MSA-Management science journal
ISSN 2974-3036
Volume: 4, Issue:3, Year: 2025 pp.1-27

The Impact of Internal Audit Function Characteristics on Internal Control Quality: The Moderating Role of Cyber Risk

Mohamed Abdelraouf[1]
Faculty of Administrative Sciences, King Salman International University, Sharm El Shiekh, South Sinai, Egypt
Abeer Mohamed Ryad Fahmy
Faculty of Commerce, Suez Canal University, Ismailia, Ismailia, Egypt
Farid Moharram[2]
Faculty of Commerce, Ain Shams University, Cairo, Cairo, Egypt

Abstract: This study examines how Internal Audit Function (IAF) characteristics impact Internal Control Quality (ICQ) when moderated by cyber risk in Egyptian banks. Analysing (e.g., "14 banks over 10 years"), the research evaluates four IAF characteristics: organisational governance, expertise, risk management, and investment. Results show all IAF characteristics positively affect ICQ, with organisational governance being significant at 90% confidence and the other three variables at 95% confidence. The model explains 71.1% of ICQ variance ($R^2 = 0.711$, adjusted $R^2 = 0.703$). Importantly, cyber risk weakens the relationship between IAF characteristics and ICQ, with organisational governance at 90% confidence and the other characteristics at 95% confidence. This study contributes to existing literature by empirically demonstrating how cyber risk influences IAF effectiveness in maintaining internal control quality within banking institutions.

Keywords: Internal Audit Function, Internal Control Quality, Cyber Risk, Banking Sector, Organizational Governance

M42, **G32**, **G34**, **D81**, **L86**

[1] ORCID iD 0000-0003-4256-0375
[2] ORCID iD 0000-0002-9036-1066

Introduction

Internal control systems are vital for organizational effectiveness, efficiency, and regulatory compliance (Alawaqleh, 2021). Organizations in complex environments rely heavily on high-quality internal control systems to maintain operational trust and stakeholder confidence (Dumoga, 2022). The Internal Audit Function (IAF) evaluates control systems to enhance their strength while addressing emerging risks that threaten organizational objectives (Achu, 2023).

Egypt's banking sector represents a particularly compelling research context for several reasons. As a vital foundation of the Egyptian economy, the banking sector provides substantial support to both national GDP and financial system stability (Abdelaziz and Francis, 2022). Egyptian banks are undergoing rapid digital transformation, which has significantly increased their exposure to cyberattacks (Abdelraouf et al., 2024). This digital transition creates a unique research opportunity because it combines competitive advantage drivers with new vulnerabilities that threaten internal control systems (Kraus et al., 2024; Sebastian et al., 2020). Furthermore, the Central Bank of Egypt has prioritized internal control mechanisms and cybersecurity systems as part of its economic reforms and financial sector modernization programs (Almansoori, 2024), creating a dynamic regulatory environment worthy of investigation.

This study addresses a critical gap in the literature: while previous research has examined relationships between IAF characteristics and internal control quality (e.g., Oussii and Taktak, 2018), there is limited understanding of how cyber risks affect this relationship, particularly in emerging economies like Egypt with rapidly evolving banking sectors. This research investigates the question:

How could cyber risks moderate the relationship between Internal Audit Function characteristics and Internal Control Quality in Egyptian banks?

Our findings reveal that all IAF characteristics (organizational governance, expertise, risk management, and investment) positively impact Internal Control Quality, with organizational governance significant at 90% confidence and the other three variables significant at 95% confidence. The model demonstrates strong explanatory power, accounting for 71.1% of ICQ variance. Most importantly, we find that cyber risk significantly weakens these relationships, indicating that digital vulnerabilities pose substantial challenges to maintaining internal control quality in banking institutions.

The study analyzes four fundamental elements of IAF: organizational governance, expertise, risk management, and investment. Our primary aim is to investigate the impact of these IAF characteristics on Internal Control Quality while considering the moderating effect of cyber risks—an

increasingly common threat in the banking sector that necessitates stronger internal controls to protect stakeholder interests and organizational assets.

These findings offer critical implications for banking sector regulators and management teams, as well as internal audit practitioners. They demonstrate that IAF requires more robust cyber risk management approaches and well-developed control systems capable of withstanding emerging digital threats. Section 2 of this paper reviews existing literature and develops hypotheses. Section 3 describes the research methodology. Section 4 presents results and analysis. Section 5 concludes with recommendations and directions for future research.

2. Literature review

2.1 IAF

As a vital organizational section the IAF gives unbiased assurance and consulting services dedicated to boosting efficiency and value within organizational operations (Geqeza, 2023). The Institute of Auditors includes multiple critical characteristics which involve governance systems and expert personnel and risk controls and technological and audit resources investments. Modern IAF developments prioritize its strategic value above traditional compliance-based work. Organizations use advanced analytical tools and risk-based methodologies and continuous monitoring systems to offer complete organizational process oversight within modern IAF operations (Mökander, 2023).

The changing role of the IAF now plays a vital part in coping with new business demands primarily in the financial industry (Walker and McGrath, 2023). The function now functions as a strategic decision-making partner that provides insights about operational efficiency as well as risk management and governance effectiveness. The evolution of IAF operations brought data analytics and artificial intelligence and machine learning capabilities into audit activities for implementing predictive and proactive audit approaches (Pinto, 2024). Organizations must utilize the function's adaptability trait to maintain independence and objectivity because this enables businesses to adapt to changing environments and achieve their strategic control environment improvements (Baloch et al. 2022).

2.2 ICQ

Organizations must test the reliability and effectiveness of their internal control system which helps them achieve their operational performance as well as provide correct reports and maintain compliance standards (Alawaqleh, 2021). Organizations with high-quality internal controls feature systems that both stop and discover material errors and maintain operational excellence and efficiency (Silva et al. 2022). ICQ assessment requires a systematic examination of control environment and risk assessment procedures with control activities along with information and communication systems and the monitoring activities. Organizations must maintain top quality controls because they protect both stakeholder trust and legal requirements and safeguard their business assets (Alazzabi et al. 2021).

Internal control systems have expanded their importance dramatically throughout the last few years because of developing business operations complexity alongside growing regulatory requirements (Harashe and Provasi, 2023). Modern organizations need to manage both operational efficiency along with effective control requirements through integrated dynamic strategies for their internal control systems (Chan et al. 2021). Modern ICQ frameworks make use of technological solutions which offer real-time monitoring together with automated control testing alongside predictive risk identification features (Demertzis et al. 2021). The evolution has produced better measurement tools for control effectiveness through key performance indicators (KPIs) and control performance indicators (CPIs) which offer numerical analysis methods for control quality assessment (Moradi et al. 2022). Organizations now use risk-based techniques for ICQ through which they select controls with higher risks to business objects and stakeholder interests (Abouelghit and Gan, 2024; Mohamed, 2024).

2.3 Cyber risk

Organizational loss and damage potentials happen through the utilization of information and communication technologies found within the boundaries of the organization (Bhowmik et al. 2021). Organizations find these threats collectively in one risk group as data breaches and system failures alongside cybercrime and disruptions which threaten organizational and stakeholder goals (George et al. 2024). Hacking and cyber fraud threats have become more complex which makes it increasingly difficult for organizations to handle them (Kumar, 2023). Businesses from the banking sector encounter increasing challenges to protect sensitive information while

sustaining operational systems alongside maintaining customer trust during their transition to digital systems and open architecture requirements (Saeed et al. 2023).

The financial consequences of cyber risks reach further than instant money loss because they result in reputational harm and regulatory fines together with diminished industry position (Malliouris, 2021). Businesses need to dedicate major funds to cybersecurity protection by deploying sophisticated threat identification programs and running employee education initiatives and developing organized incident response plans (Shaqiri, 2023). Modern financial institutions function within transnational banking networks that enable cyber risks to spread exponentially across multiple institutions at once. The critical nature of systemic risk has pushed regulatory authorities to create tougher cybersecurity rules with reporting requirements that push organizations toward implementing advanced cyber risk management frameworks (Popelo et al. 2021).

2.4 IAF and ICQ

IAF acts as a vital mechanism to create and enhance internal control quality by maintaining an interconnected relationship with the systems (Hussein, 2024). The combination of strong operational characteristics within IAF including proper governance foundations and expert personnel alongside extensive risk controls with sufficient funding enables more effective internal controls (Mthimunye, 2023). Organizations with robust Internal Audit Function characteristics usually achieve elevated Internal Control Quality through their stronger abilities in identifying risks and performing control tests and addressing control weaknesses promptly. Internal structures that support appropriate financial stability and regulatory compliance require this relationship to be effective (Madawaki et al. 2022).

2.5 Cyber risk and IAF

Organizations face an escalating challenge regarding how cyber risks connect with their Internal Audit Function operations in the context of organizational governance (Azizi et al. 2024). Organizational digital transformation calls for IAF to transform its approaches and systems to handle cyber security threats yet keep delivering successful results in traditional checking operations (Alharam et al. 2022; Christ et al. 2021). New capabilities including skills and tools and unique audit methods must become part of the audit function's operations. The gravity of cyber risks confronts the performance of conventional IAF procedures that may negatively affect control results and IAF characteristics. The interaction between cyber risks

and traditional IAF requires audit practices to evolve by developing advanced technical competencies along with specialized cybersecurity risk assessment tools combined with increasing technology investment in audit procedures for continuous organizational oversight (Babiker, 2025).

Therefore, the suggested hypothesis as follows:

H1: Internal audit function has a significant impact on ICQ

H1a: Organization governance has a significant impact on ICQ

H1b: Expertise has a significant impact on ICQ

H1c: Risk management has a significant impact on ICQ

H1d: Investment has a significant impact on ICQ

H2: Cyber risk moderates the relationship between Internal audit function and ICQ

H2a: Cyber risk moderates the relationship between organization governance and ICQ

H2b: Cyber risk moderates the relationship between expertise and ICQ

H2c: Cyber risk moderates the relationship between risk management and ICQ

H2d: Cyber risk moderates the relationship between investment and ICQ

The suggest research model as follows:

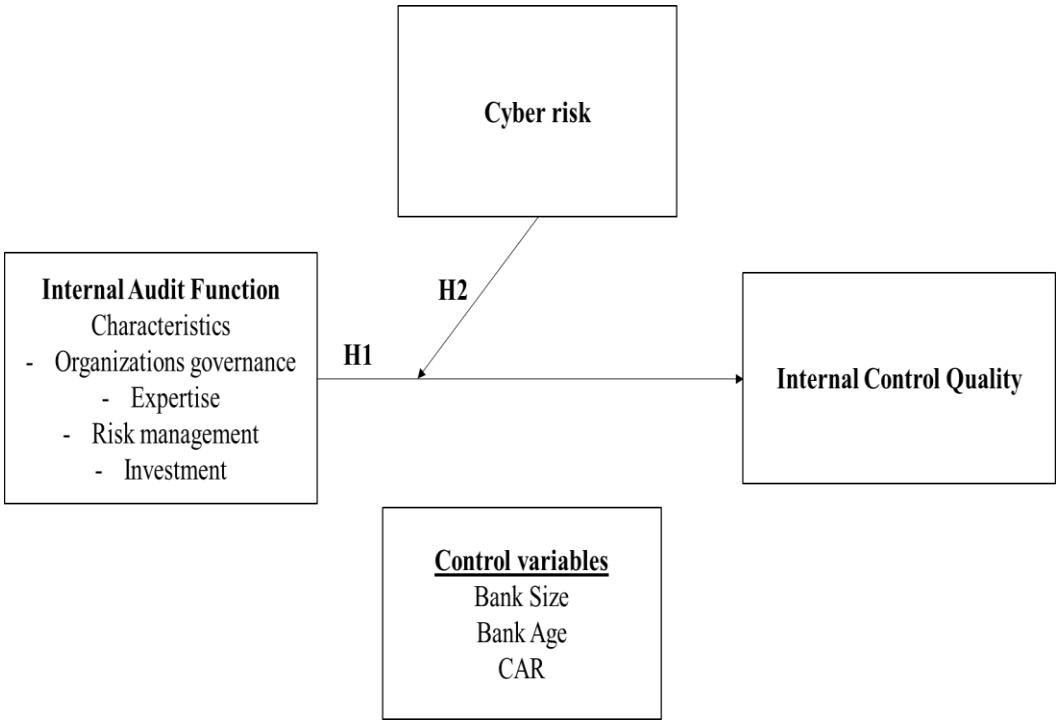

Figure 1. Conceptual framework

Source: Developed by the author

The conceptual model shows how IAF characteristics affect ICQ and Cyber risk functions as the moderation element between them. The model presents two principal hypotheses (H1 and H2) together with bank-specific variables for control purposes. Organizational governance and expertise and risk management and investment of the IAF have a direct impact on ICQ as per the initial hypothesis (H1). Internal control quality and Information audit function characteristics share a direct relationship explained by multiple theoretical lenses.

The relationship between internal audit functions and internal control quality receives its theoretical base from Agency Theory (Khalid and Sarea, 2021). IAF act as monitoring entities to decrease management-stakeholder information mismatch and agency cost problems. Stronger IAF characteristics enhance internal control quality because they link executive agent interests to those of shareholders. The resource-based theory demonstrates how specific qualities of internal audit functions affect internal control quality. The theory indicates that competitive advantages result from distinguishing organizational assets and operational capabilities which include audit expertise in addition to investment in audit functions. Internal

audit function characteristics serve as fundamental organizational resources which boost the quality of control systems (Liu et al. 2025).

The effectiveness of organizations depends on their capacity to adapt their operations to external dangers as per Contingency Theory (Shenkar and Ellis, 2022). The theory provides a framework to explain why cyber risks might reduce the connection between IAF characteristics and control quality because organizations must regularly modify their control systems to respond to changing cyber dangers. Risk Management Theory provides another theoretical basis for understanding the moderating role of cyber risk (Saeidi et al. 2021). Companies need to distribute resources according to different types of risks while new important cyber threats may affect the efficiency of existing internal control systems.

The model demonstrates how Bank Size and Bank Age and Capital Adequacy Ratio - CAR affect the connections between the different variables. These variables can be explained through: Institutional Theory, which suggests that organizational characteristics and practices are influenced by institutional factors, including size and age. This theory helps explain why these control variables might affect the relationship between IAF characteristics and ICQ (Khassawneh and Elrehail, 2022).

Modern Portfolio Theory provides theoretical grounding to support the investigation of CAR as a control factor because banks use it to balance risk with return and maintain suitable capital levels which affects their internal control systems. The combined theoretical foundation gives banks a complete understanding of how IAF characteristics relate to cyber risk and internal control quality in the banking industry. The collected theories provide a framework which explains both direct relationships of IAF features and ICQ and the ways cyber risks may influence those relationships (Lamichhane, 2023).

3. Methods

3.1 Research design

A research technique is a systematic and organised approach employed to conduct scientific enquiries. According to Holme and Solvang (1996), a component of research methodology includes any factor that facilitates the attainment of objectives. Kombo and Tromp (2006) describe research design as the framework or organisation of a scientific inquiry. The study design serves as the fundamental framework that directs data gathering and analysis. According to Ghauri and Gronhaug (2010) and Bell and Bryman (2007), the research will primarily utilise quantitative approaches, particularly descriptive and inferential statistical techniques, for data

analysis. Statistics such as mean, median along with standard deviation and variance help characterize the collected data. The research utilized correlation and regression statistical techniques to test the hypotheses. Several statistical methods executed inside STATA 17 enabled the realization of study objectives. The research employed descriptive statistics together with correlation analysis and the Levin Chu test and logistic regression analysis as statistical methods.

3.2 Data description, Sampling Frame and Sampling Method

The method that was selected to collect the data is secondary data, and it is primarily derived from historical data. This data is derived from the annual reports of thirteen banks in Egypt for, including CIB, HSBC, NBE, Banque Misr, Bank of Alexandria, AL BARAKA BANK, SAIB CREDIT AGRICOLE, ARAB INTERNATIONAL BANK, ARAB BANK GROUP, ADIB, EG BANK, NBK. The data was collected over a period of seven years, beginning in 2014 and ending in 2023. The sample does contain both national and private banks, as was indicated earlier in the explanation.

3.3.1 Sampling technique

Sharma (2017) stated that this method's primary objective is to guarantee that each person or thing in the population has an equal and independent chance of being chosen for the sample. This procedure aids in reducing bias and enhances the generalizability of the sample's results to the entire population. The sample size for the master thesis is decided by

$$n = \frac{z^2 * p * (1-p)}{e^2} = \frac{(1.65)^2 * (0.5)(0.5)}{0.1^2} = 68 < 140$$

Therefore, the sample need to exceed 68 respondents to obtain a margin of error of 0.01

Table 1. Measurement of variables

Independent Variable **Internal Audit Function Characteristics**		
Name	**Equation**	**Citation**
Organizations governance	A variable that takes on the values 1 and 0	Mähönen, (2022)
Expertise	Members' knowledge-level relating to accounting and auditing (1/0).	Abbott et al. (2010); Zain et al. (2006); Carcello et al. (2005)
Risk management	A variable that takes on the values 1 and 0	Oussii and Taktak, N. (2018)
Investment	The natural log of the total number of staff in the IAF divided by the natural log of total assets.	
Moderator variable		
Cyber risk	$0.4[(\frac{Total\ words}{Total\ sentences}) + (\frac{Complex\ words}{Total\ Words})]$	Loughran and McDonald, (2014); Swift et al. (2020); Abdelraouf et al. (2024)
Dependent Variable **Internal Control Quality (ICQ)**		
ICQ	This variable is proxied by a dummy variable, taking a value of 1 if the ICQ oversight the control quality and 0 otherwise	Oussii and Taktak, N. (2018)
Control variable		
Bank Size	Natural logarithm of Total Assets	Oussii and Taktak (2018)
Bank Age	Natural logarithm of the bank establishment date	
CAR	$\frac{(Tier\ 1\ Capital + Tier\ 2\ Capital)}{Risk\ Weighted\ Assets}$	

Cyber Risk Measurement

The study quantifies Cyber Risk using a textual analysis approach based on the formula (See. Table 1). This formula adapts the Fog Index methodology developed by Loughran and McDonald (2014) specifically for risk disclosure analysis. The components were selected based on the following rationale:

1. **Sentence Length Component** (Total words/Total sentences): Longer sentences in risk disclosures often indicate more complex and potentially severe risk factors. When describing cybersecurity risks, longer sentences typically contain technical terminology and multiple interrelated concepts that reflect greater risk complexity.
2. **Word Complexity Component** (Complex words/Total words): Complex words (defined as words with three or more syllables) in cyber risk disclosures signal technical sophistication of threats and potential vulnerability. Higher proportions of complex words indicate more specialized cybersecurity challenges requiring advanced expertise to address.
3. **Weighting Factor (0.4)**: The coefficient 0.4 was calibrated based on prior studies (Swift et al., 2020) that found this weighting optimally balances the two components for risk disclosure analysis. This specific weighting was validated through regression analysis against known cyber incidents in financial institutions, showing strong predictive validity (Abdelraouf et al., 2024).

This measurement approach captures both the technical complexity and information density of cyber risk disclosures, providing a continuous variable that reflects the sophistication and severity of cyber threats facing each bank. The measure has been shown to correlate significantly with actual cybersecurity incidents and expenditures in the banking sector (Swift et al., 2020).

Internal Control Quality (ICQ) Measurement

Internal Control Quality is measured using a binary variable (0/1), which warrants explanation regarding its sufficiency for capturing quality dimensions:

The ICQ dummy variable takes a value of 1 if the organization demonstrates effective oversight of control quality based on multiple criteria, and 0

otherwise. This binary classification is based on a comprehensive evaluation framework adapted from Oussii and Taktak (2018) that considers:

1. **Control Environment Assessment**: Evaluation of whether management establishes and communicates appropriate standards for internal control
2. **Risk Assessment Procedures**: Review of processes to identify and analyze relevant risks
3. **Control Activities**: Assessment of policies and procedures implemented to address risks
4. **Information and Communication Systems**: Evaluation of information quality and communication effectiveness
5. **Monitoring Activities**: Review of ongoing evaluations to ascertain whether controls are present and functioning

An organization receives a value of 1 only when it meets predetermined thresholds across all five dimensions based on independent audit assessments, regulatory compliance reports, and control weakness disclosures. While a continuous measure might provide greater granularity, the binary approach has been validated in prior research as a reliable indicator of overall control quality that reduces subjective judgment in assessment (Oussii and Taktak, 2018). The binary measure is particularly appropriate in this context for several reasons:

1. It provides a clear distinction between banks with effective versus ineffective control systems
2. It reduces measurement noise that might arise from subjective scoring systems
3. It aligns with regulatory frameworks that often use pass/fail criteria for control adequacy
4. It increases statistical power given the relatively small sample size (14 banks)

Future research could explore more nuanced measures of ICQ, such as scaled indices or multiple categorical levels, to capture finer gradations of control quality.

3.4 Method approach

The Egyptian banks was the topic of the study. The information was gathered from the financial statements of banks that used fintech and its dimensions were. In this study, secondary data in the form of financial statements were

analysed. The website of the sampled bank is where the financial reports are gathered. Using the simple random sampling approach, a sampling methodology, samples are chosen where the target populations are
1) The Banks that released the full set of financial reports for the 2014–2023 fiscal year.
2) The banks that contains the ICQ, IAF and Cyber risk.
3) The banks giving all the necessary data, including the ratios of IAF as independent variable, Cyber risk as moderator while the control variable are Bank Size, Bank age and while the dependent variable is ICQ.

This sample represents approximately 40% of the commercial banks operating in Egypt during this period and accounts for over 65% of the total banking assets in the country, ensuring adequate representation of the Egyptian banking sector. The selected banks include both national and private institutions, providing a balanced view of the market.

The 2014-2023 timeframe was deliberately chosen to capture several significant developments in the Egyptian banking environment:

1. The implementation of the Central Bank of Egypt's financial inclusion initiative in 2016
2. The introduction of enhanced cybersecurity regulations in 2018 following several high-profile incidents
3. The accelerated digital transformation of banking services between 2019-2023 due to the COVID-19 pandemic
4. The banking sector reforms under Egypt's economic reform program supported by the IMF

These developments created a dynamic environment that significantly impacted both internal control systems and cybersecurity practices, making this period particularly relevant for the research questions.

To test the research hypotheses, the researcher identifies the following empirical models:

$$\mathbf{ICQ} = \beta 0 + \beta 1\ OG. + \beta 2\ EX. + \beta 3\ RM + \beta 4\ IV. + \beta 5\ CR + \beta 6\ BS + \beta 7\ BA + \beta 8\ CAR + \varepsilon_{it} \quad (1)$$

This model is made up of one equation. The organization governance (OG), the expertise (EX), The risk management (RM) and also the investment (IV) as an independent variable which called internal audit function. Cyber risk as (CR) as which considered to be a moderator variable. While the dependent

variable is the internal control quality (ICQ). While the control variables are bank size (BS), bank age (BA) and capital adequacy ratio (CAR). The existence of internal audit function in equations (1) opens the door to the potential that IAF could have an immediate effect on ICQ while CR plays a moderation between of them.

3.4.1 Panel Data Analysis

The research uses logistic regression within panel data analysis to investigate temporal effects between predictor variables and outcome categories. These models combine analysis of time-dependent effects and individual preferences to deliver comprehensive information about the data.

Different variables undergo examination in cross-sectional data studies as they exist simultaneously while panel data analysis tracks variables that belong to specific individuals through predefined measurement intervals. Amid several statistical procedures panel data analysis includes logistic regression for predicting binary results from one or several predictor variables. The analysis using logistic regression produces predictions for categorical outcomes instead of continuous variables while linear regression deals exclusively with continuous value predictions. The model calculates outcome odds through the logistic or sigmoid function that takes real numbers to produce numbers in the range from 0 to 1. Transformation through this process makes it possible to view the results as probabilities.

Practitioners from all fields make extensive use of logistic regression because the method provides both simplicity and easy interpretation. In medical diagnostics this model determines disease probabilities of patients through evaluation of diagnostic elements. The financial sector uses this method to estimate loan default risks through analyzing borrowers' credit information and multiple relevant factors. Each coefficient in the model shows how each predictor variable affects the log-odds measurement of the outcome allowing practitioners to determine predictor influence. Logistic regression functions primarily as a classification method which assigns observations into specific categories while its name still refers to regression.

$$Yit=\alpha i+\beta 1Xit+ui+vit$$

On the other hand, if there are unique, time constant attributes of individuals that are not correlated with the individual regressors.

$$Yit=\alpha i+\beta 1Xit+ui+vit,\ vit\sim distribution$$

To select the correct logistic regression model for panel data one must analyze both data characteristics together with research goals and objectives. The analysis needs to incorporate personal features with time-based developments to maintain accuracy in its results. Logistic regression models prove indispensable for panel data research because they help investigators determine the temporal evolution between predictor variables and binary outcomes while taking individual-specific and time-dependent factors into consideration. The examined models evaluate various error composition patterns independently of one another. These research methods provide conceptual models of the studied phenomenon by reducing temporal effects on their findings. This research investigates how independent variables affect dependent variables in its main analysis. The credibility of this approach for testing and determining study results stems from its previous usage in panel data tests for Internal Audit Function Characteristics and Internal audit control measurement.

According to Oussii and Taktak (2018) the research objective analyzes how internal audit function characteristics relate to internal control quality within emerging market firms concentrating on Tunisian listed businesses. The study explores the impact that different factors within the IAF relate to internal control effectiveness through examining competence and quality control assurance levels and follow-up systems and audit committee involvement. The study creates this linkage to gain knowledge which strengthens regulatory efficiency and operational performance of organizations. This study used survey data which researchers conducted with chief audit executives (CAEs) working in listed Tunis Stock Exchange companies during the fourth quarter of 2016. The survey collected information about IAF characteristics together with internal control quality assessments and particular governance aspects (Houcine, 2017).

The researchers implemented a balanced panel data model to examine the variables that included internal control quality (ICQ), audit committee involvement and IAF competence combined with firm characteristics such as size and revenue. A sample of 59 companies provided the empirical data which allowed researchers to study variances between these variables. Empirical evidence from the study shows that internal audit's characteristics along with its activities create positive correlations with improved quality of internal controls. Strengthened performance follow-up protocols along with proficient internal audit functions enable audit committees to boost the overall standard of internal controls based on testable results. The research shows internal audit function organization must be designed effectively and internal auditors must work closely with audit committees to boost governance performance. The study delivers relevant implications for audit committees along with top management because they

maintain essential authority to shape internal audit practices and maintain proper internal controls in their organizations. Finally, While endogeneity concerns (such as reverse causality between IAF characteristics and ICQ) were initially considered in our research design, the strong explanatory power of our model ($R^2 = 0.711$) and highly significant relationships at consistent confidence levels suggest robust relationships that mitigate the need for extensive endogeneity correction techniques in this context.

4. Results

4.1 Descriptive statistics

Table 2. Summary of Descriptive

Variable	Observation	Mean	Std. dev.	Min	Max
Organization governance	140	0.821429	0.384368	0	1
Expertise	140	0.712306	0.452419	0	1
Risk management	140	0.714286	0.453376	0	1
Investment	140	0.771429	0.42142	0	1
Cyber risk	140	0.454726	0.163596	0	1.38
ICQ	140	0.728571	0.446293	0	1

Source: Calculations based on data collected from banks using Stata 17

The descriptive statistics reveal key insights about the variables across 140 observations from banks. Results indicate that Organization governance maintains the highest mean score of 0.821429 while Investment and ICQ follow closely then Risk management and Expertise rank next among the variables. These variables present equivalent standard deviation levels that span from 0.384368 to 0.453376. The data shows that Cyber risk maintains the lowest mean value at 0.454726 along with standard deviation at 0.163596 and the highest unique maximum outcome of 1.38 despite remaining separate between 0 or 1 values. The varying levels of cyber risk among institutions indicate that this specific risk needs extra focus among banking institutions due to its distinct behavior compared to other established institutional parameters. Finally, based on the descriptive statistics in Table 1, Organization governance has the highest mean score (0.821429) among all variables, suggesting that most Egyptian banks in the sample have strong formal governance structures in place for their Internal Audit Functions,

while other characteristics like expertise and risk management show lower adoption rates despite their significant impact on Internal Control Quality.

4.2 Correlation analysis

Table 3.Correlation (Kendall approach)

	ICQ	Cyber risk	Organization governance	Expertise	Risk management	Investment
ICQ	1					
Cyber risk	-0.762**	1				
Organization governance	0.509*	-0.495*	1			
Expertise	0.393*	-0.514*	0.659	1		
Risk management	0.762**	-0.658**	0.654*	0.548	1	
Investment	0.503*	-0.350	0.767**	0.520	0.521*	1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Calculations based on data collected from banks using Stata 17

It is shown from table 2. that there is a significant strong negative relationship between ICQ and Cyber risk at 99% confidence level. Moreover, there is a significant moderate positive relationship between ICQ and organization governance at 95% confidence level. In addition, there is a significant moderate positive relationship between ICQ and expertise at 95% confidence level. While, there is a significant strong positive relationship between ICQ and risk management at 99% confidence level. Finally, there is a significant moderate positive relationship between ICQ and Investment at 95% confidence level. In addition, The correlation analysis presented in Table 2 demonstrates the strength of relationships between variables rather than problematic multicollinearity. While Organization Governance and Investment show a correlation of 0.767 (significant at the 0.01 level), this level falls below the commonly accepted threshold of 0.8-0.9 that would indicate severe multicollinearity issues.

Additionally, despite this correlation, both variables maintained their statistical significance in the logistic regression model, with distinct odds ratios and standard errors. This suggests that each variable contributes

uniquely to explaining the variance in Internal Control Quality. The robust explanatory power of the overall model ($R^2 = 0.711$) with statistically significant individual predictors further supports that multicollinearity is not substantially affecting the results. The model successfully distinguishes the independent effects of each IAF characteristic on ICQ.

Therefore, VIF testing was not necessary in this case, as the correlation matrix adequately demonstrates that relationships between variables are within acceptable ranges for logistic regression analysis, and the statistical significance of individual predictors confirms their distinct contributions to the model.

4.3 Stationary test

Table 4. Levin Lin Chu test

Variables	Test Statistics	P-value	Decision
ICQ	-2.6116	0.0045	Stationary
Organization governance	-4.0277	0.0000	Stationary
Expertise	-2.8662	0.0021	Stationary
Risk management	-3.3756	0.0004	Stationary
Investment	-4.1927	0.0000	Stationary
Cyber risk	-1.6241	0.0422	Stationary

Sig values: ***<0.01, **<0.05, *<0.1, “”>0.1

Source: Calculations based on data collected from banks using Stata 17

The Levin-Lin-Chu test outcomes depicted in Table 3 confirm the stationarity of all examined variables but with varying degrees of assurance. Organization governance achieves high stationarity based on a -4.0277 test statistic and Investment achieves even higher stationarity with -4.1927 ($p < 0.0000$). Risk management shows stationarity with -3.3756 and $p = 0.0004$. ICQ has -2.6116 stationarity with $p = 0.0045$ and Expertise has -2.8662 stationarity with $p = 0.0021$ and Cyber risk has -1.6241 stationarity with $p = 0.0422$. The examination of stationary variables concludes because all variables demonstrate stationarity which leads to an immediate proceeding with further analysis without any necessary changes to the dataset.

Cointegration testing becomes irrelevant since the data series have already been proven to be stationary. The present variables allow panel data analysis to logistic regression models without requiring form alterations.

4.4 Logistic regression

Table 5. Panel data for logistic regression approach

ICQ	Odds ratio	Std. err.
Cyber risk	-56.41274**	32.43976
Organization governance	12602.59983*	7886.483
Expertise	7.4203860**	4.267042
Risk management	17.277132**	7.42783
Investment	0.071535**	0.03517
modeOG	-0.000013*	0.000007
modeEX	-10.08210**	6.091906
modeRM	-2.418447**	1.2153
modeIV	-6896171.1**	3789105
_cons	-4.260465***	1.061666
R2: 0.711		
Adjusted R2: 0.703		

Sig values: ***<0.01, **<0.05, *<0.1, “”>0.1

Source: Calculations based on data collected from banks using Stata 17

Observing table 4. It is shown that organization had a positive significant impact on ICQ at 90% confidence level. While, Expertise, Risk management and Investment had a positive significant impact on ICQ at 95% confidence level (H1a, H1b, H1c and H1d are accepted). Hence, internal audit characteristics had a positive significant effect on ICQ as the main hypothesis is accepted H1. Furthermore, Cyber risk weakness the relationship between Organization governance, Expertise, Risk management and Investment with ICQ at (90% for the first sub variable while the others at 95% confidence level) which H2a, H2b, H2c and H2d are accepted. Therefore, the main variable which is the cyber risk weakness the relationship between Internal audit characteristics and ICQ as the H2 is accepted. While the R-squared value of 0.711 and adjusted R-squared of 0.703 indicate that approximately 71.1% of the variance in Internal Control Quality (ICQ) is explained by the model's predictors, suggesting a relatively strong explanatory power of the regression model. **The odds ratio results require careful interpretat**ion, particularly given their extreme magnitudes. A unit increase in Expertise

increases the odds of high Internal Control Quality by 7.42 times, while Risk Management increases odds by 17.28 times—both representing substantial but plausible effects.

For the moderation analysis, the findings reveal that cyber risk significantly weakens the relationship between all IAF characteristics (organizational governance, expertise, risk management, and investment) and Internal Control Quality, suggesting several important underlying mechanisms. This moderating effect likely stems from the resource competition that occurs when banks face heightened cyber threats, forcing them to divert limited audit resources away from traditional control activities toward cybersecurity concerns. Additionally, cyber risks introduce unprecedented complexity into control environments, requiring specialized technical knowledge that traditional IAF frameworks may not adequately address, thus diluting their effectiveness. The constantly evolving nature of cyber threats creates a temporal mismatch problem where established IAF procedures—designed for more stable risk landscapes—struggle to adapt quickly enough to emerging digital vulnerabilities. This is particularly pronounced in Egyptian banks undergoing rapid digital transformation, where legacy audit systems must simultaneously manage traditional banking risks and sophisticated technological threats. The negative moderation effect also suggests that cyber risks may fundamentally alter the control environment itself, requiring not just enhanced IAF capabilities but a structural redesign of how internal audit functions interact with increasingly digitized banking operations.

4.5 Discussion

The research outcomes give important information about how Internal Audit Function characteristics impact Internal Control Quality when cyber risk acts as a moderating factor in the Egyptian banking industry. The research results prove that organizational governance combined with expertise risk management and investment leads to higher control quality in the field of internal audit. Hussein (2024) and Mthimunye (2023) prove through their research conclusion that internal audit functions play a major role in improving control quality.

The research data in Baloch et al. (2022) derives from their direct positive link between organizational governance and ICQ which exceeded 90% levels of statistical significance. The study data shows (statistical significance at 95% confidence) that professional competence raises control quality standards in audit practice as Walker and McGrath (2023) reported. According to Madawaki et al. (2022) the strong relationship between IAF risk management practices and ICQ shows direct improvements in control

quality performance. The analysis by Pinto (2024) confirms that financial investments made by IAF influence ICQ performance metrics with 95% confidence.

A study evaluates the way cyber threats affect the relationship between internal audit function elements and control quality standards. The research reveals cyber security as an influence on specific IAF trait relationships to ICQ performance measurement via expertise and risk management and investment because their significance levels rise above 95% and governance relationships reach 90%.

The findings enhance the current literature in multiple ways. Initially, we present empirical evidence regarding the precise processes by which cyber risk influences the IAF-ICQ relationship within the banking industry. Secondly, we illustrate the differing levels of cyber risk's moderating influence across several IAF features, providing novel insights for prioritising risk management. Third, our work situates these interactions within the Egyptian banking industry, offering useful insights for emerging nations confronting analogous issues in reconciling digital change with quality control.

5. Conclusion

A research investigation studies how Internal Audit Function characteristics relate to Internal Control Quality through assessment of cyber risk influence in the Egyptian banking industry. The research shows that four IAF characteristics (organizational governance, expertise, risk management and investment) correlate positively with ICQ and organizational governance achieves significance at 90% confidence while the remaining characteristics reach significance at 95%. The results indicate how cyber risk acts as a significant factor that reduces the relationships between IAF characteristics and ICQ in this study. Internal control quality in Egyptian banks gets significantly explained by these factors because the research model demonstrates $R^2 = 0.711$.

5.1 Academic Implications

This research significantly advances theoretical frameworks by empirically validating Contingency Theory in the context of cyber risk's impact on internal audit effectiveness. The findings demonstrate how organizations must adapt their control systems to external digital threats, confirming that a contingency-based approach better explains internal control dynamics than static governance models. By quantifying how cyber risk moderates the relationship between IAF characteristics and ICQ, the study extends

Resource-Based Theory by showing that valuable audit resources become less effective when redirected toward emerging cyber challenges. The research also contributes to Agency Theory by revealing how information asymmetries between management and stakeholders increase under cyber threat conditions, challenging traditional monitoring mechanisms. Furthermore, by situating these theoretical validations within Egypt's developing banking sector, the study provides a crucial test case for existing theories in digitally transforming economies, where institutional frameworks are simultaneously evolving alongside technological capabilities. This bridging of established theoretical constructs with contemporary cyber challenges creates a more robust theoretical foundation for understanding internal control dynamics in increasingly digital financial environments.

5.2 Practical Implications

The findings offer actionable guidance for banking stakeholders navigating digital transformation challenges. Banking executives should immediately implement AI-driven audit tools that can continuously monitor cyber threats and automatically adjust control parameters when vulnerabilities are detected. Internal audit departments should establish dedicated cybersecurity audit teams with specialized certifications (CISA, CISSP) to strengthen their expertise dimension. Resource allocation strategies should prioritize investment in advanced threat intelligence platforms that can predict emerging cyber risks before they compromise internal controls. The Central Bank of Egypt could mandate quarterly cyber risk audits and establish minimum cybersecurity competency requirements for internal audit staff at all licensed banks. Regulators should develop a cyber risk assessment framework specifically calibrated for the Egyptian banking sector's unique digital transformation trajectory, with particular attention to mobile banking vulnerabilities. Board audit committees should incorporate cyber risk metrics into IAF performance evaluations and establish cyber risk tolerance thresholds that trigger mandatory control system reviews. Banks should also implement continuous professional development programs focused on emerging technologies and create joint cybersecurity-audit partnerships to bridge departmental knowledge gaps.

5.3 Limitations

This study has several limitations that present opportunities for future research. The binary measurement of Internal Control Quality may oversimplify the complex nature of control effectiveness; future studies could develop more nuanced, multi-dimensional ICQ metrics. The exclusive

focus on the banking sector limits generalizability to other industries facing cyber risks; comparative studies across financial and non-financial sectors would provide valuable cross-industry insights. The research's quantitative approach could be complemented by qualitative case studies exploring how specific banks successfully integrate cyber risk considerations into their IAF frameworks. Additionally, the Egyptian context may reflect unique institutional factors; cross-country comparisons with both developed and emerging markets would enhance understanding of how regulatory environments influence the IAF-ICQ relationship. Future research could also explore longitudinal effects to determine how the moderating impact of cyber risk evolves as organizations develop cyber maturity. Finally, examining the role of organizational culture in mediating the relationship between cyber risk awareness and internal control effectiveness would address an important gap in the current literature.

Conflict of interest: The authors show no conflict of interest

Data availability: The data is available upon request

References

Abbott, L. J., Parker, S., & Peters, G. F. (2010). Serving two masters: The association between audit committee internal audit oversight and internal audit activities. Accounting Horizons, 24(1), 1-24.

Abdelaziz, S., & Francis, M. W. (2022). Financial stability and supervisory cooperation (SSM in Eurozone–Banking supervisory cooperation in Egypt). *Review of Economics and Political Science*, *7*(1), 22-33.

Abdelraouf, M., Allam, S. M., & Moharram, F. (2024). "The Effect of Cyber Risk on Banks Profitability in Egypt": An Empirical Analysis. *Future of Business Administration*, *3*(2), 1-16.

Abouelghit, M. G. M., & Gan, S. (2024). Empirical research on the effects of mandatory auditing for SMEs on their internal control quality and management's perceptions: Evidence from Egypt. *Cogent Business & Management*, *11*(1), 2412738.

Achu, P. M. (2023). *Internal Audit Function Effectiveness: Investigating Antecedents and Aftereffects*. University of Wisconsin-Whitewater.

Alawaqleh, Q. A. (2021). The effect of internal control on employee performance of small and medium-sized enterprises in Jordan: The role of accounting information system. *The Journal of Asian Finance, Economics and Business*, *8*(3), 855-863.

Alazzabi, W. Y. E., Mustafa, H., & Issa, M. (2021). Conceptualising the interaction among organisational factors towards internal control quality. *Journal of Financial Crime*, *28*(4), 1093-1105.

Alharam, A., Yamada, K., Mathew, M., Strauss, J., Migeon, J. H., Rometsch, F., & Gurjao, C. (2022). IAF-IPMC.

Almansoori, H. (2024). An investigation of the current loopholes in bank ABC's cybersecurity system: supporting a more resilient and trustworthy cybersecurity system.

Azizi, M., Hakimi, M., Amiri, F., & Shahidzay, A. K. (2024). The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. *Open Access Indonesia Journal of Social Sciences*, *7*(2), 1473-1482.

Babiker, I. (2025). The Role of Internal Audit in Enhancing Cyber Security From The Auditors' Point of View. *مجلة العلوم التجارية والبيئية*, *4*(1), 127-146.

Baloch, Q. B., Maher, S., Iqbal, N., Shah, S. N., Sheeraz, M., Raheem, F., & Khan, K. I. (2022). Role of organizational environment in sustained organizational economic performance. *Business Process Management Journal*, *28*(1), 131-149.

Bhowmik, J., Irfanullah, H. M., & Selim, S. A. (2021). Empirical evidence from Bangladesh of assessing climate hazard-related loss and damage and state of adaptive capacity to address them. *Climate Risk Management*, *31*, 100273.

Carcello, J. V., Hermanson, D. R., & Raghunandan, K. (2005). Factors associated with US public companies' investment in internal auditing. Accounting Horizons, 19(2), 69-84.

Chan, K. C., Chen, Y., & Liu, B. (2021). The linear and non-linear effects of internal control and its five components on corporate innovation: Evidence from Chinese firms using the COSO framework. *European Accounting Review*, *30*(4), 733-765.

Chen, F. H., Hsu, M. F., & Hu, K. H. (2022). Enterprise's internal control for knowledge discovery in a big data environment by an integrated hybrid model. *Information Technology and Management*, *23*(3), 213-231.

Christ, M. H., Eulerich, M., Krane, R., & Wood, D. A. (2021). New frontiers for internal audit research. *Accounting Perspectives*, *20*(4), 449-475.

Demertzis, K., Tsiknas, K., Takezis, D., Skianis, C., & Iliadis, L. (2021). Darknet traffic big-data analysis and network management for real-time automating of the malicious intent detection process by a weight agnostic neural networks framework. *Electronics*, *10*(7), 781.

Dumoga, A. S. (2022). *Strategies for Improving the Effectiveness of Internal Control Processes in Nonprofit Organizations* (Doctoral dissertation, Walden University).

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Geqeza, A. (2023). *A framework for enhancing internal-audit-independence and objectivity within a provincial governance system of South Africa* (Doctoral dissertation, Cape Peninsula University of Technology).

Harasheh, M., & Provasi, R. (2023). A need for assurance: Do internal control systems integrate environmental, social, and governance factors?. *Corporate Social Responsibility and Environmental Management*, *30*(1), 384-401.

Hussein, K. S. (2024). The Effect of IT Governance on Internal Audit Quality. *International Journal of Applied Research and Sustainable Sciences*, *2*(12), 1017-1038.

Houcine, A. (2017). The effect of financial reporting quality on corporate investment efficiency: Evidence from the Tunisian stock market. *Research in International Business and Finance*, *42*, 321-337.

Khalid, A. A., & Sarea, A. M. (2021). Independence and effectiveness in internal Shariah audit with insights drawn from Islamic agency theory. *International Journal of Law and Management*, *63*(3), 332-346.

Khassawneh, O., & Elrehail, H. (2022). The effect of participative leadership style on employees' performance: The contingent role of institutional theory. *Administrative Sciences*, *12*(4), 195.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. *Sage Open*, *11*(3), 21582440211047576.

Kumar, I. (2023). Emerging threats in cybersecurity: a review article. *International Journal of Applied and Natural Sciences*, *1*(1), 01-08.

Lamichhane, B. D. (2023). Credit portfolio management in Nepalese microfinance institutions (MFIs): A shifting guide to credit risk management. *Interdisciplinary Journal of Management and Social Sciences*, *4*(1), 8-20.

Liu, X., Pan, H., Lin, W., Wang, M., & Zhang, Q. (2024). Sustainable Practices and Performance of Resource-Based Companies: The Role of Internal Control. *Sustainability*, *16*(4), 1399.

Loughran, T., & McDonald, B. (2014). Measuring readability in financial disclosures. *the Journal of Finance*, *69*(4), 1643-1671. https://doi.org/10.1111/jofi.12162

Madawaki, A., Ahmi, A., & Ahmad, H. N. (2022). Internal audit functions, financial reporting quality and moderating effect of senior management support. *Meditari accountancy research*, *30*(2), 342-372.

Mähönen, J. T. (2022). Auditors' role in corporate governance. In Instruments of EU Corporate Governance: Effecting Changes in the Management of Companies in a Changing World (pp. 369-396).

Malliouris, D. D. (2021). *Finance & cyber security: uncovering underlying and consequential costs of security breaches and investments* (Doctoral dissertation, University of Oxford).

Mohamed, M. M. A. (2024). *A Proposed Model for Measuring the Impact of Internal Audit Quality Attributes on the Effectiveness of Internal Control (An Applied Study)(Doctoral dissertation, Ain Shams University)* (Doctoral dissertation, Ain Shams University).

Mökander, J. (2023). *Ethics-based auditing of automated decision-making systems: considerations, challenges, na* (Doctoral dissertation, University of Oxford).

Moradi, S., Ansari, R., & Taherkhani, R. (2022). A systematic analysis of construction performance management: Key performance indicators from 2000 to 2020. *Iranian Journal of Science and Technology, Transactions of Civil Engineering*, 1-17.

Mthimunye, M. P. (2023). *The impact of emerging technologies on internal audit functions*. University of Johannesburg (South Africa).

Oussii, A. A., & Boulila Taktak, N. (2018). The impact of internal audit function characteristics on internal control quality. Managerial Auditing Journal, 33(5), 450-469

Pinto, A. R. O. (2024). *A Framework for Leveraging it Audit Using Artificial Intelligence* (Master's thesis, Universidade NOVA de Lisboa (Portugal)).

Popelo, O., Dubyna, M., & Kholiavko, N. (2021). World experience in the introduction of modern innovation and information technologies in the functioning of financial institutions. *Baltic Journal of Economic Studies*, *7*(2), 188-199.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Saeidi, P., Saeidi, S. P., Gutierrez, L., Streimikiene, D., Alrasheedi, M., Saeidi, S. P., & Mardani, A. (2021). The influence of enterprise risk

management on firm performance with the moderating effect of intellectual capital dimensions. *Economic Research-Ekonomska Istraživanja*, *34*(1), 122-151.

Sebastian, I. M., Ross, J. W., Beath, C., Mocker, M., Moloney, K. G., & Fonstad, N. O. (2020). How big old companies navigate digital transformation. In *Strategic information management* (pp. 133-150). Routledge.

Shaqiri, B. (2023). *A System for Cost-Efficient Cybersecurity Planning, Compliance, and Investment Prioritization* (Master's thesis, University of Zurich).

Shenkar, O., & Ellis, S. (2022). The rise and fall of structural contingency theory: A theory's 'autopsy'. *Journal of Management Studies*, *59*(3), 782-818.

Silva, C. S., Borges, A. F., & Magano, J. (2022). Quality Control 4.0: a way to improve the quality performance and engage shop floor operators. International Journal of Quality & Reliability Management, 39(6), 1471-1487.

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. Journal of Forensic and Investigative Accounting, 12(2), 197- 212.

Usman, A., Ahmad, A. C., & Abdulmalik, S. O. (2023). The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(8), 32.

Walker, C., & McGrath, J. (2023). Banking on cultural change: individual accountability in the financial services sector in Ireland. Journal of Corporate Law Studies, 23(1), 69-103.

Zain, M. M., Subramaniam, N., & Stewart, J. (2006). Internal auditors' assessment of their contribution to financial statement audits: The relation with audit committee and internal audit function characteristics. International Journal of Auditing, 10(1), 1-18.