing and risk detection.

The study also revealed the positive role of the COBIT2019 (2019) framework in strengthening the relationship between cybersecurity assurances and internal audit quality. Adopting COBIT2019 enabled Fin Tech companies to align cybersecurity governance with audit standards, improve coordination between IT and audit teams, and enhance audit capabilities through structured governance protocols. In this context, Jadhav (2023) explained that integrating security governance into audit procedures contributes to reducing cyber incidents, and Wu, Huang, Chiu, and Yen (2024) and Sanchez-Garcia, Rea-Guaman, Gilabert, and Calvo-Manzano (2024) pointed to the ability of COBIT2019 to raise audit efficiency and security resilience.

The study's findings confirm that cybersecurity assurances are a strategic necessity for raising and enhancing the quality of internal auditing, especially in high-risk sectors such as Fin Tech. This is achieved by ensuring the integrity and reliability of audit systems, maintaining operational continuity, and reducing fraud and information breaches. COBIT2019 also stands out as a vital tool for integrating security controls and auditing standards, making it an indispensable framework for companies seeking excellence in digital governance.

6. Conclusion and Recommendations

6.1. Conclusion

This study emphasizes the pivotal role of cybersecurity assurances on the quality of internal audits at Fin Tech companies in Jordan. It clearly demonstrates that adopting integrated cybersecurity systems and measures directly contributes to improving the quality of audits by enhancing the reliability and accuracy of financial data, ensuring the integrity of operational processes, and raising the level of regulatory compliance.

The results indicate that cybersecurity dimensions affect the quality of internal auditing differently, with systems security being the most important because it directly protects the auditing process, ensures the accuracy of the information being audited, and minimizes breaches that could disrupt auditing activities.

The COBIT2019 (2019) framework is an effective tool for maximizing the benefits of cybersecurity measures, providing a systematic mechanism for aligning cybersecurity requirements with internal audit standards. This framework not only improves security controls but also enhances integration between information security units and audit teams, leading to better integrated risk management and decision-making.

6.2. Recommendations

This study results in a set of important recommendations that contribute to strengthening cybersecurity measures, building operational resilience against cyber threats, improving the quality and efficiency of internal audit operations, and enhancing IT governance (COBIT2019, 2019) in Fin Tech companies. The most important of these is the need to achieve integration between cybersecurity systems and internal audit procedures, as modern internal audit standards in financial technology institutions require the adoption of an integrated cybersecurity model. This includes incorporating cyber risk assessments into annual audit plans, employing artificial intelligence technologies to continuously monitor suspicious activities, developing early warning systems to predict potential security threats, and establishing joint units between cybersecurity and audit departments.

The study recommends adopting a regulatory and governance framework that ensures organizational effectiveness by adopting the COBIT 2019 standards as a basis for digital governance, designing specialized training programs for auditors that focus on understanding the cybersecurity infrastructure and applying key performance indicators for digital auditing, and establishing a continuous evaluation system to measure the extent to which IT governance practices comply with international standards for internal auditing.

The study also recommends that Fin Tech companies adopt advanced cyber risk management technologies, develop smart monitoring systems based on network behavior analysis and deep learning to detect fraud and breaches, and prepare cyber incident response plans that include a clear classification of threat levels and containment measures within a specific timeframe.

This study represents a qualitative addition to academic knowledge and professional practice, providing a practical framework for measuring and assessing the impact of cybersecurity assurances on internal audit quality in the Fin Tech environment. It also highlights the factors that contribute to enhancing and supporting this impact, opening new avenues for research and development in this vital field.

In this context, the study recommends that researchers broaden their research scope to encompass various sectors, including banks, insurance companies, and government institutions. This expansion aims to provide insights into cybersecurity assertions across different regulatory and operational environments, and examining the impact of advanced digital technologies, including blockchain, artificial intelligence, and cloud computing, on cybersecurity assurances and the effectiveness of internal audits. This study may provide compelling evidence of how these technologies can enhance the quality of internal audits, bolster cybersecurity measures, and enable organizations to adapt to rapidly evolving digital threats.

References

Addaraini, F., & Erlina, H. (2020). Analysis of the effect of independence, professionalism, and competence on the quality of internal audit results with auditor ethics as moderating variable. *Journal of Public Budgeting, Accounting and Finance, 3*(1), 62-73.

Al-Naimat, H. (2022). The impact of internal audit on the quality of accounting information at the New Ayil Municipality. *Ramah Journal of Research and Studies, 74*, 25–74.

Al-Toni, S. M. (2023). The impact of customers' awareness of cyber piracy as a tool for achieving cybersecurity: A field study on government banks in Port Said governorate. *The Scientific Journal of Commerce and Finance, 43*(4), 609–653.

American Institute of Certified Public Accountants (AICPA). (2017). *Description criteria for management's description of the entity's cyber security risk management program.* New York: AICPA Assurance Services Executive Committee.

Beretas, C. (2024). Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology, 1*(1), 1–10.

Central Bank of Jordan. (2024). *Homepage, legislation list - instructions – cyber risk adaptation instructions No. (26/1/1/1984).* Cbj.Gov.Jo.

COBIT2019. (2019). *A business framework for the governance and management of enterprise IT.* Rolling Meadows, IL: ISACA.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679. https://doi.org/10.1002/sec.1657

Fawzi, I. (2019). Cybersecurity: Social and legal dimensions – A sociological analysis. *The National Social Journal, 56*(2), 99–139.

Győrffy, K., Leitold, F., & Arrott, A. (2017). Individual awareness of cyber-security vulnerability-Citizen and public servant. *Central and Eastern European eDem and eGov Days, 325*, 411-422. Https://Doi.Org/10.24989/Ocg.V325.34

Haouam, D. (2020). IT governance impact on financial reporting quality using COBIT framework. *Global Journal of Computer Sciences: Theory and Research, 10*(1), 1–10.

Hu, T., Wang, K., Chih, W., & Yang, X. (2018). Trade off cybersecurity concerns for co-created value. *Journal of Computer Information Systems, 60*(5), 468–483. https://doi.org/10.1080/08874417.2018.1538708

IIA The Institute of Internal Auditors. (2024). *Standards and guidance.* Retrieved from Https://Www.Theiia.Org/En/Content/Guidance/Recommended/Supplemental/Gtags/Gtag-Assessing-Cybersecurity-Risk/. [Accessed March 14, 2024]

Jadhav, K. D. (2023). The role of cybersecurity audits in managing company systems and applications. In (pp. 1-7). NJ, USA: Organization: Tech Mahindra Americas Bedminster.

Kotb, A., Elbardan, H., & Halabi, H. (2020). Mapping of internal audit research: A post-Enron structured literature review. *Accounting, Auditing & Accountability Journal, 33*(8), 1969-1996.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*(6), 898. Https://Doi.Org/10.3390/App8060898

Majidah, N., & Falikhatun, F. (2024). The role of internal audit on the quality of financial reports. *JPPI (Jurnal Penelitian Pendidikan Indonesia), 10*(4), 616-627.

Ministry of Digital Economy and Entrepreneurship. (2018). *National cybersecurity strategy 2018–2023.* Retrieved from https://modee.gov.jo

Ndubuisi, A., & Ezechukwu, B. (2017). Determinants of audit quality: Evidence from deposit money banks listed on Nigeria stock exchange. *International Journal of Academic Research in Accounting, Finance and Management Sciences, 7*(2), 117–130.

Pourmadadkar, M., Lezzi, M., & Corallo, A. (2024). Cyber security for cyber-physical systems in critical infrastructures: Bibliometrics analysis and future directions. *IEEE Transactions on Engineering Management, 71*, 15405-15421.

Romney, M. B. S., & Steinbart, P. J. (2020). *Accounting information systems* (15th ed.). Harlow, England: Pearson Education Limited.

Sanchez-Garcia, I. D., Rea-Guaman, A. M., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2024). Cybersecurity risk audit: A systematic literature review. *New Perspectives in Software Engineering*, 275-301. https://doi.org/10.1007/978-3-031-50590-4_18

Wu, T.-H., Huang, S. Y., Chiu, A.-A., & Yen, D. C. (2024). IT governance and IT controls: Analysis from an internal auditing perspective. *International Journal of Accounting Information Systems, 52*, 100663.

Youssef, A. A. W. (2022). The reality of cybersecurity risk management disclosure and its impact on investment and credit granting decisions in the stock market: An applied study. *The Scientific Journal of Commercial and Environmental Studies, 13*(2), 28–109.